EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Towards a New EU Legal Framework for Data Protection and Privacy

STUDY

EN 2011

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Towards a New EU Legal Framework for Data Protection and Privacy

Challenges, Principles and the Role of the European Parliament

STUDY

Abstract

This study addresses the new challenges stemming from data processing policies and systems falling in the scope of police and judicial cooperation in criminal matters in the EU Area of Freedom, Security and Justice. It identifies a set of common basic principles and standards for the genuine assurance of data protection in all the phases of EU policy-making and for the effective implementation of this fundamental right. The study puts forward a set of recommendations to guide the European Parliament's role and legislative inputs into the upcoming revision of the EU legal framework on data protection, which is expected to be launched by the end of 2011.

PE 453.216 EN

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs

AUTHORS

Prof. Didier Bigo (Centre d'Etudes sur les Conflits, C&C)
Dr Sergio Carrera (Centre for European Policy Studies, CEPS)
Ms Gloria González Fuster (Vrije Universiteit Brussel, VUB)
Prof Elspeth Guild (CEPS and Radboud University of Nijmegen)
Prof. Paul de Hert (Vrije Universiteit Brussel, VUB)
Dr Julian Jeandesboz (Centre d'Etudes sur les Conflits, C&C)
Dr Vagelis Papakonstantinou (Vrije Universiteit Brussel, VUB)

The authors would like to express their gratitude to Mr João Soares da Silva (CEPS) for his assistance in the research and editing of this report.

Under coordination of Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS) and the Centre d'Etudes sur les Conflits (C&C)

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department C - Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@europarl.europa.eu

Manuscript completed in September 2011

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
API	Advanced Passenger Information
BMS	Biometric Matching System
CEPOL	European Police College
CFSP	Common Foreign and Security Policy
CIREFI	Centre for Information, Discussion and Exchange on the Crossing of Frontiers and Immigration
CIS	Customs Information System
CISA	Convention on the Implementation of the Schengen Agreement
CJEU	Court of Justice of the European Union
COE	Council of Europe
COSI	Committee of Internal Security
DPA	Data Protection Authority
DPD	Data Protection Directive
DPF	Data Protection Framework
DPFD	Data Protection Framework Decision
DPIA	Data-Protection Impact Assessment
DRD	Data Retention Directive
ECB	European Central Bank
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENNIR	European Network of National Intelligence Reviewers
EP	European Parliament
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research Innovation Forum
EU-ESTA	EU Electronic System of Travel Authorisation
EUROSUR	European Border Surveillance System
FIS	FRONTEX Information System
FRA	Fundamental Rights Agency

FRAN	FRONTEX Risk Analysis Network
FSC	FRONTEX Situation Centre
ILPA	Immigration Lawyers and Practitioners Association
IMS	Information Management System
ISS	Internal Security Strategy
JOU	Joint Operation Unit
JRO	Joint Return Operations
LIBE	Committee on Civil Liberties and Internal Affairs
MDG	Multidisciplinary Group on Organised Crime
OFAC	Office of Foreign Assets Control
OLAF	European AntiFraud Office
PASR	Preparatory Action on Security Research
PET	Privacy Enhancing Technologies
PNR	Passenger Name Record
RTP	Registered Traveller Programme
SIS	Schengen Information System
SIS II	Schengen Information System II
SitCen	Joint Situation Centre
SOA	Service-oriented Architecture
STOA	Science and Technology Options Assessment Unit
SWIFT	Society for Worldwide Interbank Financial Communication System
TECS	The Europol Computer System
TFTP	Terrorist Financial Tracking Programme
UMF	Universal Message Format
VIS	Visa Information System
WP29	Article 29 Data Protection Working Party
WPPJ	Working Party on Police and Justice

EXECUTIVE SUMMARY

The protection of personal data enjoys unprecedented legal status in the EU. It is recognised as an autonomous fundamental right in the legally binding EU Charter of Fundamental Rights (EU Charter). Additionally, the Treaties now provide a legal basis for the establishment of a comprehensive and coherent legal instrument for data protection, covering both the former first and third EU pillars around which EU Justice and Home Affairs cooperation was structured. In the context of the Lisbon Treaty and the 2009 Stockholm programme, ensuring the effectiveness of the protection of personal data has been set as a major priority of the EU Area of Freedom, Security and Justice (AFSJ). Yet, guaranteeing the protection of this right has been extremely hard in these policy domains. Significant, persisting obstacles and an increasing number of challenges render the achievement of this crucial objective particularly difficult.

This study looks at the protection of personal data in the AFSJ and explores data protection and privacy, along with their relation to the development of EU security policies and data processing practices in the context of cooperation on security and law enforcement. It addresses the following research questions:

- How can the new (post-Treaty of Lisbon) institutional and legal context contribute to the consolidation of the emergent – but still precariously developing – fundamental right to the protection of personal data in the AFSJ?
- What are the main challenges resulting from the increasing deployment of (data processing) technologies and systems for law enforcement purposes and EU-level (home affairs) inter-agency cooperation?
- What should be the main components included in the new legal framework and the common, basic legal principles by which it should be guided in order to address these data protection concerns genuinely and effectively?
- What can and should be the role of the European Parliament (EP) in this evolution, in accordance with its traditional position and new capabilities recognised in the new Treaty framework?

These questions are addressed while taking into account a number of factors:

- The Lisbon Treaty and the legally binding EU Charter have modified the obligations of EU institutions and agencies in terms of personal data protection. These new EU data protection obligations, however, do not replace the necessity of additionally complying with all the requirements derived from Article 8 of the European Convention on Human Rights and relevant case law of the Strasbourg Court. Such obligations and requirements apply across all EU policy fields, including security-related policies.
- The upcoming EU Data Protection Framework (DPF) needs to be designed in a way that ensures it has a genuine impact on future EU security measures and delivers protection in a practical way to individuals subject to these new law enforcement and data processing technologies.
- Such an impact can only be realised if data protection becomes relevant at all stages of EU policy-making processes.
- For data protection to be fully relevant at all stages of policy-making in the AFSJ, the principles of accountability, openness and transparency, along with other specific, common legal standards and monitoring mechanisms for data protection need to be established and guaranteed.

KEY FINDINGS

- The protection of personal data is recognised as an autonomous fundamental right in the legally binding EU Charter. This goes along with the provision of the current Treaties of a legal basis for the establishment of a comprehensive legal instrument for data protection that would cover the entire AFSJ. Ensuring the effectiveness of personal data protection has been highlighted as a key policy priority for the next generation of the EU's AFSJ by the Stockholm programme. Still, significant challenges to attaining this objective persist.

- The debate on the new legal framework on data protection in the field of law enforcement should focus on the extension of the general data protection provisions and principles provided in the Data Protection Directive (DPD) to the domains of police and judicial cooperation in criminal matters in the wider AFSJ. The drafting of a comprehensive regulatory framework for data protection has to take into account the specificities of EU policy-making practices in technology and data processing in the field of security. The framework must provide not only for solid and uniform common safeguards and legal principles, but also for policy guidelines and effective monitoring mechanisms in a field that so far has been characterised by two tendencies:

  - the tendency to treat technology as an 'unchallenged policy option', as seen in the substantial number of data processing schemes that have proliferated in EU AFSJ policies in relation to police and judicial cooperation in criminal matters during the last few years; and
  - the tendency towards 'programmatic policy-making'. More specifically, the absence of agreement among policy-makers and in relation to the private sector has resulted in policy practices whereby new data processing systems are initiated before schemes that have already been agreed upon are fully implemented. An overview of current and forthcoming schemes shows that there are currently more than 25 such initiatives. Programmatic policy-making has limited the possibility to run proper impact assessments, including privacy and budgetary impact assessments, and limits the possibility to assess the necessity and proportionality of the measures envisaged.

- The drafting of the new EU DPF has to take into consideration the specific directions of policies and practices in the field of police and judicial cooperation in criminal matters, in terms of the growing reliance on technology and particularly on data processing. These directions pose profound challenges to the fundamental right of data protection and privacy. There are four specific policy dilemmas concerning data protection and privacy:

  - a shift towards 'dataveillance', proactivity and profiling. The growing, systematic and massive collection of personal data is concomitant with the pursuit of anticipatory actions in relation to criminal offences. It involves the use of pattern recognition techniques (profiling), which tests the functioning of criminal justice systems and particularly the presumption of innocence as well as the principles of adequacy, proportionality, transparency and the right to effective legal remedies;
  - the extension of the 'life of data' and the risk of unregulated function-creep 'by default', which is problematic with respect to data protection principles, such as purpose limitation, consent and access;

  - the promotion, through the development of policy prescriptions on the technical architecture of data processing schemes, of a 'data sharing by default' attitude among law enforcement practitioners and authorities; and
  - the growing reliance of EU home affairs agencies (such as EUROPOL and FRONTEX) on dataveillance, which also includes the promotion of data processing schemes through the upcoming EU agency for the management of large-scale IT systems.

- The EP has played a major role in the construction of the right to the protection of personal data as an autonomous fundamental right in the EU, and in its recognition in a legally binding instrument, namely the EU Charter. Until now, however, it has relied only very timorously on the specificity of this innovative right, owing to a lack of comprehensive understanding of its nature or of political will (or both), generally framing the impact of data processing practices in terms of mere privacy infringements.
- Over the years, one of the main priorities for the EP has been to call for the reinforcement of data protection standards in the fields of police and judicial cooperation in criminal matters. The EP has commonly portrayed this as a precondition for the deployment of a series of data processing initiatives that it eventually supported. Another recurrent concern of the EP has been the issue of profiling through predictive data-mining. The EP's contribution to the framing of EU data protection and privacy policies offers a picture of where the institutional and substantial concerns are intrinsically linked. Many data protection and privacy controversies in which the EP has played an active role also mirror inter-institutional tensions, be it in relation to the applicable legislative procedure, to the division of competences through 'comitology' or to the powers linked to the conclusion of international agreements.
- There is no linear relationship between more involvement of the EP in decision-making, on the one hand, and a higher level of personal data protection granted to individuals, on the other. On the contrary, the strengthened participation of the EP in legislative procedures has lead in some cases to a lowering of data protection and privacy standards. Despite its formal commitment to the assurance and promotion of fundamental rights in the EU, as well as its different initiatives contributing to the assurance of the rights to data protection and privacy, the EP has not yet effectively questioned the factors underpinning the development of measures that threaten them the most. Notable in this regard are the modern transformations of policing and their connection with AFSJ policies and data processing systems, and the progressive design of an increasingly opaque web of data exchanges among EU home affairs agencies and from these nodes to the authorities of the Member States, as well as those of third countries.
- EU data protection rules in security and law enforcement matters are currently fragmented and heterogeneous. Police and judicial cooperation in criminal matters are excluded from the scope of the DPD. The 2008 Data Protection Framework Decision (DPFD) only applies to cross-border data processing. It provides for exemptions to all established data protection principles, and is flanked by a number of sector-specific rules adopted in the legal instruments related to the Schengen Information System, EUROPOL, EUROJUST and the Prüm Decision.
- The proposals tabled by the European Commission for a comprehensive legal framework, which have been partially endorsed by the European Data Protection Supervisor (EDPS), the Article 29 Data Protection Working Party (WP29) and the European Parliament, envisage the possible extension of this framework to police and judicial cooperation in criminal matters.
- The now imminent accession of the EU to the European Convention on Human Rights (ECHR) is expected to benefit the consideration of data protection principles.

Although no explicit mention of the right to data protection is made in the text of the ECHR, the European Court of Human Rights (ECtHR) has strongly linked data protection principles to the development of the right to privacy, as set in Article 8 of the Convention. The ECtHR has issued extensive case law in the field, rigorously applying the necessity and legitimacy of the processing criteria. In addition, it is not restricted in examining AFSJ data processing by any of its statutes. Even before the accession takes place, EU institutions must nonetheless ensure that the level of protection granted to individuals does not restrict or adversely affect human rights as recognised in the ECHR and as interpreted by the ECtHR case law.

- From a law-making point of view, two conceivable ways forward may be identified at this stage: i) either a new, single, comprehensive, standard-setting text will be introduced that will set the general rules for all personal data processing within the EU; or ii) processing not related to police and judicial cooperation in criminal matters, on the one hand, and processing in such fields, on the other, shall remain separate within the EU, through the continued existence of the DPD and the DPFD respectively, properly amended in the post-Lisbon environment. Although the merits and drawbacks of each option are elaborated, either option matters little as far as effective personal data protection is concerned: what matters is that power configurations and the identified challenges to data protection are dealt with and controlled, regardless of the legal means through which this goal is achieved.

RECOMMENDATIONS

Recommendation 1: One of the key elements of the revision of the EU DPF should be the extension of the applicable rules of general data protection to data processing in police and judicial cooperation in criminal matters, which have until now been kept separate, fully substantiating the fundamental right to the protection of personal data across EU law. A fully comprehensive DPF should provide benchmarks or standards against which legislative and policy initiatives aiming at establishing new data processing schemes could be evaluated and scrutinised.

- **Recommendation 2:** The new DPF applicable to AFSJ data processing practices should put the data subject at the heart of policy attention. It should focus on strategies for enabling individuals to make use of the subjective rights granted by the fundamental right to the protection of personal data, and to seek effective redress and remedies against any data controllers, including law enforcement agencies, that might have unlawfully processed their data. The right to data protection may ultimately prove irrelevant if individuals are not afforded the proper means to build and prove their case and contest illiberal practices. But this task seems to be difficult under the data protection framework currently in effect. Individuals need to collect evidence and establish jurisdiction – tasks that are difficult to accomplish and potentially expensive. Similar difficulties met in the DPD context have led to discussions in the direction of introducing a 'closest to home' individual right of redress. Such a right ought to be extended in AFSJ processing as well. In this context, independent and effective supervision of data protection also has a key role to play.
- **Recommendation 3:** The principle of accountability is of central importance in AFSJ personal data processing. To create added value in the amended EU DPF, this principle needs to address such questions as how to reconcile the need for specificity with a general principle and how to resolve the issue of scalability or proportionality. After all, the requirement for the introduction of accountability checks in AFSJ processing is particularly important given the actual, perhaps unrecognised, role of individual consent; increased accountability checks of data controllers warrant the efficient protection of individual rights.

- **Recommendation 4:** The principles of transparency and openness are equally central at times of providing a clear response to the challenges posed by AFSJ data processing policies, systems and practices. Yet so far law enforcement processing has been granted wide margin for exceptions. Because transparency mechanisms such as the notification system or the right to information and access or even the oversight by an independent authority could be said to hinder police work, substantial derogations have been granted in favour of such processing. The amended EU DPF needs to explicitly make reference to these principles. Their implementation in practice might require changing the structure of coordination and cooperation among data protection authorities (DPAs), with the competences for supervising data processing practices falling under the AFSJ (or further strengthening and further developing the role of the current WP29) or reversing the burden of proof in data protection litigation in favour of data subjects.
- **Recommendation 5:** Specific emphasis should be placed on the foreseeable orientations in data processing for security purposes to ensure that the data protection framework is robust and long lasting. The new DPF should develop a set of legal principles governing profiling in the EU's AFSJ. A definition of profiling should be included in the revised framework. This definition should also include the types of profiling that should be definitely prohibited under all circumstances and solid legal safeguards for those considered legitimate. The first type of profiling to be expressly prohibited is that which uses sensitive personal data as part of its basis. The second prohibition for profiling in the AFSJ should be on the use of unlawfully acquired data. Lastly, the profiling logic needs to adhere expressly to the general data protection principles, particularly that of fair and lawful processing.
- **Recommendation 6:** Particular attention should be given also to the rights of third-country nationals. A number of imminent or foreseen data processing schemes, such as the Visa Information System, the Registered Traveller Programme and the Entry/Exit System, will entail the intensive processing of personal data of individuals who are neither nationals nor residents of EU Member States, but who are also entitled to the enjoyment of the fundamental right to the protection of personal data, as well as to the right to privacy.
- **Recommendation 7:** Because the EU DPF review process is ambitious in scope, it needs to remain focused on primarily addressing the basic, contemporary, data protection issues. In the field of AFSJ personal data processing, it could make use of existing data protection means or those that are newly devised and currently under consideration (mostly, in the DPD review context):

  - The list of the fair information principles, as developed in the text of the DPD, needs to be extended to cover AFSJ processing as well.
  - New ideas currently elaborated in the DPD review context, such as the introduction of data-protection impact assessments and the implementation of the 'privacy-by-design' system architecture could prove of particular value for data protection purposes in AFSJ processing as well.
  - The role of national DPAs, while monitoring and controlling AFSJ personal data processing, needs to be strengthened in the amended EU DPF.
  - The introduction of a central coordination mechanism of supervisory authorities in the AFSJ, such as the WP29, is of paramount importance for data protection purposes.
  - Comprehensive provisions on data protection and the EU Charter should be integral to the legal mandates of all EU home affairs agencies, requiring full compliance with the principles of purpose limitation, purpose specification and rights for the data subject to access and correct the personal data held by agencies. Legal provisions must be accompanied by a robust supervisory mechanism that would ensure the practical delivery of these common principles

and standards. The above-mentioned establishment of an independent, central, EU coordinating authority for AFSJ processing compliance with data protection and privacy in the EU would constitute the proper approach for attaining this goal.

- **Recommendation 8:** An independent evaluation or review of existing and future EU data processing systems in the EU's AFSJ should be carried out by the EP. The adoption of a comprehensive data protection framework is not a panacea in the short run. Initiatives, proposals and programmes for the development and deployment of new data processing schemes in the EU have proliferated over the past few years, to the extent that keeping track of all of them is proving a considerable strain for not only civil society organisations and DPAs, but also for the EU institutions. The revision of the data protection framework therefore seems a good occasion to undertake a general, in-depth review of existing, upcoming and envisaged schemes for AFSJ data processing, complementing the stocktaking efforts of other EU institutions. Since the entry into force of the Treaty of Lisbon places the EP in the position of co-legislator in addition to its pre-existing powers as a budgetary authority, it is fully competent and entitled to conduct this exercise. Such a review should consist of the following elements:

  - an account and budgetary review conducted by the Court of Auditors; and
  - a data protection and privacy review to be initiated by the EP through its Science and Technology Options Assessment unit (STOA), in liaison with the EDPS, the WP29 and the European Union Agency for Fundamental Rights acting in their advisory capacities. It should include consultations with civil society organisations and an independent network of interdisciplinary academics.

1. INTRODUCTION: PUTTING EU DEBATES ON DATA PROTECTION IN THE CONTEXT OF THE EU'S AGENDA

Personal data protection is at a crucial point in the EU. EU institutions are to establish a new and comprehensive legal framework for the protection of individuals in relation to the processing of personal data, which is also possibly to apply to data processing in the area of police and judicial cooperation in criminal matters. This is of the foremost importance for the consolidation of the Area of Freedom, Security and Justice (AFSJ), where the reliance on security technologies and personal data processing is being constantly restated and continuously reinforced. By taking full advantage of the post-Lisbon architecture for the protection of fundamental rights and by actively contributing to its refinement, the European Parliament (EP) can play a decisive role in the design of a legal framework that effectively serves to redirect, influence, limit or oppose, when necessary, the adoption and deployment of measures that are dependent on intensified data processing and constitute infringements of fundamental rights and freedoms in general, and of the fundamental rights to personal data protection and privacy in particular.

This introductory chapter provides contextual background for an understanding of the current phase in EU law and policy on personal data protection, privacy and security. It offers an initial overview of traditional and recent struggles and debates, describes the major institutional and substantive implications of the Lisbon Treaty and the Stockholm programme (the third multi-annual programme on the EU's AFSJ) in this field, and introduces the major notions that frame and are used in the present study. Finally, it circumscribes the scope of the analysis, identifies the key issues at stake and puts forward the questions guiding the research.

1.1. A legacy of struggle from the pillar era

Ensuring effective personal data protection across the EU is one of the objectives of the current EU policy for the AFSJ. The European Council repeatedly referred to the momentousness of data protection and privacy in its strategic, multi-annual policy guidelines for the period 2010-14 enshrined in the Stockholm programme.[1] Commenting on the Programme, the EP insisted on the need to make sure "that the fundamental rights dimension of data protection and the right to privacy will be respected in all the Union's policies".[2] And, in the same context, the European Commission has underlined the importance and relevance of safeguarding privacy and data protection for the respect for the individual and for human dignity.[3]

Yet securing personal data protection in the AFSJ has over the years repeatedly appeared to be extremely challenging. Various factors can explain this situation. First is the sustained trend of EU institutions adopting, in the name of law enforcement or migration control (or both), and sometimes in the context of post-9/11 events, policy measures and tools that rely on the massive processing of data related to individuals, be it by widening data collection, by accumulating data stored, by enlarging data access opportunities to stored data or by multiplying data exchanges. In the words of the European Commission, "policies in the area of freedom, security and justice have developed in an incremental manner,

[1] European Council, The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens, OJ C 115, 4.5.2010, pp. 1-38.

[2] European Parliament, *Resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme*, P7_TA(2009)0090, 2009, § 83.

[3] European Commission, *Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen*, COM(2009) 262 final, Brussels, 10.06.2009, pp. 7-8.

yielding a number of information systems and instruments of varying size, scope and purpose".[4] Some of these instruments are directed towards the acceleration of intra-EU data flows, while others facilitate data transfers from the EU to third countries. The pressure by the US to multiply, enhance and speed up such data flows has been continual since 2001. Sometimes it has focused on the establishment of new EU–US personal data streams, whereas in other cases it has favoured the development of EU practices or information systems indirectly facilitating access by US authorities to data originating in the Union.

By supporting the creation of large-scale databases with specific technical requirements that favour the interconnection of sources, EU institutions have contributed to the establishment of an infrastructure that facilitates, and de facto appears to attract, continually reinforced data-processing practices.

Second, ensuring the protection of personal data in the AFSJ has also been rendered particularly difficult by the existence and progressive growth in the AFSJ of security agencies that present a predominantly 'home affairs' orientation and have as their main activity the processing of personal data. Among these are EUROPOL (the European Police College), EUROJUST, FRONTEX (the EU Border Agency) and the upcoming European agency for the operational management of large-scale IT systems. This is particularly the case of EUROPOL, which is a support service for the law enforcement agencies of the EU Member States and has no executive powers. The support provided to Member States primarily consists of ensuring rapid information exchange and providing national authorities with sophisticated intelligence analysis. Its role is to gather, analyse and redistribute data. To carry out its functions, EUROPOL has been extremely interested in accessing various sources of data related to individuals, including data stored in databases created for purposes unrelated to law enforcement or managed by other EU agencies. Although its core activity entails assisting the authorities of Member States, it also transfers information to the authorities of third countries, such as the US.

The relations and cooperation between these EU home affairs agencies, as well as with national authorities and third-country actors, have resulted in a complex, de-centralised reticulation of data flows where the protection of personal data is outstandingly hard to track and implement.

Third, the heterogeneous legal framework for the protection of personal data in the AFSJ offers only limited defence against encroachments and actual and potential threats to this right. The lack of uniformity of the legal framework essentially stems from the period when the EU was structured around 'pillars', when the AFSJ used to include areas falling under both the first pillar (former Title IV of the Treaty establishing the European Community, TEC) and the third pillar (corresponding to 'police and judicial cooperation in criminal matters' under the former Title VI of the Treaty on the European Union, TEU). Data protection in the first pillar was generally governed by the Data Protection Directive (95/46/EC) (DPD),[5] providing some relatively well-established norms and procedures for the protection of personal data. This Directive, however, did not apply to the third pillar (police and judicial cooperation in criminal matters), which therefore lacked a generally applicable, horizontal legal instrument. For many years, personal data protection in this policy field was governed exclusively by disparate provisions adopted on an ad-hoc basis coinciding with the creation of different mechanisms for data processing (for instance,

[4] European Commission, *Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice,* COM(2010) 385 final, Brussels, 20.7.2010, p. 3.

[5] Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50.

large-scale databases like the Schengen Information System (SIS),[6] or instruments dependent on national databases, such as the Prüm Decision)[7] or coinciding with the establishment of EU home affairs agencies processing personal data (such as EUROPOL and FRONTEX).

Additionally, the increasing use for security purposes of data originally collected by private parties for other uses (for example, the processing of financial data in the name of counterterrorism) generated much doubtfulness as to which legal framework was applicable (as illustrated, for instance, by the judgements of the Court of Justice of the European Union (CJEU) for the passenger name record (PNR) case and regarding the legal basis of the Data Retention Directive (DRD)).[8] The dividing line between contrasting data protection regimes was recurrently challenged, and appeared in any case to be discretionary. Overall, data protection in the AFSJ resulted in a diverse and fragile patchwork that contrasted with the powerful and uninterrupted support of personal data processing in the field.

Some of these factors (mainly the constant push towards enhanced data processing practices in the AFSJ, and the deficiencies of applicable data protection, especially concerning European cooperation in police and criminal justice) are certainly not unrelated to the limited powers traditionally granted to the EP in this area, and more concretely, in what was formerly known as the third pillar. Over the course of many years, the EP criticised the persistence of the intergovernmental method for decision-making in the field, notably because it prevented the EP from exercising any effective democratic scrutiny. As some policy areas were eventually moved from the third to the first pillar, the EP also started to prioritise other objectives, such as the enhancement of fundamental rights in the area.

The EP's efforts to reinforce the protection of personal data in the third pillar have been particularly striking during the last decade. It has again and again called for the establishment of uniform data protection rules across the third pillar, to provide equivalent standards to those of Directive 95/46/EC.[9] The Council addressed the question intermittently from 1998 onwards, only to adopt at the end of 2008 a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[10] with a remarkably limited scope and establishing only minimum harmonisation of data protection standards. The European Commission has for many years manifested that in its view the data protection principles of Directive 95/46/EC are suitable to be applied in the context of the third pillar as well, and has been overtly critical of the Framework Decision.[11]

---

[6] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, p. 19.

[7] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1; Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 12.

[8] Judgement of the Court (Grand Chamber) of 30 May 2006, Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union*; and Judgement of the Court (Grand Chamber) of 10 February 2009, Case C-301/06, *Ireland v. European Parliament and Council of the European Union.*

[9] See Resolutions of March 27, 2003, and March 9, 2004.

[10] Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

[11] European Commission, *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, 4.11.2010, Brussels, pp. 13-14.

1.2. The new institutional and legal context

The attention given to the protection of personal data by the Stockholm programme contrasts with its absence in the strategic EU policy agendas and guidelines that were provided for previous periods. It needs to be envisaged in the context of the entry into force in December 2009 of the Lisbon Treaty.[12] Indeed, the Lisbon Treaty has already had major consequences for the status of personal data protection in the EU and is also to have significant implications for legislative developments in the area.

The recent focus on enhancing EU data protection is to be of the foremost importance as the Internal Security Strategy adopted in March 2010 by the European Council[13] confirms the persistent support for incessantly strengthened, data processing practices. Under the motto of "prevention and anticipation: a proactive, intelligence-led approach", the Internal Security Strategy asserts that it is necessary to develop and improve "prevention mechanisms", such as the systematic processing of data on all individuals travelling by air to and from the EU, for the purposes of the fight against terrorism and serious crime.[14] It also aims at establishing a "comprehensive model for information exchange" for the AFSJ "culminating in the principle of information availability".[15]

1.2.1. The Lisbon Treaty and EU data protection: Innovations and exceptions

The entry into force of the Lisbon Treaty has brought about major innovations relevant for EU data protection, although the Treaty also foresees some exceptions and complimentary provisions that might mitigate the expected impact of such innovations:

- the collapse of the pillar structure of the EU. The pillar structure introduced by the Maastricht Treaty has formally disappeared under a sole Title V called the "Area of Freedom, Security and Justice" (Articles 67-89) in the Treaty on the Functioning of the European Union (TFEU). This enables the adoption of a legal instrument for data protection covering the areas that used to fall under the first and third pillars. *Nevertheless*, the area formerly falling under the second pillar, the Common Foreign and Security Policy (CFSP), remains subject to special rules and specific procedures.[16] Furthermore, the Republic of Ireland and the UK benefit from a complex set of 'opt-out/opt-in' provisions annexed under various protocols that could hinder the general homogeneity of the AFSJ;[17]
- the inclusion of a new legal basis for personal data protection in the Treaties. Article 16 TFEU, in its first paragraph, asserts that "[e]veryone has the right to the protection of personal data concerning them". In its second paragraph,[18] it introduces a new legal basis that refers to the need to regulate the protection of personal data within the entire scope of EU law and can thus be used (and arguably, must be used) for the adoption of a 'comprehensive' data protection instrument,

[12] The Treaty of Lisbon was signed on 13 December 2007 by the 27 Heads of State or Government of the Member States of the Union. It amended the Treaty on European Union (TEU) and the former Treaty establishing the European Community, now known as the Treaty on the Functioning of the European Union (TFEU).

[13] European Council, *Internal Security Strategy for the European Union: Towards a European security model,* adopted by the Justice and Home Affairs Council on 25 and 26 February 2010, and approved by the European Council on 25 and 26 March 2010.

[14] *Idem,* p. 22.

[15] *Idem,* p. 24.

[16] Under Title V of the EU Treaty (Article 24 TEU).

[17] See notably Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice; on the implications for data protection, see in particular its Art. 6(a) of said Protocol, on the non-applicability of Art. 16 TFEU to both Member States when they do not participate in activities that would require its application. See also Protocol (No 22) on the position of Denmark.

[18] The second paragraph replaces Article 286 EC.

rendered possible by the end of the pillar structure. Article 16 TFEU is therefore to become the central element of EU data protection. *Yet, notably*, Article 16(2) TFEU includes a reference to Article 39 TEU, which establishes that for the processing of personal data by Member States in the area covered by the CFSP, the Council shall adopt specific rules for data protection, thus excluding the EP from co-legislating on data protection in this field. Furthermore, two Declarations annexed to the Final Act of the Intergovernmental Conference that adopted the Treaty of Lisbon, signed on 13 December 2007, nuance the possible impact of Article 16 TFEU. Declaration 20 recalls that where the regulation of personal data protection could have an impact on national security, due account must be taken of the specific characteristics of the matter.[19] Declaration 21 underlines that in the fields of judicial cooperation in criminal matters and police cooperation, specific rules on the protection of personal data "may prove necessary because of the specific nature of these fields";[20]

- the binding force granted to the Charter of Fundamental Rights of the EU (EU Charter). Proclaimed in 2000,[21] the EU Charter, as amended in 2007, now has the same legal value as the Treaties.[22] Its provisions address all EU institutions, bodies, offices and agencies, as well as Member States when they are implementing EU law. Respect for the fundamental rights enshrined in the EU Charter, such as the (well-established) right to respect for private life, recognised in Article 7, and the (innovative) right to the protection of personal data, acknowledged in Article 8, is thus now a legal requirement. The CJEU can declare invalid a provision of EU legislation that does not comply with them.[23] *That notwithstanding*, there are some uncertainties regarding the legal status of the EU Charter for the UK, Poland and the Czech Republic, for which Protocol No. 30 of the TFEU is applicable.[24] It is not clear whether this Protocol constitutes for these Member States an opt-out from the Charter or an interpretative tool of unsettled effects;
- the accession to the European Convention on Human Rights (ECHR), based on Article 6(2) of the TEU. For the moment, the ECHR is one of the sources from which the CJEU deduces fundamental rights as general principles of the Union's law.[25] It is eventually to become directly binding on EU institutions. *Still*, this will be so only when the EU's process of accession, which is already underway, has been finalised; and
- the extended jurisdiction of the CJEU. The CJEU has acquired general jurisdiction to give preliminary rulings in the AFSJ, and thus regarding police and judicial cooperation in criminal matters. This improvement in judicial protection implies that any court or tribunal is able to request a preliminary ruling from the CJEU on issues concerning this domain. *Even so*, transitional provisions provide that the full jurisdiction of the CJEU, and in particular the inclusion in its scope of police and

[19] Declaration 20 on Article 16 of the TFEU.

[20] Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

[21] The EU Charter was adopted by the three central EU institutions (Parliament, Council and Commission) in Nice on 7 December 2000.

[22] Art. 6(1) TEU.

[23] European Commission, *Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments*, Commission Staff Working Paper, SEC(2011) 567 final, Brussels, 6.5.2011, p. 4.

[24] Protocol No. 30 annexed to the TFEU on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom; it was later agreed to extend this derogation also the Czech Republic, although the Protocol is still to be amended (in principle, coinciding with the next accession to the EU).

[25] Article 6(3) TEU.

judicial cooperation in criminal matters, will not apply until the end of 2014.[26] Furthermore, the UK may choose whether to accept the full jurisdiction even after the transitional period.[27]

These elements could mark the beginning of a new era for EU data protection, at least as soon as the transitional periods are over. But the entry into force of the Lisbon Treaty has resulted other important institutional changes as well.

1.2.2. The Lisbon Treaty, the EP and EU data protection

The Lisbon Treaty has directly or indirectly affected the powers of the EP. The changes could have an impact on the new legal framework for data protection, as well as on the everyday assurance of data protection in the deployment of EU policies in the AFSJ, more specifically through two developments:

- the generalisation of the legislative procedure formerly known as 'co-decision'. The EP is now in general terms at equal level with the Council in processing EU law, thanks to a new 'ordinary legislative procedure',[28] which also applied in the former third pillar. There are nonetheless a few exceptions to the general application of the ordinary legislative procedure. In specific instances, such as operational cooperation between the law enforcement authorities,[29] or in matters related to passports, identity cards, residence permits or "any other such document",[30] special legislative procedures apply. In such cases the Council can adopt measures by acting unanimously, and the EP is relegated to having a merely consultative role. Additionally, during the legislative process, Member States might opt to take steps through the 'enhanced cooperation' procedure; and
- the strengthened role of the EP in relation to international agreements. Under a new 'consent' procedure established by Article 218 TFEU, the EP's consent is needed for international agreements in all fields where the ordinary legislative procedure applies. Furthermore, under Articles 300(6) and 218(11) TFEU, the EP has the power to require the CJEU to provide an opinion on the compatibility of international agreements.

Finally, the EP is also to take part in the encouraged inter-parliamentary cooperation with national parliaments.

1.2.3. The Lisbon Treaty, national parliaments and the AFSJ

The Lisbon Treaty introduced various provisions intended to encourage greater involvement of national parliaments in EU policy-making. Some of them are particularly relevant for the AFSJ. National parliaments are to contribute actively to the good functioning of the EU in several ways:

- by receiving from the European Commission any draft legislative act and verifying its compliance with the principle of subsidiarity, according to which action at the EU level should be taken only when the objectives envisaged cannot be achieved at the national or local level. If a minimum number of national parliaments raise objections on the issue of conformity with the subsidiarity principle, the proposal must be re-examined;

[26] Article 10(1) of Protocol No 36 on Transitional Provisions, which also specifies that during the transitional period the European Commission will not be able to make use of its new powers to initiate infringement procedures and take legal action against Member States for failing to fulfil their obligations in this field.

[27] Article 10(4) of Protocol No 36 on Transitional Provisions.

[28] Article 289 TFEU.

[29] Article 87 TFEU.

[30] Article 77(3) TFEU.

- by taking part in evaluating the implementation of EU policy in the AFSJ;
- by being involved in the political monitoring of EUROPOL and the evaluation of EUROJUST's activities, under the conditions to be determined by relevant regulations adopted by the Council and the EP; and
- by taking part in inter-parliamentary cooperation with the EP.

The potential relevance of the enhanced involvement of national parliaments relies notably on the fact that Member States share with the EU crucial obligations in the field of the implementation and enforcement of fundamental rights.[31] Aware of their political responsibilities in exercising their respective powers in the legislative process, they have already been working with the EP on the creation of a network of European expertise relating to the monitoring of intelligence services (ENNIR – European Network of National Intelligence Reviewers) aimed at improving democratic control of the functioning of these services.[32] Reinforced cooperation between the EP and national parliaments is likewise being developed in relation to EUROPOL.[33]

In the area of the EU protection of personal data, the involvement of national parliaments has until now still been of limited significance – compared, for instance, with the impact of decisions of national constitutional courts, which have been sending critical messages to EU institutions about the compatibility of some security policies and the protection of fundamental rights in the EU.[34]

1.3. Data protection and privacy

To allow for a considered reflection on data protection, privacy, transparency, accountability and the policies that surround them in the EU, some conceptual clarifications are necessary.

1.3.1. Data protection and privacy

The term 'data protection' is generally recognised as designating the protection of 'personal data', this notion being understood not as 'private' or 'intimate' data, but in the sense of 'data that can be referred to a specific person', and thus can include publicly available data. Since the beginning of the 1970s, data protection laws across Europe have been regulating who is allowed to access personal data, what can this data be used for, how it must be stored, and for how long. In the current EU legal framework, personal data protection as a legal concept refers to a series of subjective rights granted to those whose personal data is processed, a number of obligations imposed on those who process personal data and the compulsory existence of a supervisory authority to monitor compliance with these rules.

The meaning of the word 'privacy' is less straightforward. The 'right to privacy' originally emerged as a legal concept at the end of the 19th century. It was understood at the time mainly as the right to be left alone or to be protected against external interferences. In

[31] European Parliament, *Resolution of 15 December 2010 on the situation of fundamental rights in the European Union– effective implementation after the entry into force of the Treaty of Lisbon, 15 December, Strasbourg*, P7_TA(2010)0483, § 36. A tool for increase exchange of information between parliaments is the IPEX database (available at: http://www.ipex.eu).

[32] See, notably, the Declaration of Brussels, adopted on 1 October 2010 by the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the Member States of the European Union, and Conference of the Speakers of the Parliaments of the EU, *Presidency Conclusions,* Brussels, 4-5 April 2011.

[33] See, for example, European Commission, *Communication from the Commission to the European Parliament and the Council on the procedures for the scrutiny of EUROPOL's activities by the European Parliament, together with national Parliaments*, COM(2010) 776, Brussels, 17.12.2010.

[34] In this sense, see European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM(2011) 225, Brussels, 18.4.2011.

Europe, the right to privacy acquired special relevance after the Second World War, often encompassing by then more much than a mere right to seclusion, and sometimes covering, as an umbrella right, other rights such as the right to confidentiality of communications. By the 1970s, in many English-speaking countries and especially in the US, it became common to use 'privacy' as an abridged version of the expression 'informational privacy', which refers to a series of information practices and control prerogatives on the use of information related to individuals that actually shares many features with the EU notion of personal data protection.

Nowadays, the EU legislator commonly uses the expression 'right to privacy' to refer to the right established in Article 8 of the ECHR. This can lead to some confusion given that Article 8 of the ECHR does not mention privacy at all, but recognises a right to respect for private life. The European Court of Human Rights (ECtHR) has actually consistently refused to use the word 'privacy' in relation to this Article. It has also repeatedly underlined that 'private life' is a wide notion, and that it cannot be defined exhaustively. The 'right to respect for private life' concerns a sphere within which everyone can freely pursue the development of his/her personality, which integrates the relations of individuals with other persons and with the outside world. Under this broad notion, the Strasbourg Court has included the protection of individuals against the processing of data related to them. In short, in EU law 'privacy' is (in principle) a broad notion that includes in its scope the protection of personal data, at least partially (insofar as the ECtHR considers that a particular data processing practice constitutes an interference with the 'right to respect for private life', an assessment that is dependent on the nature of the data and the circumstances of its storage, and which might result in ensuring protection of only part of the data falling under the category of 'personal data' as recognised by EU law).[35]

The EU Charter mirrors Article 8 of the ECHR in two separate provisions. One of these is Article 7, which merely replicates it. The other is Article 8 on the protection of personal data, which reflects the content of Article 8 of the ECHR insofar as the protection of the individual against data processing is concerned, and in addition incorporates some data protection elements from primary and secondary EU law, thus audaciously configuring EU personal data protection as a new fundamental right of the EU.

The exact legal implications derived from this approach are yet to be determined. From its proclamation in 2000 until December 2009, the EU Charter had a peculiar legal status. During that period, the CJEU did not really enter into the discussion of the possible existence of a fundamental right for the protection of personal data and of its eventual effects. When dealing with EU data protection, it preferred to reaffirm its link with Article 8 of the ECHR. The EU legislator, as if unsure of the boundaries between privacy and data protection, has since 2000 systematically mentioned both in EU legal instruments regulating data protection.

The wording of the EU Charter's Article 8 on the protection of personal data mentions as possible grounds for legitimising the processing of data related to individuals "the consent of the person concerned" and any "other legitimate basis laid down by law". As a general rule, in the AFSJ data processing is legitimated on the grounds of the latter type, i.e. on a basis laid down by law – the existence of consent or the lack of consent of the person concerned being thus irrelevant in this context. Nevertheless, the increased tendency to process for security purposes personal data originally collected for other purposes (purpose

[35] The ECtHR has repeatedly emphasised over the years that the broad notion of the right to respect for private life as established in its case-law in reference to Article 8 of the ECHR corresponds to the scope of application of the Council of Europe's legal instrument on the protection of personal data, Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 (known as 'Convention 108'). Nevertheless, the scope of application of Convention 108 is limited to *automated* processing of data, contrary to the EU fundamental right to the protection of personal data, which concerns *any* processing of 'personal data'. Thus, the extent to which the broad notion of right to respect for private life as recognised by the Strasbourg case-law matches the protection granted by EU data protection is still to be clarified.

(un)limitation or 'function creep'), and often gathered by private companies on the basis of the consent of the person concerned, can render the validity of such initial consent particularly problematic.

1.3.2. Transparency

The term 'transparency' has multiple connotations. It can paradoxically refer to both a principle of the EU that personal data protection needs to be balanced against, and to a principle that data protection needs to enforce.

The principle of transparency, as a general principle of the EU legal order,[36] enables EU citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and accountable to the citizen in a democratic system. It is linked with the principles of civic participation and good administration.

The CJEU has already dealt with some cases of tension between the principle of transparency and the protection of personal data.[37] In the judgement in *Shecke and Eifert*,[38] it underlined the obligation of the EU legislator to strike a balance between the EU's interest in guaranteeing the transparency of its acts, on the one hand, and the fundamental rights enshrined in Articles 7 and 8 of the EU Charter, on the other.[39]

The European Ombudsman, who investigates complaints about maladministration in the EU institutions and bodies, has regularly warned against the possible "threat to openness" represented by personal data protection, and especially by the failure to recognise its limits.[40] The European Data Protection Supervisor (EDPS), the independent authority responsible for monitoring compliance with personal data protection by EU institutions and bodies, has been working in close cooperation with the European Ombudsman. For many years the EDPS has supported an understanding of the relationship between access to EU public documents and personal data protection that tended to favour the former to the detriment of the latter. This approach, however, was dismissed by the CJEU, leading to a re-positioning of the EDPS on the subject.[41]

A major obstacle to the transparency of public decision-making is secrecy grounded on security concerns. This is particularly relevant in the AFSJ and more concretely regarding the development of EU security policies, given that national and EU 'security concerns' tend to be blurred and amalgamated as grounds for refusal of access to public documents, be it in relation to EU internal or external security policies (including in the context of international negotiations). Recently, the EP has been noticeably vocal in requesting enhanced transparency in the EU funding of security research.[42]

But transparency has other connotations as well. It can refer to one of the principles that, in accordance with the case law of the ECtHR, must be ensured by any limitation to the

[36] Articles 1 and 10 TEU and Article 15 TFEU.

[37] See for instance, Court of Justice of the European Union, Case C-28/08 P, *Commission v. Bavarian Lager*, 29 June 2010.

[38] Court of Justice of the European Union, C-92/09 and C-93/09, *Volker und Markus Schecke* and *Eifert*, 9 November 2010.

[39] § 80.

[40] See, for instance, European Ombudsman, *Note on Openness and Data Protection,* Strasbourg, 14 November 2001.

[41] In this sense, see European Data Protection Supervisor, *Public access to documents containing personal data after the Bavarian Lager ruling*, Brussels, 24 March 2011.

[42] In particular, in reference to research funded through the 7th Framework Programme for Research (FP7), in a non-legislative Resolution the EP called on the European Commission to increase the transparency of a project concerned with surveillance technologies (European Parliament Resolution of 8 June 2011 on the mid-term review of the Seventh Framework Programme of the European Union for research, technological development and demonstration activities (2011/2043(INI)), P7_TA(2011)0256, § 27).

right of Article 8 of the ECHR. By virtue of the principles of predictability and transparency, indeed, any such limitation must imperatively be provided by law, which must be clear and accessible to everyone.

The term 'transparency' is often used in the data protection field with additional meanings. In this context, transparency is envisaged as a requirement applying to the way in which personal data are collected and the purposes for which they are processed,[43] as well as a condition for rendering consent valid.[44] Although not yet formally recognised as a general principle of data protection, according to the EDPS transparency is already implicitly an integral part of the present legal framework on data protection.[45] The possibility to include in EU law some transparency mechanisms is increasingly being considered and is studied in detail in chapter 4 of this study.

1.3.3. Accountability

'Accountability' is another term that has both generally well-known meanings and a specific use in data protection jargon.

Accountability, as in 'political' or 'democratic accountability', can be regarded as inherently linked to transparency, which reinforces it. The above-mentioned Internal Security Strategy alludes to both transparency and accountability in security policies as notions that ensure they are "easily understood by citizens" and that they "take account of their concerns and opinions".[46] But they can also imply more than that.

Accountability has traditionally been one of the major challenges of EU integration. For many years, the AFSJ was identified as one of the areas with a major accountability deficit, especially owing to the restricted role played by the EP in third-pillar decision-making. The 'Lisbonisation' of the field is to contribute to solving this problem.[47]

Accountability in the AFSJ, however, still has other challenges to overcome, in particular as the proliferation of agencies and specific bodies seem to diffuse decision-making and enforcement related to EU security policies and border control management in a series of opaque practices. Despite the institutional changes introduced by the Lisbon Treaty, which moved AFSJ agencies under the scope of 'ordinary' EU law and methods of cooperation, there is still progress to be made regarding their different activities. In this sense, the EP has called on the EU to ensure the full legal accountability of its agencies with respect to their commitment to the protection of fundamental rights and to integrate a fundamental-rights approach into all their activities.[48]

A closely related, but allegedly different issue is the question of ensuring the 'accountability' of personal data processing by these agencies, and more specifically, the supervision of their data processing practices. The right to the protection of personal data includes as a core component the need for independent monitoring, i.e. by an independent authority. Arrangements for supervision in the AFSJ have traditionally been complex, involving the multiple national agencies for data protection along with different bodies constituted by representatives of such agencies, as well as the EDPS. The body that

[43] See, for instance, Committee of Experts on New Media (MC-NM), *Draft Recommendation on the protection of human rights with regard to search engines*, Strasbourg, 11 March 2010.

[44] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP187, Brussels, 13 July 2011, p. 9.

[45] European Data protection Supervisor, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union",* Brussels, 14 January 2011, § 73.

[46] European Council, *Internal Security Strategy for the European Union*, 2010, p. 19.

[47] European Parliament, *Resolution of 15 December 2010 on the situation of fundamental rights in the European Union*, § 23.

[48] European Parliament, ibid., § 34.

coordinates national data protection authorities (DPAs) at the highest EU level, the Article 29 Data Protection Working Party (WP29), was created as a first-pillar body and thus excluded from playing its coordinating and consultative role for a large part of the AFSJ. These arrangements have sometimes been described as not fully operational by the authorities involved. Furthermore, the 'accountability' of these authorities can also be discussed.

The EP has underlined that to ensure accountability on matters related to fundamental rights in the AFSJ, there is a need to develop more effective inter-institutional cooperation. The EP has also pointed out that, in general, the assurance of fundamental rights in the EU is dependent on its role in evaluating the work of other EU institutions. In addition, it has underscored the importance of its right, enshrined in Article 218(10) TFEU, to be immediately and fully informed at all stages of the procedure for concluding international agreements between the Union and third countries or international organisations.[49]

'Judicial accountability' is also a crucial concern for EU institutions. The EP has called for the deployment of "effective accountability mechanisms", at both the national and EU levels, to address human rights violations.[50] Until the entry into force of the Lisbon Treaty, measures falling under the scope of the third pillar, despite their major potential implications for the safeguarding of fundamental rights, enjoyed a restrained level of judicial accountability. This was perceived as a major problem and was one of the elements motivating various attempts to regulate measures implying the processing of personal data, preferably through first-pillar legislation, especially in those cases where due to the complex nature of the processing, the question of its exact nature was unclear or debatable. The Lisbon Treaty has represented a significant step forward in this area, by establishing that every individual has a right to the protection of personal data that can be invoked through the courts.

In the data protection field, accountability is a term increasingly used with distinct connotations, although its exact meaning is contested. In this field, the notion has already been discussed for a few decades.[51] The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980 by the Organisation for Economic Co-operation and Development (OECD) (1980) used the term in the sense of allocating liability for compliance with data protection rules, but nowadays it tends to be predominantly envisaged as an alternative to some requirements for compliance with rules.[52] The WP29, which has been advocating the recognition of accountability as a statutory principle in the future legal framework for EU data protection, describes it as a principle that would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of EU data protection law and demonstrate this on request.[53] (For a detailed discussion on accountability as an element of data protection law, see chapter 4.)

A crucial concern regarding transparency and accountability in EU decision-making is their relation to contemporary transformations of policing. These transformations are being triggered by the deployment of new surveillance practices that make use of available information and communication technologies to assess risks and probabilities associated with persons or groups, based on data volunteered by individuals or inferred from other available data. These practices are marked by an attraction to logics of 'prevention', not

[49] European Parliament, ibid., § 29.

[50] European Parliament, ibid., § 1.

[51] See, for instance, Flaherty, David H., "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies ", *Science, Technology & Human Values,* 11(1), 1986, pp. 7-18.

[52] Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L., Lloyd, I. and Saxby, S., "30 years on - The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Report,* 27, 2011, p. 227.

[53] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, Brussels, 13 July 2010, p. 3.

only of crime and threats to public order, but also of any other undesired activities. They are typically preventive, proactive and 'intelligence-led', and involve the processing of vast amounts of personal data, sometimes obtained through intrusive means of data collection, and intensified participation of the private sector. These modern manifestations of policing, as addressed in chapter 2, pose profound challenges to data protection. They are also characterised by their transborder nature, as international cooperation, now routinely taking the form of data exchanges, plays an increasingly important role in policing strategies.

1.4. Scope, key issues and questions

This study looks at the protection of personal data in the AFSJ, and explores data protection and privacy along with their relation to the development of EU security policies and data processing practices in the context of law enforcement. As data protection is a horizontal issue that is relevant in many areas of EU law, not all EU issues for which data protection is a concern are examined. The study notably does not address data protection and privacy in the telecommunications sector, except where relevant to illustrate some tensions derived from the 'pillar era' in the AFSJ. In particular, the study does not cover complexities provoked by the use for law enforcement purposes of data originally collected by private parties for strictly commercial reasons (for instance, introducing debates on the DRD). Another subject not directly addressed, but which needs to be mentioned as an element of the background against which the protection of privacy and personal data are to be ensured in the EU, is the pressure to resort to the systematic monitoring of communications of the entire EU population in the name of policy objectives other than security, such as the protection of intellectual property rights.

This study centres on the current EU policy discussions on the upcoming European legal framework for personal data protection, which were launched in the spring of 2009 by the European Commission, with a public consultation. The European Commission is expected to introduce to the EP and the Council a proposal modifying this framework, or a series of legislative proposals, by the end of 2011. The review process should be over before the end of the current mandates of the both EP and the European Commission.

The new EU process for amending data protection is ambitious in its nature and goals. One of the main challenges in this area will be to design a legal framework for personal data protection that will have a real impact on the deployment and further development of data processing practices in the AFSJ. A central concern is to devise effective policy strategies and common legal principles ensuring the practical and genuine provision of data protection and privacy at times of addressing the contemporary challenges in data protection affecting AFSJ policies on data processing. From this perspective, a number of crosscutting issues have crucial relevance from the outset of this study:

- **The Lisbon Treaty, by giving legally binding force to the EU Charter, has modified the obligations of EU institutions in terms of personal data protection.** The recognition of the protection of personal data as an autonomous fundamental right in Article 8 in the now legally binding EU Charter confers on it an unprecedented legal status. The EU Charter does not establish the protection of personal data as an absolute right: public authorities may take measures that interfere with such a right under certain conditions. These requirements, set out in Article 52, notably establish that any limitation of the right to personal data protection must be provided for by law and respect its essence, and that, subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others. These constraints are similar to the conditions imposed by Article 8(2) of the ECHR to any interference with the right to privacy, but are not exactly the same. They are in a sense less protective, as they allow for interferences in the name of any "general interest recognised by the Union", which can include, for instance, the principle of transparency. But they are also more safeguarding, as under Article 52 the core content of the fundamental

right to the protection of personal data (a right that did not exist as such in the ECHR) must in all cases be guaranteed.

In the light of this analysis, two questions must be addressed:

- Which common basic principles and legal elements need to be established in the new EU legal framework on personal data protection to guarantee full compliance with its fundamental rights dimension?
- What is needed to ensure that the core essence of the EU fundamental right to the protection of personal data is in all cases guaranteed?

- **The data protection obligations derived from Article 8 of the EU Charter do not replace the necessity of additionally complying with all the requirements imposed by Article 8 of the ECHR and its relevant case law.** The fact that the EU Charter has acquired legally binding force does not imply that the fundamental rights requirements derived from the ECHR are to be put aside. On the contrary, the forthcoming accession of the EU to the ECHR confirms the unquestionable necessity of taking them fully into account. Article 8 of the ECHR can apply to the processing of data related to individuals, and when it does, it imposes a series of obligations that are listed in Article 8(2). Among the obligations is that of imperatively pursuing these interests: national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others. The case law of the ECtHR provides extensive guidance on when measures that interfere with the right to privacy amount to a violation of such a right.

  From this perspective, the key questions that must be examined are the following:

  - How can it be ensured that the increased significance of the right to the protection of personal data in EU law does not displace the need to take into account the requirements imposed by the ECHR, and in particular Article 8?
  - How can it be ensured that the core essence of the EU's fundamental right to privacy, as recognised by Article 7 of the EU Charter, is in all cases guaranteed?

- **The privacy and data protection requirements derived from the EU Charter and the ECHR apply across all fields, including security policies.** The fact that Member States can, under certain strict conditions, approve certain interferences with such rights in the name of security does not mean that the fundamental rights to privacy and to personal data protection are not already fully applicable in the AFSJ. The debate on whether the existing legal instruments (such as the DPD) should be amended to ensure their applicability to all data processing taking place in this area is a different issue, which refers to the concrete scope of applicability of each instrument. Therefore, policy discussions do not currently concern whether the protection of personal data should be *extended* to the ex-third pillar, as data protection is already granted across the ex-first and third pillars as a fundamental right.

  Rather, the pivotal issues now are how should such protection be translated into clear legal instruments, and perhaps most importantly, how any interferences with personal data protection adopted in the name of security should be regulated and the data protection challenges be effectively addressed in practice – and with which degree of homogenisation or 'uniformity' across the EU and its decision-making processes. Taking into account the principle of subsidiarity and the relevant provisions of the Treaties, the EU has a limited competence on the regulation of security. On the one hand, it shall aim at ensuring a high level of security, notably by adopting measures to prevent and combat crime, and for the coordination and cooperation between police and judicial authorities.[54] On the other hand, this is not

[54] Article 67(3) TFEU.

to affect the fact that safeguarding 'internal security' remains under the remit of the national level.[55] The Lisbon Treaty might represent a step towards more homogeneity in some aspects of EU law, but paths to be potentially followed by Member States in search of more 'flexibility' or 'variable geometry' through enhanced cooperation also exist, and the innovations introduced are in any case to operate against the particular background of the current EU security field.

In this context, there are several key questions:

- How should (EU/internal) security modulate the EU's future legal framework on data protection?
- What role should Member States have in the articulation of the security/data protection relationship, and how does it affect the degree of protection effectively granted?
- Is increased 'uniformity' both desirable and possible as a policy and legal option in the EU's current AFSJ landscape?
- How does the relationship between (EU/internal) security and the EU's legal framework for data protection impact upon the role of the EP as a protector of EU fundamental rights?

- **The upcoming EU DPF needs to be designed in a way that ensures it addresses current challenges and has an impact on future security measures and practices in the AFSJ.** There are a number of specific policy dilemmas pertaining to data protection as a consequence of the increasing personal data processing in EU AFSJ policies, and the shift towards dataveillance, proactivity and profiling. One of the main issues for data protection in the AFSJ concerns how to have a real impact on the continuous reinvigoration of 'data processing by default' and its architecture in the AFSJ, including the increasing role (and inter-agency cooperation) of EU home affairs agencies, such as EUROPOL, EUROJUST and FRONTEX, as 'data controllers'. The 2009 Stockholm programme gives attention to privacy and data protection, but unfortunately tends to portray them not as rights that might preclude the adoption of massive data processing measures, but rather as requirements to be complied with as much as possible when such data processing measures are deployed.[56]

  From this perspective, the following questions are important:

  - What are the main challenges stemming from the increasing deployment of security technologies and processing of personal data for law enforcement purposes in the EU AFSJ policies?
  - How can it be guaranteed that the legislative development of the right to privacy and personal data protection does not transform these rights into mere enablers of data processing practices?

- **To have an appropriate impact in the AFSJ, data protection needs to become relevant at *all stages* of policy-making.** This means notably (yet not only) *at the initial stages* of the procedure leading to the adoption of legislation and other acts. The European Commission has publicly underlined this need by referring to the judgement of the CJEU of 9 November 2010. In this judgement, the Court criticised particularly the Council and the European Commission for having failed to ascertain *ahead of adopting contested provisions* whether in light of the fundamental rights protected by the EU Charter the chosen measure did not go beyond what was necessary for achieving the legitimate policy objective pursued.[57] In this sense, the

[55] Articles 72 and 73 TFEU.

[56] "The Union must address the necessity for increased exchange of personal data whilst ensuring the utmost respect for the protection of privacy", European Council (2010), op. cit., p. 10.

[57] § 81 and § 83.

EP has already been considering ways to strengthen its autonomous impact assessment on fundamental rights in relation to legislative proposals and amendments under examination in the legislative process. These include enlarging the possibilities currently foreseen by Rule 36 of the EP's Rules of Procedure on the respect for the EU Charter and asking the Legal Service for opinions on legal issues related to fundamental rights in the EU.[58] But data protection issues can also emerge and require attention *at later stages* of the policy process. For instance, they may arise owing to the unsatisfactory implementation of the agreed measures or as a consequence of subsequent changes introduced to the original legislative proposals during the decision-making processes, some of which might be of a fundamental nature and affect data protection and privacy (e.g. SIS II).

From this viewpoint, it is crucial to ask these questions:

- Which particular mechanisms can the EP rely upon to ensure that data protection concerns are duly taken into account during the full duration of the policy process, ranging from the initial discussions leading to the adoption of security measures to the eventual evaluation of their implementation?
- What actions can be undertaken if evidence indicates that the implementation of international agreements, EU legal instruments or other concrete initiatives in practice constitutes infringements of any EU fundamental right?

- **For data protection to be fully relevant at all stages of policy-making in the AFSJ, accountability, openness and transparency issues need to be prioritised in the security-related context.** It is not enough to ensure that the major EU institutions take duly into account the protection of personal data in their respective institutional roles. All actors involved in the processing of personal data in the AFSJ must contribute to ensuring that data processing practices remain accessible and predictable, and that they can be subject to a full evaluation and scrutiny of their proportionality. This applies especially to agencies whose data processing practices have important effects on fundamental rights, such as EUROPOL, EUROJUST and FRONTEX. They must not only comply with the letter of EU data protection law, particularly in terms of independent supervision, but also ensure levels of accountability (including legal accountability and access to justice) and transparency that allow for a full fundamental rights assessment of their practices insofar as the processing of data related to individuals is concerned.

  In this sense, the key question that arises is the following one:

  - How should accountability, openness and transparency be improved in the AFSJ to contribute to the fundamental rights compliance of personal data processing practices?

This study explores these questions by giving particular attention to the EP's contribution to privacy and data protection in the pre-Lisbon EU, and its efforts to reinforce their assurance across the EU. Ultimately, it aims at identifying what role the EP can and should play in current and upcoming developments in the framework of a renewed EU DPF in the AFSJ.

[58] European Parliament, *Resolution of 15 December 2010 on the situation of fundamental rights in the European Union,* § 25.

2. CHALLENGES POSED BY THE INCREASING USE OF TECHNOLOGY FOR LAW-ENFORCEMENT AND INTER-AGENCY COOPERATION

KEY FINDINGS

- The main debate for the upcoming DPF regarding the field of law enforcement lies in the extension of general provisions concerning data protection to the area of police and judicial cooperation.
- The drafting of a comprehensive data protection framework, firstly, has to take into account the specificities of EU policy-making regarding technology and data processing, and provide not only safeguards and principles, but also policy guidelines for a field that has so far been characterised by two tendencies:
  - The tendency to treat technology as an 'unchallenged policy option': In recent years, data processing schemes have proliferated in EU AFSJ policies in relation to police and judicial cooperation in criminal matters. This is due to the lack of agreement among the EU institutions, and in relation to the private sector, on the overall orientations of such policies.
  - The tendency to 'programmatic policy making': The absence of agreement among policy-makers and in relation to the private sector resulted in policy practices whereby new data processing schemes are initiated before schemes that have already been agreed upon are implemented fully. An overview of current and upcoming schemes shows that there are currently more than 25 such initiatives. Programmatic policy-making has limited the possibility to run proper impact assessments, including privacy and budgetary impact assessments, and limits the possibility to assess the necessity and proportionality of envisaged measures.
- The drafting of a comprehensive data protection framework, secondly, has to take into account the specific directions taken by practices in the field of police and judicial cooperation in criminal matters, in relation with the growing reliance on technology and particularly on data processing. These directions include:
  - A shift towards dataveillance, pro-activity and profiling: the growing and massive collection of personal data is concomitant with the pursuit of anticipatory actions in relation to criminal offences. It involves the use of pattern recognition techniques (data mining and profiling), which challenges the functioning of criminal justice systems and particularly the presumption of innocence.
  - The extension of the 'life of data' and the risk of unregulated function-creep 'by default', which challenges data protection principles such as purpose limitation, consent and access.
  - The promotion, through the development of policy prescriptions on the technical architecture of data processing schemes, of a 'data sharing by default' attitude among law-enforcement practitioners.

- The growing reliance of EU home affairs agencies (such as EUROPOL and FRONTEX) on dataveillance, which also includes the promotion of data processing schemes through the future EU agency for the management of large-scale IT systems.

2.1. Introduction

This chapter examines the challenges resulting from the increasing deployment of technologies for the collection, analysis and exchange of information and personal data among EU and Member State security agencies, with specific attention to the intensifying EU-level inter-agency cooperation. It is meant to provide background and supporting material to the analysis of the legal implications of the upcoming EU DPF, particularly in the light of the European Commission's proposals in this area.

The chapter surveys recent trends in EU internal security policies regarding technology and the use of personal data for law enforcement purposes. It assesses in particular a series of developments stemming from the adoption of the Stockholm programme,[59] the Internal Security Strategy (ISS)[60] and the Information Management Strategy (IMS).[61] Through these documents, the EU has placed technology at the very core of its law enforcement policies. Reliance on technology is not in itself a novelty in internal security policies. The SIS, for one, has been a cornerstone of cooperation among European police forces since it became operational in 1995. In recent years, however, proposals for the deployment of new data processing systems expected to manage personal data for law enforcement purposes have multiplied, while the two most ambitious projects in this domain – the Visa Information System (VIS) on the one hand and the second generation of the SIS (SIS II) – have experienced significant technical and political delays and are yet to become functional. This has contributed to blur the contours of the European data processing landscape, generating the conditions for what the WP29 has recently called a 'data deluge'.[62] The criteria, including necessity and proportionality, which inform the launching of such initiatives, remain unclear. So too are their implications as regards the legal obligations of the EU and its Member States regarding the protection of the personal data of the persons affected by the operation of these data systems.

The chapter is divided into two main sections:

- The first section assesses the status of technology in the policies related to the AFSJ. It argues that technology currently constitutes an 'unchallenged policy option' in AFSJ policies, which results in practices of 'programmatic policy-making' whereby initiatives regarding the establishment of systems processing personal data are allowed to proliferate with little consideration for their concrete outcomes.
- The second section examines the specific challenges arising from this state of play for privacy and data protection. It highlights how the increasing deployment of technology supports the evolution of law enforcement towards dataveillance, pro-activity and profiling, and analyses in this regard the recent proposals for a

[59] European Council, *The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens*, op. cit.

[60] Council of the European Union, *Draft Internal Security Strategy for the European Union: Towards a European Security Model*, 5842/2/10, 23 February, Brussels, 2010.

[61] Council of the European Union, *Draft Council Conclusions on an Information Management Strategy for EU internal Security*, 16637/09, 25 November, Brussels, 2009.

[62] See Article 29 Data Protection Working Party, Opinion 3/2010, 13 July 2010, p. 4.

European information management model. Dataveillance is used here following the recent coining of the term in a report to the United Kingdom's Information Commissioner as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons".[63] It further scrutinises the implications of this evolution for some EU home affairs agencies and cooperation between them (such as FRONTEX and EUROPOL), particularly with regard to the fact that they are increasingly called upon to exchange and process data related to individuals.

2.2. Technology in EU AFSJ policies: An unchallenged policy option for programmatic policy-making

In recent years, technology has evolved into a major policy option for the EU's security policies in the AFSJ. A number of contributions have suggested, in this respect, that the challenge for the updated data protection framework is not only to establish and clarify the legal principles applicable to data processing schemes in the EU, but also to provide guidelines for the organisation of the policy-making process itself. This has been recognised by the recent opinion of WP29 on accountability, which stresses that the principle of accountability should be a cornerstone of data protection in the upcoming EU data-protection framework. The effective implementation of such a principle would require data controllers to ensure, among others, the "[e]stablishment of internal procedures *prior* to the creation of new personal data processing operations (internal review, assessment, etc.)" and the "[m]apping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations".[64]

This section provides evidence on current practices regarding the deployment of new data systems at the EU level highlight the relevance of such recommendations. It shows in particular that technology is currently an unchallenged policy option in the Union's AFSJ policies and the object of a programmatic policy making which sees initiatives proliferate independently of any concrete outcomes.

2.2.1. Technology as an unchallenged policy option

Over the past few years, technology has been embraced without much debate as a core component for the EU's AFSJ policies. The argument is best articulated in the June 2008 report from the Future Group on European home affairs, which considers that "[d]atabases and new technologies will play a central role in further developing Home Affairs policies […] Even if technology can never completely replace the human factor, technological progress can provide the necessary means to optimise mobility, security and privacy simultaneously".[65] The Stockholm programme has formally endorsed this position, by making the mobilisation of the 'necessary technological tools'[66] an integral component of the EU's internal security policies. Computer systems designed to collect, exchange and process information, including personal data, are the cornerstone of this emphasis on technology in law-enforcement activities. The European ISS, for instance, calls for a 'European Information Exchange Model' that "will include all the different EU databases relevant for ensuring security in the EU so that there can be interaction between them, as

[63] See Surveillance Studies Network, *A Report on the Surveillance Society – for the Information Commissioner by the Surveillance Studies Network*, London, September 2006.

[64] Article 29 Data Protection Working Party, *Opinion* 3/2010,, 13 July 2010, p. 11.

[65] Future Group. *Freedom, Security, Privacy - European Home Affairs in an open world*. Brussels, Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, June 2008, p. 18.

[66] Council of the European Union, *The Stockholm Programme - An open and secure Europe serving and protecting citizens*, 5731/10, 03.03.2010 p. 65.

far as it is needed and permitted, for the purpose of providing effective information exchange across the whole of the EU and maximising the opportunities presented by biometrics and other technologies for improving our citizens' security within a clear framework that also protects their privacy".[67]

The centrality of technology for AFSJ policies nonetheless raises a number of questions. The discussion of this issue cannot be dissociated from a broader reflection on how policy-making regarding technology for law-enforcement purposes has been conducted in the EU institutions. There has been a tendency, particularly from the European Commission and the Council, to present the deployment of large data systems as a 'technical matter' requiring extensive periods of research and development[68]. In the process, some procedural requirements have been circumvented. This includes the submission of proper impact assessment reports that cover the legal and financial aspects of policy initiatives, examine their necessity, added value and proportionality,[69] as well as their anticipated effects on fundamental rights including privacy and data protection.[70] Not only have such initiatives developed with unclear justification of their compliance with the principles of necessity and proportionality, but this has also been done, in some cases, with limited involvement from the European Parliament and bodies such as the EDPS and the WP29, and with even less inputs from civil society organisations.

Policy-making with regard large-scale IT systems has been 'programme-driven' rather than 'evidence-driven',[71] echoing the respective political priorities of some Member States, the European Commission as well as the private sector,[72] rather than responding to a demonstrated need. This appears to have been all the more problematic as the tensions between the European Parliament and the Council around the Terrorist Financial Tracking Program (TFTP) or PNR agreements with the U.S. have shown a considerable degree of concern among some parliamentarians, civil society and citizens at large regarding the question of privacy and data protection in the context of large-scale exchanges of information for law-enforcement purposes.

A good illustration of this trend is provided by the measures adopted in the wake of the European Commission's February 2008 'border package'. Composed of three communications,[73] the package examined the possibility of establishing four new EU-level

[67] Council of the European Union, *Draft Internal Security Strategy for the European Union: "Towards a European Security Model"*, 5842/2/10, 23.02.2010p. 13.

[68] As noted for instance by Joanna Parkin, this has typically been the argument of the European Commission's DG JLS services involved in the development of SIS -II, presented as a mere update which did not require an impact assessment or a public consultation. See Parkin, J., *The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law*, CEPS Liberty and Security in Europe, April, 2011

[69] As laid out in the European Commission's internal impact assessment guidelines. See European Commission, *Impact Assessment Guidelines*, SEC(2009) 92, 15 January 2009

[70] The EDPS has recently noted on this question that '[Privacy impact assessments] are significant as they allow institutions and bodies to gain better insight into relevant privacy risks and ways to address these risks. They may also lead to notifications and possibly prior checks, recommendations and follow-up'. See European Data Protection Supervisor, *Monitoring and Ensuring Compliance with Regulation (EC) 45/2001* Policy Paper, 13 December 2010

[71] Parkin, J., op. cit.p. 25.

[72] On the role of the defence and security industry in the formulation of EU security policies (the "public-private dialogue"), see for instance Bigo, D., Jeandesboz, J., *The EU and the European Security Industry: Questioning the 'Private-Public Dialogue'*, CEPS INEX Policy Briefs No. 5, February 2009

[73] A report on the evaluation and future development of the FRONTEX agency (COM (2008) 67 final, 13.2.2008), a communication examining the creation of a European Border Surveillance System

data-systems: a Registered Traveller Programme (RTP), Entry/Exit System (EES) and EU Electronic System of Travel Authorisation (EU-ESTA) on the one hand, and a European border surveillance system (EUROSUR) aimed primarily at Member States southern maritime reaches on the other. Despite the ambitious nature of the proposals, however, research on the issue has shown that the elements of impact assessment provided for in the accompanying working documents remained piecemeal.[74] The preliminary comments of the EDPS on the 'border package' reflected the disagreements that had accompanied the tabling of these proposals. They suggested that the necessity and proportionality of the envisaged measures is not properly demonstrated: "[F]ar-reaching proposals implying surveillance of the movements of individuals follow each other at an amazing pace. Many proposals are tabled or are about to be tabled in this area (SIS II, VIS, review of Eurodac Regulation, access of law enforcement agencies to these systems, PNR, etc.) […] The sheer number of these proposals and the seemingly piecemeal way in which they are put forward makes it extremely difficult for the stakeholders (European and national Parliaments, DPA's including EDPS, civil society) to have a full overview. This limits the possibility to contribute meaningfully".[75] The EDPS further requested "to see evidence that there is a master plan for all these initiatives, giving a clear sense of direction".[76] This was echoed by the Conference of European DPAs, which called upon the European institutions and the Member States to "first evaluate whether already existing legal measures are implemented and executed in an effective way", establishing the principle that a "new proposal should be put forward only when clear evidence is available to support new actions".[77] This is not by far a singular pattern: in 2006, already, the EDPS had regretted that the European Commission's proposal for a regulation on SIS II had not been accompanied by an impact assessment study, on the argument that the first version of SIS was already in place.[78]

The question might however not be that there is a lack of 'master plan', but that there are too many of them. The European Commission advocates technology as a support to a 'European' approach to security, while Member States consider it as a means to retain their competencies in the field of security, and private providers frame it as a 'solution' to security issues. As previous research has pointed out,[79] the so-called security industry in

(COM(2008) 68 final, 13.2.2008) and another on preparing the next steps in border management in the European Union (COM(2008) 69 final, 13.2.2008)

[74] In the case of EUROSUR, see for example Jeandesboz, J. *An analysis of the Commission communications on future development of FRONTEX and the creation of a European Border Surveillance System*, PE 408.295, Brussels, 2008; see also the work conducted in the framework of the FP7 INEX project, in particular: Amicelle, A., Bigo, D., Jeandesboz, J., Ragazzi, F., *Catalogue of Security and Border Technologies at Use in Europe Today*, D.1.2., Oslo, 2009.

[75] European Data Protection Supervisor, *Preliminary Comments on COM(2008) 69 final, COM(2008) 68 final, COM(2008) 67 final*, March, 2008, p. 3

[76] Idem.

[77] Conference of European Data Protection Authorities. *Declaration on three communications from the Commission on border management*. Rome, 18 April 2008, p. 1.

[78] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final)*. Official Journal C 91, 19 March 2006

[79] See Bigo, D., Jeandesboz, J., *Review of Security Measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*, PE 393.289, May, 2008; Jeandesboz, J., Ragazzi, F., *Review of Security Measures in the Research Framework Programme*, PE 432.740, October, 2010.

particular has played a central role in defining the technological orientations of EU security policies. One important trend in the priorities advocated in settings such as the 2004 Group of Personalities on Security Research, the 2006 European Security Research Advisory Board (ESRAB) and the 2009 European Security Research Innovation Forum (ESRIF) has been the development of large-scale, integrated systems involving the mass processing of personal data. These priorities have also been echoed in the various projects funded under the EU's Preparatory Action on Security Research (PASR) and the Security Theme of the 7th Framework Research Programme. They have coalesced, more than converged, with the diverging objectives of the Commission and the Council in the field of security, and nurtured the tendency to consider technology as an unchallenged policy option.

The impact of such practices for fundamental freedoms and rights should not be underestimated. In a previous briefing paper for the European Parliament, DG Home Affairs of the European Commission has been found to be particularly expeditious in its assessment of the data protection and privacy implications of EUROSUR,[80] stating that "[t]he different activities referred to […] may involve the processing of personal data", the section dedicated to data protection essentially argues that "the principles of personal data protection law applicable in the European Union are to be observed".[81] The data protection considerations for the RTP and EES initiative are slightly more developed, giving specific details as to how data would be stored and suggesting that the VIS data protection provisions would offer one policy option in this regard. While these considerations appear to match the formal methodological requirements for ensuring the compliance of European Commission proposals with the Charter of Fundamental Rights,[82] however, they do not address privacy, fundamental freedoms and rights concerns substantially.

While they offer lengthy technical specifications on the functioning of the proposed systems, they lack a similarly detailed description of the steps taken to ensure that these systems will not breach privacy and data protection law. In the meantime, a number of activities have been undertaken to develop the proposals of the 'border package'. In the name of "pressing operational needs facing the Union in particular at the southern maritime borders of the Schengen area"[83] and despite some concerns expressed within the European Parliament,[84] for instance, the development of EUROSUR has been allowed to proceed. The initiative has been singled out as a priority in the Stockholm Programme and the ISS, as well as in the Commission's Action Plans on the implementation of both documents.[85] The

[80] Jeandesboz, J., An Analysis of the Commission Communications On Future Development of Frontex and the Creation of a European Border Surveillance System (EUROSUR), LIBE Committee, PE 408.295, June 2008, p. 15.

[81] European Commission, *Commission staff document – Examining the creation of a European Border Surveillance System*, SEC(2008) 151, Brussels, 2008, p. 57

[82] As foreseen in COM(2005) 172 final, 27.4.2005 and restated recently in COM(2010) 573 final, 19.10.2010. Coherence with the Charter is also an integral part of the abovementioned Commission Impact Assessment Guidelines laid out in SEC(2009) 92 of 15.1.2009. See European Commission, *Compliance with the Charter of Fundamental Rights in Commission legislative proposals*, COM (2005) 172 final, 27.4.2005, Brussels; European Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*, COM (2010) 573 final, 19.10.2010, Brussels; European Commission, *Impact Assessment Guidelines*, SEC (2009) 92 final, 15.1.2009, Brussels.

[83] European Commission, *Report on progress made in developing the European Border Surveillance System*, SEC(2009) 1265 final, 24.9.2009, Brussels, p.2.

[84] See the opinion of the Committee on Development for the LIBE Committee (2008/2157(INI), 7.10.2008) which highlights the fact that 'third country nationals may lack adequate means to monitor whether personal information on them gathered in the planned 'system of systems' of the EU is handled in accordance with the principles of data protection law applicable in the EU' (p. 4).

[85] See respectively European Commission, *Delivering an Area of Freedom, Security and Justice for Europe's citizens: Action Plan Implementing the Stockholm Programme*, COM(2010) 171 final,

European Commission has provided a degree of reporting on progress,[86] but this has not been the case for all the 'border package' initiatives. The entry/exit system initiative here is a case in point. A number of discussions have taken place within the Council's Working Party on Frontiers under the auspices of the French and Czech presidencies, with questionnaires being circulated to delegations[87] and a 'data collection exercise' involving the border control authorities of the Member States at the external borders was organised between 31 August and 6 September 2009.[88] These elements have been considered good enough for DG Home Affairs to move along and draft legislative initiatives on EUROSUR and the EES (as part of the so-called 'smart borders' initiatives), but the process has been less than transparent, and the overall strategic outlook called for by European DPAs on these measures has yet to be provided.

2.2.2. The proliferation of data-systems and programmatic policy-making

One consequence of the current standing of technology as an unchallenged policy option for the AFSJ has been the proliferation of initiatives regarding data systems at the EU level in recent years. The trend is problematic, as suggested above, insofar as it challenges the principles of sound and effective policy-making that govern the activities of the EU institutions. It also puts a strain on the possibility to keep track of how many initiatives are currently under way, the persons that are targeted by these systems and their expected impact - be it from a financial perspective or more importantly in terms of their possible effects on the fundamental freedoms and rights of EU citizens and third country nationals alike. There is, in this respect, a lack of public knowledge as to the exact number of these data-systems, as to what they are supposed to do and how they are being developed, as to their effectiveness and cost, and possibly as to their redundancy.

It is only in July 2010, following the adoption of the Stockholm Programme and of the Commission's action plan for its implementation,[89] that DG Home Affairs provided a first general overview of data systems in operation, under implementation or consideration in the EU AFSJ. The assessment accounted for twenty-five EU data processing mechanisms (existing or under consideration) involving the processing of personal data, but provided very little information as to their effective functioning.[90] Most of these mechanisms have been agreed upon during the last decade while at the same time the two foremost EU efforts in the area of large-scale IT systems – the SIS II and VIS – have yet to become operational. Policy-making in this regard is increasingly becoming programmatic: new initiatives are launched while previous ones have not brought any concrete outcomes and remain 'under implementation'. This has resulted in the setting up of systems which exist 'virtually', and for some already being promised to obsolescence should they actually go online. Programmatic policy-making, in this regard, is supported by divergences in the

20.4.2010, Brussels; European Commission, *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM(2010) 673 final, 22.11.2010, Brussels..

[86] See European Commission, *Report On Progress Made In Developing The European Border Surveillance System (EUROSUR)*, as well as European Commission, *Determining the technical and operational framework of the European Border Surveillance System (EUROSUR) and the actions to be taken for its establishment*, SEC(2011) 145, 28.1.2011, Brussels

[87] Council of the European Union, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 12251/08, Brussels, 2008.

[88] See Council of the European Union, *Results of the data collection exercise*, 13267/09, Brussels, 2009.

[89] European Commission, Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme,2010

[90] European Commission, *Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, 20.7.2010, Brussels.

policy agendas of the European Commission's services, of Member State representatives, of the private sector, but also of the European Parliament and of DPAs.

This section provides an overview of these various initiatives,[91] It is complemented by Table 1 provided in the Annex of this study, which provides a summarised overview of tabled, upcoming and envisaged proposals for additional data-processing schemes in the EU's AFSJ. One can distinguish, firstly, the data-processing schemes controlled or managed at least partially by the EU institutions and bodies. These include:

- Six data-systems in activity: Eurodac, the Customs Information System (CIS) and the SIS, EUROPOL's Computer System (TECS)[92], the EUROJUST information system and the information exchange structure of the Joint Situation Centre (SitCen);[93]
- Two future systems are yet to be activated, and have been held back due to problems with private contractors as well as political and bureaucratic disagreements over what their purpose should be: SIS II and VIS.

In addition to these systems managed by EU institutions and bodies, one can also mention the following data processing schemes that are controlled/managed at Member State level:

- As regards the circulation of persons and goods:
  - Advanced Passenger Information (API) scheme, established through Council Directive 2004/82/EC,[94] which calls on Member States to create an obligation for air carriers to transmit API data (including name, date of birth, nationality, type and number of ID document, initial point of embarkation and border crossing point of entry) to Member States border control authorities.
  - Naples II Convention scheme,[95] which is complemented by the CIS and enables the exchange of information between Member States central coordination units on infringements of national and Community customs rules.
- As regards cooperation in criminal matters and counter-terrorism:
  - Financial Intelligence Units scheme, initially adopted under Council Decision 2000/642/JHA for the purpose of combating money laundering and later adapted for anti-terrorist financing purposes (as per the Third Anti-Money Laundering Directive – Directive 2005/60/EC).[96]

[91] Drawing among others from Geyer, F., *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS CHALLENGE Research Papers No. 9, May 2008;Hempel, L., Carius, M., Ilten, C., *Exchange of information and data between law-enforcement authorities within the European Union*, PE 419.590, April 2009, Brussels.

[92] TECS further comprises three distinct data processing schemes: the EUROPOL Information System, the EUROPOL Analytical Workfiles and the Index System.

[93] SitCen is said not to process personal data as such, although the information circulated through the Centre might include details on specific individuals. For instance, SitCen provides files on persons falling within the remit of Common Position 2001/931/CFSP of 27 December 2001 on the freezing of assets of "persons, groups and entities involved in terrorist acts" to the Council Working Party in charge of implementing the Common Position (CP 931 WP).

[94] Council Directive 2004/82/EC of 29 April 2004 on the obligations of carriers to communicate passenger data, OJ L261, 6.8.2004, p. 24

[95] Council Act of 18 December 1997 drawing up, on the basis of Article K.3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations (98/C 24/01), OJ C24, 23.1.98, p. 1.

[96] See, respectively Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA), OJ L271, 24.10.2000, p. 4 ; Directive 2005/60/EC of the European Parliament and

- Swedish Initiative scheme[97] on the sharing of information among Member States for criminal investigation or criminal intelligence operations.
- DRD scheme[98] under which an obligation is created for telecommunication service providers to retain electronic communication traffic, location data and information about customers (telephone number, IP address, mobile equipment identifiers) for the investigation, detection and prosecution of 'serious crime'.
- Asset Recovery Offices scheme[99] on information for tracking and identifying the proceeds of crime. Exchanges of information take place on the basis of the Swedish initiative.
- The Prüm agreement signed in 2005 between the Benelux countries, Austria Germany, France and Spain was transformed, under the auspices of the German presidency, into an EU instrument. The Prüm Decision[100] establishes a decentralised system interconnecting participating states' DNA, fingerprint and vehicle registration databases, looking to establish by 2011 automated data comparisons. For DNA and fingerprints, comparisons operate through a hit/no hit system and rely on the Swedish initiative scheme to exchange additional information.
- The Council has adopted Decision 2009/316/JHA which implements Framework Decision 2009/315/JHA and establishes the European Criminal Records Information System (ECRIS).[101]

A final category of data processing schemes is established in the context of relations with third countries, the two main examples being PNR agreements and the EU-US TFTP Agreements:

- PNR agreements: PNR agreements have been negotiated between the EU and the United States[102] and Australia. An API/PNR agreement was negotiated with Canada

of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L309, 25.11.2005, p. 15.

[97] Council of the European Union, Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union, OJ L386, 29.12.2006, p. 89

[98] European Parliament and Council of the European Union, Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L105, 13.4.2006, p. 54.

[99] Council of the European Union, Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, OJ L332, 18.12.2007, p. 103.

[100] Council of the European Union, Decision 2008/615/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210, 6.8.2008, p. 12

[101] See: Council of the European Union, Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L93, 7.4.2009, p. 23; Council of the European Union, Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ L93, 7.4.2009, p. 33

[102] The 2007 agreement is the last of three initial agreements on PNR data between the EU and the US. The 2004 agreement was annulled by an ECJ decision on 30 May 2006. An interim agreement was signed on 16 October 2006. For further details see Guild, E., Brouwer, E., *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, July 2006, Brussels; Guild, E., *Enquiry into the EU-US Passenger Name Record Agreement*, CEPS Policy Brief No. 125, March 2007, Brussels; Hobbing, P., *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, CEPS Special Report, September 2008, Brussels.

and signed in October 2005.

- EU-US TFTP Agreements: just like PNR agreements, the EU-US TFTP Agreements are specific data processing arrangements in the field of counter-terrorist cooperation in that they involve a third country. They involve the processing by the US Department of Treasury of financial messaging data obtained from the Society for Worldwide Interbank Financial Communication System (SWIFT) company, including data on transactions carried out by European citizens. The process through which the first agreement was reached does not need to be detailed further,[103] but it illustrates very well how the positions of the European Parliament and European DPAs were circumvented in this policy area.

All these systems involve or foresee the processing of personal data. Some further include the processing of sensitive personal data (e.g. criminal records) and of biometric data. They also target a wide range of groups. TECS for instance records information on suspects or persons convicted of a crime, but also on possible future offenders, victims or possible victims, witnesses, contacts and associates of the previous (particularly in its Analytical Work Files component). The VIS, when it finally becomes operational, will systematically include the records of all persons applying for a Schengen visa for a five-year period (totalling 70 million records for any such period). It will also single out EU citizens who host visa applicants, by withholding some biographical information.

In addition to these already established schemes, a number of data processing operations are currently being considered:

- References have multiplied regarding the development of a 'FRONTEX information system' (FIS). We will return to the issue of the processing of personal information by FRONTEX below, but at this stage it should be specified that what the FIS does or is expected to do, however, remains unclear at this stage. The initial rationale for its development is the establishment of secure communications between Member States border services, the European Commission and the agency,[104] but not the processing of personal data. This is echoed in the Commission's February 2010 proposal amending Regulation (EC) 2007/2004 includes a modification (replacing Article 11 of the initial Regulation) whereby the agency "shall develop and operate an information system capable of exchanging classified information with the Commission and the Member States", specifying that the "exchange of information to be covered by this system shall not include the exchange of personal data".[105] In its draft report on the proposal, however, the LIBE Committee foresaw the deletion of this last sentence and the introduction of a new Article 11 according to which the Agency "may process personal data […] obtained during joint operations or pilot projects or rapid border intervention operations".[106] In addition, the Commission's

[103] See for instance Amicelle, A., *The Great (Data) Bank Robbery: Terrorist Finance Tracking Programme and the "SWIFT Affair"*, CERI Research Questions, No. 36, March 2011, Paris.

[104] See for instance the FRONTEX General Report for 2007.

[105] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union*, COM(2010) 61 final, 24.2.2010, Brussels, p. 27

[106] Draft report of Simon Busuttil (PE450.754v01-00) on the proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), 2010/0039(COD), 6.7.2011, Amendment 59. The persons whose data can be collected include 'persons who are suspected on reasonable grounds of involvement in cross-border criminal activities, in illegal migration activities or in human trafficking activities […], persons who are victims of such activities and whose data may lead to the perpetrators

2008 impact assessment on EUROSUR and subsequent reports on the development of the system imply that the FIS will be the component that will enable FRONTEX to become the key data-processing node in this system.

- As regards the circulation of persons and goods, the Commission's 2008 'border package', as mentioned previously, has led to a number of initiatives aiming at developing EUROSUR.[107] It is to be followed in 2011 by several legislative proposals pertaining to DG Home Affairs' 'smart borders' initiatives. These include a proposal for introducing an EU EES and RTP, for providing EUROSUR with a legal instrument, and a communication on the setting up of an EU ESTA.
- Review of the DRD: The Commission submitted on 18 April 2011 an evaluation of the DRD.[108] It concludes that a revision of the Directive is necessary, without providing more information as to how the review might unfold. Over the years, the DRD has drawn intense criticism, including from the EDPS who argues in his opinion on the evaluation report that: a) the DRD has "failed to meet its main purpose", namely providing for a harmonised framework for national legislations on data retention and, b) that it "does not meet the requirements set out by the right to privacy and data protection" with regard to the criteria of necessity, proportionality and foreseeability.[109]
- Two EU data systems have been given impetus as a result of recent developments in international and transatlantic relations, regarding PNR data on the one hand,[110] and financial information in the context of the tracking of terrorist financing (TFTP agreements with the US):
  - EU-PNR: the Commission tabled a proposal on the development of a European PNR scheme in November 2007.[111] Work in the Council on this issue began in February 2008, but the Parliament refused in November 2008 to vote on the issue. The idea resurfaced in the Stockholm Programme.[112] The European Commission's next proposal was tabled, together with an impact assessment and Commission working paper, in February 2011.[113]
  - EU-TFTP: the idea of an EU equivalent to the US TFTP scheme was first proposed by the European Parliament, with the aim to prevent bulk data transfers to the US and ensure that extraction and analysis of SWIFT data takes

of such illegal activities as well as persons who are subject to return operations in which the Agency is involved'.

[107] Work on the RTP has mainly involved surveying initiatives on automated border checks in Member States as well as in some third countries. See for instance the BIOPASS I (2007) and II (2009) studies conducted by FRONTEX.

[108] European Commission, *Evaluation Report on the Data Retention Directive*, COM(2011) 225 final, 18.4.2011, Brussels.

[109] See European Data Protection Supervisor *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, 31 May 2011, Brussels.

[110] Agreeements with Canada (signed October 2005), the U.S. (July 2007) and Australia (June 2008).

[111] European Commission, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, 6.11.2007, Brussels.

[112] Where the European Council 'calls upon the Commission to propose an Union measure, that ensures a high level of data protection, on PNR for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime' (op.cit., p. 65).

[113] See European Commission, *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, 2.2.2011, Brussels and accompanying documents SEC(2011) 132 and SEC(2011) 133 final

place on European territory. In its 2010 legislative roadmap, the European Commission has adopted a 'EUROPOL option', placing the European Police Office at the centre of the collection and analysis of flows of financial information.

The programmatic and anticipatory quality of EU policy making with regard data processing schemes in the field of AFSJ is clearly demonstrated by the evidence provided here. Before we examine the specific challenges raised by these practices for data protection, two general points can be made.

Programmatic policy making, firstly, raises questions as to the overall consistence of envisaged data processing schemes and the quality of the impact assessments provided to demonstrate the necessity and proportionality of new initiatives. A case in point, here, is the relation between the VIS and the EES to be proposed by the end of 2011. In the 2004 impact assessment document accompanying the proposal for the VIS Regulation, DG Home Affairs examined the setting up of an EES as an alternative to the creation of the VIS. It found the EES "extremely costly to implement" and "less advantageous than VIS with biometrics".[114] Four years later, the impact assessment document accompanying the 2008 communication on next steps in border management in the EU argued that "the technical feasibility of an entry/exit system has in the meantime improved due to the development of the VIS" and finds it "therefore timely to reassess the option more thoroughly".[115] The EES is identified as a flanking measure to the VIS and would use the biometric data stored in the latter, whereas it was originally considered as an alternative, and this despite the fact that there is no information as to the impact of the VIS since this system has yet to come online. By the same token, the 2008 communication on border management envisages the creation of a Registered Traveller Programme as "a response to the additional constraints and implications for cross-border travel that the entry/exit system could impose"[116] – establishing yet another data processing scheme involving sensitive data (biometrics) without any notion of whether the EES is practically operable.

Programmatic policy making, secondly, results in recurrent challenges for fundamental freedoms and rights. In the example provided in the previous paragraph, it multiplies the occurrences of (particularly sensitive) data processing for some persons (third country nationals facing visa obligations for short stays in the EU) and extends processing to the data of other groups: the EES and RTP would, depending on the policy option pursued, apply to third country nationals exempted of visa requirements and EU citizens. Another striking illustration is the case of PNR data exchanges with third countries. The purpose of the September 2010 communication of the Commission (DG Home Affairs) on a global approach to the question was to promote a consistent and horizontal approach to these matters. This has however led the EDPS to question "the general timing of the different initiatives directly or indirectly related to the processing of PNR data" in its 16 October 2010 opinion. The proposals for a global approach on PNR data, on the one hand, risk to duplicate the work in progress on the conclusion of an EU-US general agreement on data sharing for law enforcement for which the Commission (DG Justice) opened a public consultation in January-March 2010 and that would provide, in the EDPS' view, a template for agreements with other third countries. On the other hand, it excludes from its scope discussions concerning the EU-PNR scheme and does not relate this latter issue to the

[114] European Commission, *Annex to the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas – Extended Impact Assessment*, SEC(2004) 1628 final, 28.12.2004, Brussels, p. 32.

[115] European Commission, *Preparing the next steps in border management in the European Union – Summary of the impact assessment*, SEC(2008) 153 final, Brussels, 2008, p. 24.

[116] Ibid, p.29.

updating of the data protection framework. The EDPS highlights in this regard that "[t]he global agenda should therefore concentrate first on the general EU data protection framework, then on the possible need for an EU PNR scheme, and finally on the conditions for exchanges with third countries, based on the updated EU framework".[117]

In the current situation, the development of a global approach to PNR exchanges with third countries, of an EU-PNR scheme, the negotiation of an EU-US agreement on data sharing and the updating of the DPF will all take place simultaneously, considerably limiting the possibility for data protection principles to be duly taken into account. The overall impact of this virtual policy-making is already being experienced. On 18 May 2011, shortly before the Commission circulated the draft EU-US PNR agreement to the Council,[118] the Commission's legal service transmitted a note to the director general of DG Home Affairs, pointing out "grave doubts as to its compatibility with the fundamental right to data protection".[119] Among other elements, the Commission's legal service points out the problem of defining "serious crime" (the main purpose for which PNR data processing is allowed) as "extraditable offence" defined as offences punishable by deprivation of liberty for a maximum period of more than one year, which is larger than the EU PNR proposal (3 years) or the draft agreement with Australia (4 years) and considerably widens the range of data that could be processed.

2.3. Technology for EU law-enforcement: dataveillance and the challenges to data-protection

After examining the standing of technology in EU AFSJ policies, this section details the specific data protection challenges posed by the increased processing (ongoing or envisaged) of personal data for law-enforcement:

- The first set of challenges relates to the logics underpinning the generalisation of data processing in law enforcement, namely the shift towards dataveillance, pro-activity and profiling.
- The second set of challenges is tied to the 'life of data' in EU data-systems. The increasing processing of personal data, the proliferation of data-systems and the tendency to consider technology as a one-size-fits-all solution is problematic with regard to one of the key principles of data-protection, namely purpose limitation, and leads to 'function-creep by design' in the development of current and upcoming data-systems.
- The third set of challenges follows from the very architecture of data processing. One of the key arguments to justify the proportionality of EU initiatives in establishing data-systems for law-enforcement purposes is that they are not envisaged as steps in the creation of a centralised and fully integrated Union-wide database system. Networked convergence, which is pursued through the promotion of the principle of availability, of interoperability and the fostering of common infrastructure is however not a guarantee that privacy and data-protection will be upheld, and it is in this respect that the development of a European information model can be critically assessed.

[117] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Personal Name Record (PNR) data to third countries*, 16 October 2010, Brussels, p. 3-4.

[118] See Council of the European Union, *Draft Agreement between the United States of America and the European Union on the use and transer of Passenger Name Record data to the United States Department of Homeland Security*,10453/11, 20.5.2011, Brussels

[119] Statewatch, Commission document SJ.1 603245, 2011, available from Statewatch: http://www.statewatch.org/news/2011/jun/03eu-us-pnr-com-ls.htm (accessed September 2011)

- The fourth set of challenges relates to EU home affairs agencies. These bodies – and chiefly EUROPOL and FRONTEX – have become over the past ten years data controllers in their own right. A further source of concern is the foreseen creation of the EU agency for the management of large-scale IT systems, which might serve as a platform to launch additional initiatives for new data processing schemes.

2.3.1. Dataveillance, pro-activity and profiling

Current EU law-enforcement activities are premised upon the generalisation of data processing. This is strongly emphasised in the ISS, which considers that an objective of the 'European Security Model' should be to "increase substantially the current levels of information exchange" between European internal security agencies and bodies. Increasing data-processing is supposed to contribute to the development of "a stronger focus on the prevention of criminal acts and terrorist attacks before they take place". The European Security Model advocated by the ISS, then, should "emphasise prevention and anticipation, which is based on a proactive and intelligence-led approach as well as procuring the evidence required for prosecution".[120] DPA's have also noted the combination of increased data processing and a growingly preventive stance in law enforcement. In their December 2009 contribution to the consultation organised by the European Commission on the data protection framework,[121] WP29 and the Working Party on Police and Justice (WPPJ) suggest a threefold shift in policing practices:

- the use of personal data at earlier stages, beyond the investigation and detection of crime and for preventive purposes, as well as the processing of data from a wider group of persons beyond those actually involved in an investigation such as suspects or witnesses: travellers, users of banking services, of public transportation, etc;
- the use of technology to predict behaviours through automated tools and techniques such as data-mining and profiling and, concomitantly, the evolution in the type of data used (the growing inclusion of data that is not 'objectively determined' and based on evaluation and analysis – 'hard' and 'soft' data); and
- the accelerated circulation of information, through the processing of information originating from private sector organisations, the promotion of interoperability between data systems and the widening of access to information beyond police and judicial authorities to border control authorities or national security services.

The relation between the increased use of personal data for law enforcement purposes and prevention needs to be detailed further, insofar as it leads to an issue that should be considered central for the updated EU DPF, namely profiling.

A good example of the use of data at an earlier stage and for increasingly wider numbers of persons, firstly, is the VIS. The system purports to collect records on all the persons applying for a short-term visa to the EU. The system will, according to the European Commission's own figures and as already previously noted, hold at any given time the biographic and biometric data of 70 million persons.[122] Data processing schemes currently under consideration would extend this process. Depending on the option pursued, the EU

[120] Council of the European Union, *Draft Internal Security Strategy for the European Union*, 2010, p. 11

[121] See Article 29 Data Protection Working Party & Working Party on Police and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Working Paper No 168, 1.12.2009.

[122] European Commission, Commission Staff Working Document, Annex to the Proposal for a Regulation to the European Parliament and to the Council concerning the Visa Information System (VIS), p. 25.

EES could hold the personal data (biographic and biometric) of all third country nationals entering and exiting the EU, including of persons who do not face visa requirements.[123] The VIS, in this regard, also illustrates a long-standing trend in EU policies regarding data processing for law-enforcement purposes, namely the tendency to test such schemes on foreigners, before expanding them to EU citizens.

These illustrations point out to a central trend in contemporary European law-enforcement. In the VIS/EES/PNR cases, the scrutiny of persons travelling to, entering and exiting the EU extends beyond the various moments of control (upon delivery of the visa, upon entering Member State territory and exiting it): law-enforcement then relates to surveillance and, insofar as it is premised on the processing of personal data, to dataveillance. The expansion of data processing, whether to larger groups of persons or to additional data (e.g. biometric data in addition to biographic information) is certainly problematic in itself. The issues raised by dataveillance for privacy and data protection are made more stringent, however, by the correlation between dataveillance, pro-activity and profiling.

Pro-activity refers, in this context, to the increased emphasis placed on anticipative measures with regard to security matters. In the impact assessment of its 2011 EU-PNR Directive proposal, the European Commission makes a telling distinction, in this regard, between the three ways in which Member States authorities can use the proposed data-system:

- "re-actively: use of the data in investigations, prosecutions, unravelling of networks after a crime has been committed;
- in real-time: use of the data prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is being committed; and
- pro-actively: use of the data for analysis and creation of assessment criteria, which can then be used for a pre-arrival and pre-departure assessment of passengers" (p. 11).

The 'reactive' stance is the one traditionally adopted by criminal police services and the judiciary: it relates to an evidence-based and investigative procedure, where a certain number of rights, including the presumption of innocence and access to redress, are guaranteed to the person(s) under investigation. The 'real-time' and 'pro-active' options, which are very close in the definition, are considerably more problematic in that they are not based on evidence, but on profiling, a question that is arguably central for the updating of the DPF as regards AFSJ matters.

Profiling has been a remarkably absent terminology in EU documents related to law-enforcement. As noted by some observers, the EU institutions have shown some reluctance in using the word, favouring terms such as 'risk assessment'[124] or more complex formulae such as – in the case of the proposed EU-PNR Directive mentioned above – the "use of data for analysis and creation of assessment criteria". Not all data processing schemes are open to profiling, of course. Among the above-mentioned mechanisms, the possibilities opened by Directive 2005/60/EC (Third Money Laundering Directive) or foreseen for the EES or the EU-PNR system are the best examples. Profiling is nonetheless increasingly advocated as a key component in the EU's AFSJ policies and is an established practice in Member State law-enforcement agencies and bodies.

[123] The exact number of persons who would be concerned by this data-processing scheme, however, has not been documented so far.

[124] De Hert, P., Bellanova, R., *Data Protection in the Area of Freedom, Security and Justice: A System Still to Be Developed?*, PE 410.692, March, Brussels, 2009

The Future Group on European Home Affairs recommended for instance in the run-up to the Stockholm programme that Member States prioritise "technologies that enable automated data analysis".[125] In its recommendations on EU-PNR, the ISS argues that this data processing scheme would enable "impact assessment […] to deepen our understanding of the different types of threat and their probability and to anticipate what might happen, so that we are not only prepared for the outcome of future threats but also able to establish mechanisms to detect them and prevent their happening in the first place".[126] As the number of data processing schemes and the size of datasets constituted by European security agencies, bodies and services increase both at the EU and Member State levels, the generalisation of profiling supported by data-mining software is likely to become a central issue with regard privacy and data-protection.

It is crucial to highlight, in this regard, that profiling is not evidence. There are three categories of profiling, based on whether the person profiled is known or not.[127] A profile can be build out of the behaviour of a person who is already known, to infer that person's behaviour in a given situation. Profiles can secondly be used to build categories of persons who are already known, in order to have some indications of how they would behave in a given situation. Both types here can be accommodated within a criminal justice system, and can be used to conduct an investigation on an event that has already happened. A third type of profiling, however, occurs when patterns of behaviour are made anonym, and used to identify persons who were previously unknown. Profiling, in this third configuration, refers to a twofold process: first, to the analysis of a given dataset that serves to determine seemingly relevant patterns, and second, to the application of these patterns to the same dataset in order to identify items corresponding to these patterns.[128] In this third type, profiles are constructed from correlations and not from causal inference. They are, to use the words of some commentators, 'probabilistic knowledge', which implies that "even if a pattern appears to occur each time certain conditions are met, it is not absolutely sure that it will occur again in the future".[129] Profiling, as stated, is of course used in criminal investigation procedures, but it is then mostly descriptive, based on the characteristics of a criminal act that has already taken place, and supports the placing in custody of specific individuals. The problem with the current take on profiling in EU AFSJ policies is that it is overly geared towards the prediction of future behaviours within increasingly larger groups of persons. It enables a generalisation of suspicion, rather than the search for specific suspects. Predictive, technology-based profiling, as the EDPS pointed out in a 2008 intervention on the Commission's proposals for an EU entry/exit system, then raises concerns for a number of core principles of privacy and data protection as well as other fundamental freedoms and rights.

Insofar as it aims to predict actions that might be undertaken, profiling can entail

- a reversal of the presumption of innocence: large-scale profiling implies that every person whose data is submitted to such processing is placed under suspicion and considered as a would-be offender.
- a challenge to the principle of adequacy: the predictive orientation of profiling raises

[125] Future Group, op. cit., p. 43.

[126] Council of the European Union, *Draft Internal Security Strategy for the European Union*, 2010, p. 12.

[127] See for example Baldaccini, A. et al. (2008), *Controlling Security*, C&C CHALLENGE, Paris: L'Harmattan

[128] For an in-depth analysis, see González Fuster & al., Profiling in the European Union: A high-risk practice, CEPS INEX Policy Brief No.10/ June 2009; Hildebrandt, M., Gutwirth, S., eds., *Profiling the European Citizen: Cross Disciplinary Perspectives*, Dordrecht: Springer, 2008

[129] González Fuster & al., op.cit., p. 2.

the question of the relevance of the information selected to establish a profile and of the evidence available to establish that the scope of data collected to establish profiles is adequate.

- a challenge to the proportionality principle: the fact that profiling focuses on acts that might happen in the future makes it very difficult to determine, in the absence of evidence, the proportionality of the processing of personal data.
- a challenge to transparency: profiling is hardly a new practice in law-enforcement, but profiling through technologies such as data-mining limits for transparency on the decision to profile such and such person as suspicious. If based on a human decision, profiling can be accounted for in front of a court, a process that is more difficult if profiling is based on an algorithm; and
- a challenge to the right of redress: following the previous point, there is a question as to the possibility of challenging a decision based on technology-driven profiling. There is no procedure for notifying a person that s/he has been profiled. In addition, profiling as prediction does raise the question of time limits: when does a person stop being considered as suspicious? How does one challenge suspicion, and on what legal basis?

As it will be further addressed in Chapter 3, the EP initiated an attempt at establishing a definition of profiling in EU legislation. In its 24 April 2009 Recommendation to the JHA Council,[130] Parliament considers that "profiling controversially departs from the general rule that law enforcement decisions should be based on an individual's personal conduct". It suggests two definitions of profiling, the second of which is particularly relevant since it associates the issues of data-mining and profiling: profiling is framed as "a technique whereby a set of characteristics of a particular class of persons is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics".[131] The recommendation considers that a legal definition of profiling, its legitimate use and limitations, is mandatory in order to introduce the necessary data protection safeguards and mechanisms for establishing responsibility. Since profiling raises a number of concerns, including on ethnic profiling and other forms of discriminatory practices, the recommendation considers it important to adopt a set of criteria for assessing current and foreseen profiling activities. Although the Commission and the Council have not yet specifically reacted to this EP request, the updating of the EU data DPF should definitely take on this task.

2.3.2. The life of data: purpose (un)limitation and function-creep

The 'life of data' is the second set of challenges that the updated data protection framework will have to meet. It is related to the question of purpose limitation and function of existing and envisaged data processing schemes in the EU. Purpose limitation, as recalled in Chapter 1 of this study, is a fundamental principle of data protection law. It implies, among other considerations, that information systems should be built with a specific purpose in mind, and that 'function-creep' should therefore be strictly limited in order to prevent personal data from 'living on' beyond the specific purpose for which it has been collected. 'Life of data' also involves in this respect the possibility for persons to know that their data is being processed, to have access to it and be able to correct and/or apply for deletion.

[130] See European Parliament, *Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control*, (2008/2020(INI)), OJ C 184 E, 8.7.2010, pp. 119-125.

[131] Ibid, §. C.

In its 2010 overview of information exchanges in the EU, the Commission considers that "[m]ost of the instruments analysed […] have a unitary purpose": it recognises, however, that "SIS, SIS II and VIS appear to be the main exceptions to this pattern".[132] In other words, the feature of the main existing and forthcoming EU databases challenge the principle of purpose limitation. Three different aspects of this issue need to be considered: in some cases, the purpose of data systems has been explicitly extended, this even before they have been effectively implemented. In other cases, the single purpose is sufficiently vague for some systems to be considered as *de facto* multipurpose. A third element to consider here is the question of access by Member State authorities, whereby the extension of access to a given data-system can modify its original purpose.

The SIS-II and VIS are good examples here. The SIS II, firstly, has often been presented as an upgrade of the SIS established by the 1990 Convention on the Implementation of the Schengen Agreement (CISA). The development of the SIS II has however generated a number of controversies, particularly from the standpoint of DPA's. As noted by the EDPS in its March 2006 Opinion, for instance, the SIS II develops new characteristics, including wider access, new functionalities such as the interlinking of alerts, new data categories (biometrics), a new technical platform and new categories of records, reflecting a "shift of purpose of the SIS, from a control tool to a reporting and investigation system".[133] There have been a number of discussions since the SIS came online in 1995 to extend the functionalities of the database and the range of Member States authorities that should have access to it. These discussions became more intense after the 9/11 events, with certain Member States (Belgium and Germany in particular) arguing in favour of widening the access to the SIS to EUROPOL, national Prosecutors' offices, immigration and asylum authorities and developing functionalities of computerised profile searches for counter-terrorism purposes. Providing access to the SIS for security and intelligence services was also a recurrent item on the agenda, supported in particular by the United Kingdom.

These discussions form the background against which the development of SIS II, enabled by Regulation 2001/2424 and Decision 2001/886 of 6 December 2001,[134] took place. While the two instruments do not make explicit reference to this view, it was nonetheless understood that the SIS II would be developed as a 'flexible tool' that would accommodate new functionalities and purposes if needed. The Commission and Member State delegations (Germany and the United Kingdom) supported the 'flexibility option' while the European Parliament opposed it. As we will study in detail in the next Chapter, in the different reports, recommendations and resolutions it issued between 2001 and 2006, it advocated an extended role for the SIS II Joint Supervisory Body, criticised the piecemeal approach adopted by the Council with regard the development of new functionalities and the overlap in purposes (border control, immigration control, counter-terrorism, organised crime).

---

[132] European Commission, *Communication on the overview of information management in the area of freedom, security and justice*, 2010, p. 22.

[133] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final),* OJ C 91, 19.4.2006.

[134] See: Council of the European Union, Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II), OJ L 328, 13.12.2001, p. 1; Council of the European Union, Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II), OJ L 328, 13.12.2001, p. 4.

The final text of the SIS II Regulation adopted by the Council in December 2006[135] nonetheless leaves a wide margin of interpretation as to the purpose of the system (which is to ensure "a high level of security"). It also expands the reach of the system, providing for instance (Article 26) a basis for creating records on persons facing a travel ban issued by the UN Security Council. Security and intelligence services have not been granted access to the system, but Article 27(1)(b) of the SIS II Regulation introduces an ambiguity by mentioning the possibility for 'designated authorities' to access the database for purposes of coordination, thus leaving the door open to there being no limits on the purposes to which the SIS II is used. Among the issues singled out by the EDPS in its March 2006 opinion, in this regard, is the 'new vision of access' embodied in the SIS II Regulation: namely, the tendency to provide access to authorities with insufficiently specific guidelines as to how this access is related to the actions to be undertaken under one of the alerts serving the initial purpose of the system.

The story of the development of VIS presents striking similarities. There have been discussions from the onset regarding the possibility to establish an EU visa database that would not only serve the purpose of controlling the visas of travellers entering the Union, but also offer possibilities for identifying persons. The VIS Regulation[136] establishes in this regard that the VIS should serve not only in the context of visa policies, but also to facilitate the fight against fraud, and to assist in the identification of persons who may not fulfil the conditions for entry, stay or residence in the territory of the Member States (Article 2). It further includes a reference to the broad purpose of "contributing to internal security", in a similar way to the SIS II Regulation. Article 3, in this regard, envisages that VIS data can be made available, under specific conditions, for the (again, rather broad) purpose of "prevention, detection and investigation of terrorist offences and other serious criminal offences". The VIS Regulation has been 'completed' for this purpose by Council Decision 2008/633/JHA which provides for the access of EUROPOL and Member States 'designated authorities' to the system in the name of 'the fight against terrorism and other serious crimes'.[137] As such, it establishes the VIS as a *de facto* multipurpose system, where the data processed serves the EU's visa policy as much as EU and Member States internal security policies.

The Decision is furthermore problematic in at least two regards. Firstly, it defines (Article 2(c) and (d)) 'terrorist offences' and 'serious criminal offences' as the offences listed in Council Framework Decision on combating terrorism 2002/475/JHA and Framework Decision 2002/584/JHA,[138] respectively, or their 'equivalent' in national law. Since the definition of such offences is not harmonised across EU Member States, the notion of equivalence leaves open-ended the purposes for which the system can be used by Member State authorities. Secondly, the decision on which national authorities are to be designated is left to the discretion of Member States: as Article 2(e) puts it, these are "the authorities which are responsible for the prevention, detection or investigation of terrorist offences or

[135] European Parliament and Council of the European Union, Regulation (EC) No 1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, p. 4.

[136] Regulation (EC) No 767/2008, *op.cit.*

[137] Council of the European Union, Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.8.2008, p. 129.

[138] See Council of the European Union, Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), OJ L 164, 22.6.2002, p. 3; Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002, p. 1.

of other serious criminal offences", which is again vague. As one scholar has put it, this makes the VIS, beyond its initial purpose in the context of the EU's visa policy, a "general purpose intelligence tool",[139] relying on the processing of personal data including biometrics.

Purpose and function are by themselves important issues with regard data protection concerns. They also relate to a third dimension, which is the question of access to their data for persons confronted with processing, as well as correction and deletion of this data and ultimately access to effective remedies. Such issues, and particularly effective remedies, are already a concern with currently operating databases in the EU. A notorious example here is the case of Mr. Moon, leader and founder of the Unification Church and his wife who were reported as 'inadmissible' in the SIS after an initial alert introduced in the system by the German authorities in 1995 on grounds of public order.[140] The case triggered heated discussions in the courts of several Member States, including Belgium, France, Germany and the Netherlands as the Moons appealed their being reported in the SIS in several national jurisdictions. By 2007, the various alerts introduced in the SIS by Member State authorities were finally removed, but the result was obtained after 12 years of legal proceedings. The case highlights how dataveillance, if not properly framed by data protection principles, can have far-reaching fundamental freedoms and rights implications. In the Moons' case this was freedom of religion and freedom of movement: dataveillance, however, can have implications not only with regard to the right to personal data protection as such but as also with regard to the right to privacy, the right of protection against torture (in the case of refugees), the right to liberty, to family life, the prohibition of discrimination and so forth. The point to stress here is that data protection is not only important in its own terms: data processing impacts upon a wide range of rights and freedoms. Data protection constitutes a point of entry for their upholding rather than a stand-alone issue.

Upcoming and envisaged data processing schemes, in this respect, intensify concerns with access, correction and deletion. In the case of the EU-PNR proposal, for instance, these rights are not clearly specified and only include (Art.11 of the proposal) the obligation for carriers to inform passengers of the transfer of PNR to Member States law-enforcement authorities.[141] Contrarily to databases such as the SIS or Eurodac, schemes such as the 2006 DRD or the EU-PNR proposal involve the blanket collection and retention of data. As a number of high profile court cases in recent years have shown, blanket collection and retention raise a number of concerns regarding data protection. The most high profile occurrence is certainly the judgement of 2 March 2010 by the German Federal Constitutional Court that abrogated the German national implementation of the DRD. While the court chose not to refer the case to the CJEU and in fact did not question the DRD itself, it found that the national implementation law did not meet the criteria of proportionality regarding data security standards, purpose limitation, transparency, judicial control and effective legal remedies.[142] The German judgement, while notable due to the number of plaintiffs (34 000 supported by the Working Group on Data Retention *AK Vorrat*), is but one of a series of court decisions on the DRD and its implementing national legislations (including the CJEU in Luxembourg, the Bulgarian and Romanian Constitutional

[139] Brouwer, E., *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden: Martijnus Nijhoff, 2008

[140] Brouwer, E., *The Other Side of Moon: The Schengen Information System and Human Rights: A Task for National Courts*, CEPS Working Documents, No. 288, April 2008

[141] See Brouwer, E., *Ignoring Dissent and Legality: The EU's proposal to share the personal information of all passengers*, CEPS Liberty and Security in Europe, June 2011

[142] See De Vries, K. et al., *Proportionality overrides Unlimited surveillance: The German Constitutional Court Judgement on Data Retention*, CEPS Liberty and Security in Europe, May 2010.

Courts), which have all found them infringing upon fundamental freedoms and rights dispositions. On a different data processing mechanism, the ECtHR found in the *S. and Marper* case that blanket retention of fingerprint and DNA data of non convicted persons by the UK police authorities violated Art.8 ECHR because it failed to strike a fair balance between competing public and private interests.

These examples point out to several key issues that the updated EU DPF should deal with:

- Purpose in AFSJ data processing schemes, particularly with regard 'wide-spectrum' purposes such as 'serious crime' or 'terrorism', and of the association that are often made between these purposes such as the one between crime and immigration, or crime and terrorism.
- Access by authorities of the Member States: access can transform the purpose of a data-system. While it is important to take into account the diversity in the organisation of law-enforcement activities between Member States, the possibility of 'open-ended' access should nonetheless be regulated; and
- Access by data subjects: in view of the growing number of court cases involving blanket collection and retention, there is a clear need for a harmonised set of rules on access at the EU level, which should not be left to sector specific instruments but defined directly by the DPF, particularly in cases where the implementation of an EU measure is left to Member States.

2.3.3. The architecture of data: the European information model and the risk of 'information exchange by default'

The third set of challenges for data processing in the AFSJ relate to the architecture of data processing, that is to the legal, policy and technical arrangements organising the circulation of data for law enforcement purposes. The current trend is a model whereby the default position is information exchange, with data protection being reduced to a set of safeguards against gross violations of the rights of data subjects. Safeguards are important, but it is worth recalling again that the EU's objective is to establish an area of freedom and justice as much as an area of security. A key challenge facing the upgraded DPF is accordingly to reassert the centrality of data protection as a point of departure, and not as an afterthought, in data processing schemes for security purposes.

The EU security model advocated by the ISS prioritises information exchange. The ISS considers that "[t]he interoperability of different technology systems used by any agency or service must be a strategic objective so that equipment does not pose a barrier to cooperation between Member States on the sharing of information or the carrying out of joint operations".[143] The ISS further notes that efforts promoting data exchanges in EU internal security policies should be "culminating in the principle of information availability". This last principle of availability was initially established in the Hague Programme[144], the second multi-annual programme on the EU's AFSJ. Information exchanges, in this regard, have been approached as an operational and technical matter rather than as a legal issue involving the freedoms and rights of EU citizens. The IMS adopted by the Council at the end of 2009[145] exemplifies this trend. The IMS is primarily a policy document (i.e. with no formal legal value) that seeks to provide guidelines for information exchanges. It is explicitly 'business-oriented', the business side here being the agencies and bodies in

[143] Council of the European Union, *Draft Internal Security Strategy for the European Union*, 2010, p. 15.

[144] Council of the European Union, *The Hague Programme : Strengthening freedom, security and justice in the European Union*, 16054/04, 13.12.2004, Brussels.

[145] Council document 16637/09, op.cit.

charge of internal security in the Member States. 'Information management' was initially coined in the 2008 'Future of European Home Affairs Report' of the eponymous informal high-level group. The IMS itself was proposed by the incoming Swedish Presidency in June 2009[146], and developed by the Council's Ad Hoc Working Group on Information Exchange.

The IMS considers information management as "functionally defined, i.e. depends on the task to be carried out, as opposed to competence-based or organisationally defined". In other words, information management is not a legal principle as such, and is not considered to have any legal effects. The IMS defines eight 'focus areas', where data protection comes in third position. The section dedicated to this focus area, however, clearly prioritises so-called 'business needs': "Personal privacy as well as business security have to be ensured, while providing for business needs to use and share information". In the meantime, it reduces considerations of data protection to the question of data security, considering that "a high level of security will protect business interests as well as citizens' private lives, without reducing the availability of information, so that correct information is available to authorised users in a traceable way, when needed and permitted by existing legislation".[147] As recalled by the EDPS in a July 2009 intervention at the behest of the Swedish Presidency, data security is indeed a data protection principle, but it is embedded within other concerns such as legitimate purpose and legitimate access[148]. Data security, however, is the only principle of data protection explicitly addressed by the IMS, which considers it as a key component for "enhanced trust in these areas between competent authorities" and thus as "an important step towards an attitude of data-sharing by default".

The IMS points out to a broader issue here: the legal standing of principles such as availability and interoperability, and the development of a data protection take on technical questions such as the architecture of data systems. The two questions are interrelated, insofar as availability and interoperability both reflect an effort to find a technical (and technological) solution to what is ultimately a political problem, namely the extent to which personal data is being processed (including exchanges) in the context of the internal security policies of the EU and its Member States and the means available to protect the fundamental rights and freedoms of individuals in this regard.

Interoperability is a technical option enabling collaboration between law enforcement agencies on the basis of specific requests.[149] In its 2005 communication on European databases in the AFSJ, the European Commission defines interoperability as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge".[150] Availability goes beyond interoperability. As defined in the Hague programme, availability involves that "throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and […] the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirements of ongoing investigations in that State".[151]

---

[146] Council of the European Union, *Proposal for an EU Information Management Strategy for Justice and Home Affairs*, 11312/09, 26.6.2009, Brussels.

[147] Council of the European Union, *Draft Council Conclusions on an Information Management Strategy for EU internal Security*, 2009, p. 10.

[148] Hustinx, P., *Data Protection and the need for an EU Information Management Strategy*, Council Ad Hoc Working Group on Information Exchange Reception by Swedish Presidency, Brussels, 6 July 2009.

[149] Bigo, D., *The principle of availability of information*, PE 378.272, January 2006.

[150] European Commission, *Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597 final, 24.11.2005, p. 3.

[151] Council of the European Union, *The Hague Programme*, 2004, p. 18.

Availability is a general measure and does not allow for any discretionary margin for manoeuvre for Member States law enforcement bodies and agencies. Availability, however, presupposes a degree of proximity in the respective remits of these bodies and agencies, and a shared understanding of the categories of data that are being exchanged. This is far from being the case: the understanding of 'law enforcement' and its organisation varies significantly from one Member State to the other, and so does the legal definition of offences involving the creation of a record in a database. In the absence of a legal harmonisation of data categories, availability challenges the principles of legitimate access and legitimate purpose. As such, the notion that EU information management can be defined functionally without references to the competencies of the agencies and bodies exchanging information and their organisation, as advocated in the IMS, is problematic. There is therefore a need of legal clarity from a data protection point of view as to such broad principles as availability and interoperability.

This need is enhanced by the current tendency to consider the technical organisation of data systems as providing by themselves guarantees that data protection principles are upheld. The argument surfaces in the European Commission's 2010 assessment of information management in the AFSJ. The services of DG Home Affairs point out that "a single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing. Creating such a system would, however, constitute a gross and illegitimate restriction of individuals' rights to privacy and data protection and pose huge challenges in terms of development and operation. In practice, policies in the area of freedom, security and justice have developed in an incremental manner, yielding a number of information systems and instruments of varying size, scope and purpose. The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' rights than any centralised alternative".[152]

The technical architecture of data processing has undeniably a role to play in upholding data protection principles: hit/no hit systems such as the SIS are more protective of individuals' fundamental freedoms and rights than data processing schemes involving blanket collection and retention or bulk data transfers, and the same can be said of 'push' systems over 'pull' systems for instance. Decentralisation and compartmentalisation, however, are not by themselves enough of a guarantee with regard data protection. Convergence can happen without centralisation. The non-systematic networking of different information systems occurring under principles of unclear legal value such as 'availability' or 'interoperability' can lead to potential breaches of the principles of legitimate purpose and access. One issue already mentioned is when availability and interoperability enable access by national services deemed 'equivalent' but whose remits are nonetheless different, a situation that can lead to data being used for different purposes. Additionally, different forms of technical integration can challenge data protection. The Commission envisaged already in 2005 that "the development of a service-oriented architecture of European IT systems would help maximise synergies"[153] between various European data systems. At the moment, Eurodac, VIS and SIS-II share the European Commission's s-TESTA secure communication system and Biometric Matching System (BMS). Following on the 'Swedish Initiative' of 2006 and the Prüm Decision of 2008, the Ad Hoc Group on Information Exchanges has conducted work on messaging formats for EU law enforcement, with the aim of developing a European-wide Universal Messaging Format (UMF). Other technical

[152] European Commission, *Communication on the overview of information management in the Area of Freedom, Security and Justice*, 2010, p. 3.

[153] European Commission, Communication, on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, 2005, p. 10.

developments include work on so-called 'service-oriented architectures' (SOA) which makes services available to different IT systems, irrespective of the platform they are based on.[154] In the current context of emphasis on 'data sharing by default', such developments can lead to overemphasise the technical aspects of data processing to the detriment of legal and political considerations.

There seems to be a need, in this regard, to reaffirm the positive dimension of data protection. Data protection should not be considered only as a set of safeguards needed to match technical developments, but should provide a framework within which technical developments take place. In view of the reluctance of the European Commission and the Council to give legal contents to availability and interoperability, the updated EU DPF should definitely account for them from a legal, data protection oriented point of view.

2.3.4. Technology, intelligence-led policing and EU inter-agency cooperation in the AFSJ

The last set of challenges for data processing in the AFSJ involves EU Home Affairs agencies, some of which have become data controllers in their own terms, and cooperation between them. This is particularly the case of EUROPOL through its TECS and it seems to be the case now of FRONTEX. Another development, which will be scrutinised here, is the establishment of a European agency for the operational management of large-scale IT systems.

A key issue is that through the emphasis placed on 'intelligence-led' forms of policing, the work of EU agencies in the field of AFSJ is increasingly leaning towards dataveillance,. As noted in Chapter 1, this is largely due to the fact that EU agencies have not been granted direct executive powers by the Member States: their core remit consists in 'coordinating' the operational activities conducted by the law-enforcement authorities of Member States, out of which the transfer and analysis of data constitutes a core 'business'. The situation follows from the emphasis placed by Member State authorities on their exclusive competence over matters of internal security. Conferring upon EU agencies a remit limited to coordination, to the facilitation of data exchanges and the provision of some analytical documents based on information initially circulated to them by Member State law enforcement agencies, bodies and services ensures that this exclusive competence remains in place by enforcing an information monopoly in favour of national law enforcement services.

The management of EUROPOL and FRONTEX, accordingly, have been particularly keen on obtaining access to personal data over the past few years. This trend is reinforced by the emphasis placed on 'intelligence-led' security policies in recent EU documents. In the above-mentioned 2009 Stockholm programme, the European Council calls on the European Commission and the Council to develop an ISS that would be "the reflection of a proactive and intelligence-led approach". Technology is considered as an essential component of such an approach. In the case of integrated border management, for instance, the ISS highlights that the "further development of the Schengen Information System as well as electronic border-control systems, such as an entry-exit system, will contribute to intelligence-led integrated border management". The question in this respect is on the role of data protection and of the upcoming EU DPF as to these trends.

Cooperation among EU home affairs agencies is a high-profile policy issue. Following the informal Justice and Home Affairs (JHA) ministerial meeting of 1 October 2009, the Swedish presidency tasked EUROPOL with drafting a report on cooperation between EU home affairs agencies. An interim report was forwarded to the JHA Council and COSI on 29 January

[154] On architecture and infrastructure of IT systems in the field of law enforcement, see also the Common Requirements Vision elaborated by the Conference of the Chief Information Officers of EU Member States police forces, circulated to CATS in March 2008 (Council document 7758/08).

2010, and the final report to the same two bodies on 9 April 2010.[155] Data processing is not presented as an explicit component of cooperation between the agencies. The report does advocate, however, the establishment of bilateral secure communication channels for the exchange of information between EUROJUST, EUROPOL and FRONTEX, which would be conducive to the circulation of personal data. The most important element appears in the section on multilateral cooperation, which recommends in particular "harmonised provisions in the agencies' legal framework" and singles out the impossibility for FRONTEX to process personal data considered as a limitation to full operational coordination.

The independent evolution of each agency also gives an indication of how crucial the processing of personal data has become for EU internal security agencies. EUROPOL and FRONTEX are central here. The case of EUROPOL has already been mentioned in previous sections. Through the TECS and its different components, the agency is currently processing personal data. Access to SIS-II and VIS is foreseen, and access to Eurodac has been discussed at some length. The EU-US TFTP agreement has further led to EUROPOL's involvement in the blanket collection and processing of the financial data of EU citizens, and the EU-TFTP initiative, should it develop further, would reinforce this trend. An important point to consider in the context of cooperation between EU agencies is Article 22 of the EUROPOL Decision[156] which envisages the possibility for the Office to conclude agreements or working arrangements with other Community institutions, bodies, offices and agencies including (but not limited to) EUROJUST, the European Anti-Fraud Office (OLAF), FRONTEX, the European Police College (CEPOL), the European Central Bank (ECB) and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). Article 22(2) opens up the possibility that such agreements or arrangements might include the exchange of personal data.

The case of FRONTEX is possibly more telling insofar as the current evolution of work among EU home affairs agencies is concerned. The agency was initially barred from having access to data processing schemes such as the SIS.[157] Article 11 of the FRONTEX Regulation[158] establishes that the agency "may take all necessary measures to facilitate the exchange of information relevant for its tasks with the Commission and the Member States", but since its remit does not include border control *per se*, direct access to personal data in the conduct of the agency's work is not foreseen. One needs to distinguish in this regard access to information that is not associated with a specific individual from access to personal data. Since its inception, FRONTEX has had access to statistical data circulated through the Centre for Information, Discussion and Exchange on the Crossing of Frontiers and Immigration (CIREFI) ICONet information system. Following the entry into force of the Lisbon Treaty and COREPER's decision to modify the working structures of the Council in the field of JHA,[159] the functions of CIREFI and the management of ICONet have been transferred to the agency,[160] who has now control over most of the statistical information

[155] See Council of the European Union, *Interim Report on Cooperation between JHA agencies,* 5816/10, 2.2.2010, Brussels; Council of the European Union, *Final report on cooperation between JHA Agencies*, 8387/10, 9.4.2010, Brussels.

[156] Council of the European Union, *Decision of 6 April 2009 establishing the European Police Office (2009/371/JHA)*, OJ L121, 15.5.2009, p. 39.

[157] See Jeandesboz, *op.cit.*, 2008.

[158] Council of the European Union, *Regulation (EC) No 2007/2008 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union*, OJ L 349, 25.11.2004, p. 1.

[159] Council of the European Union, *Implications of the Treaty of Lisbon provisions for the JHA working structures*, 17653/09, 16.12.2009, Brussels.

[160] Council of the European Union, *New JHA working structures: Abolition of CIREFI and transfer of its activities to FRONTEX and the Working Party on Frontiers*, 6504/10, 22.2.2010, Brussels.

on irregular migration generated at the EU level and distributes it in the framework of the FRONTEX Risk Analysis Network (FRAN). The key body within FRONTEX, in this regard, is the agency's Risk Analysis Unit (RAU). RAU Sector 1 is tasked with collecting via ICONet statistical data from Member States on a monthly basis, as well as other information considered relevant (e.g. incident reports regarded by a sending Member State as particularly relevant). RAU Sector 2 ("Operational Analysis and Evaluation") receives information collected during Joint Operations. The main channel for the collect of data through RAU S2 is the FRONTEX Situation Center (FSC), which receives statistical information and incident reports from Member States involved in a joint operation on a daily basis. Information collected during joint operations by the FSC is also forwarded to the agency's unit in charge of operations (Joint Operations Unit, JOU).

Access to personal data, however, is another matter, and one that has been consistently pursued by the agency's management over the past few years.[161] In the meantime, the provision on exchange of data under Article 11 of the FRONTEX Regulation has been the subject of a number of controversies. In a 2008 memoir transmitted to the House of Lords, for example, the UK-based Immigration Lawyers Practitioners' Association (ILPA) indicated that 'Particular attention should be given to whether the institutional and legal framework ensures accountability of FRONTEX on matters of data protection. There is no Data Protection framework for FRONTEX. Article 11 of Regulation 2007/2004/EC is very much an enabling provision and does not spell out constraints'.[162] Subsequent developments, however, showed that the scope of Article 11 of the FRONTEX Regulation was not the only area where access to and processing of personal data by the agency could take place. Such access has been requested, in fact, in the context of the organisation of joint return operations (Article 9 of the FRONTEX Regulation). In April 2009, the agency's Data Protection Officer forwarded to the EDPS a notification for prior checking on the "Collection of names and certain other relevant data of returnees for joint return operations (JRO)". The purpose of the collection was, among others, to have knowledge of the numbers and identification of returned persons, to provide airline companies with a passenger list and ascertain their degree of 'risk', health status as well as their age.[163] The EDPS considered that Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies was applicable in this case. While the processing was found lawful, the opinion nonetheless points out that Article 9 of the FRONTEX Regulation and Article 5(a) of Regulation 45/2001 could only serve as a provisional legal base and called for a more specific one to be adopted. The episode does suggest that the agency has been processing personal data for some time without a clear notion of whether it had the legal basis to do so.

The EDPS' opinion on the processing of personal data by FRONTEX in the context of JROs falls in the broader context of the revision of Regulation 2007/2004 establishing the agency, on which the Council and Parliament have recently found a political agreement.[164]

---

[161] See for instance the hearing of General Ilkka Laitinen, executive director of FRONTEX, in front of the UK House of Lords' Select Committee on European Union in October 2007. House of Lords European Union Committee, *FRONTEX: the EU external borders agency – Report with evidence*, 9th Report of Session 2007-2008, HL Paper 60, 5 March, London.

[162] Ibid, p. 110.

[163] See European Data Protection Supervisor, *Opinion on a Notification for Prior Checking received from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) concerning the "Collection of names and certain other relevant data of returnees for joint operations (JRO)"*, 26 April, Brussels 2010.

[164] Council of the European Union, *Strengthening the European external borders agency Frontex – Political agreement between Council and Parliament*, 11916/11, 23.6.2011, Brussels. At the time of

The processing of personal data is among the options considered by the European Commission, and has been recommended by the agency's management board. The Commission's initial proposal for the revision of the Regulation leaves the issue out for later consideration in the context of the strategy for information exchange and of the strategy for cooperation among EU agencies.[165] In any case, the impact assessment attached to the proposal rules out the possibility for FRONTEX to process, store, collect and transfer all personal data gathered by participants to its joint operations that was advocated by some Member States and the agency.[166] It does, however, point out that the collection of personal data on so-called 'facilitators' for the purpose of risk analysis would be envisaged, in the name of 'a pro-active stance' regarding this issue. The point proved controversial in several respects. On the one hand, some Member States requested during the first reading of the European Commission's proposal for amending Regulation 2007/2004 in the Frontiers Working Party, a clarification from the Commission representatives regarding the exact scope of such data processing. The Commission representatives specified that 'this Article does not aim at changing FRONTEX mandate and at creating an alternative system to the Schengen information system'.[167] The request highlights that even in a context where the Frontiers Working Party was mostly favourable to the introduction of a provision enabling FRONTEX to process personal data, concerns with regard the predominance of national competence in the conduct of border checks, of which the SIS is a cornerstone, remained strong. On the other hand, the EDPS expressed concern over this question, pointing to the Prior Check Opinion issued on FRONTEX JROs. In its opinion on the European Commission's proposal, it underlined that the Commission's approach "could lead to an undesirable legal uncertainty and a significant risk of non-compliance with data protection rules and safeguards".[168] The EDPS advocated the clear spelling-out of provisions regarding the processing of personal data by the agency.

The LIBE Committee rapporteur for the proposal on the revision of Regulation 2007/2004 establishing FRONTEX took up the issue and it is at the behest of the European Parliament that an amendment regarding the processing of personal data has now been introduced in Article 11 of the FRONTEX Regulation[169] (for further details, see Chapter 3 below). This will

completion of this study, the political agreement over the final text by the Council is expected to take place on 22 September 2011 during the JHA Council meeting, and is not yet available.

[165] European Commission, *Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, COM(2010) 61 final, 24.2.2010, Brussels

[166] European Commission, *Impact Assessment accompanying the Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, SEC(2010) 149 final, 24.2.2010, Brussels, p. 34-35

[167] Council of the European Union, *Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 8466/10, 3.5.2010, Brussels, p. 3.

[168] European Data Protection Supervisor, *Opinion on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union*, 17 May, Brussels, 2010, p. 4.

[169] See: European Data Protection Supervisor, *EDPS' comments on Amendment 59 in the Draft report on the Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)(COM(2010)0061 – C7-0045/2010-2010/0039(COD))*, 3 December 2010, Brussels.

enable the agency to collect, analyse, but also exchange with EUROPOL (see new Article 11(5) of the amended proposal): First, data of persons suspected on reasonable grounds of involvement in cross-border criminal activities, illegal migration activities or human trafficking activities as defined in Article 1(1) (a) and (b) of Council Directive 2002/90/EC; second, data of persons who are victims of such activities; and third, data of persons who are subjects to return operations.

The negotiations between the European Parliament and the Council and the political agreement reached on 23 June 2011 have confirmed that the agency would be entrusted with the processing of personal data. The Council's press release specifies that the amended FRONTEX Regulation would include 'the possibility to transfer personal data to EUROPOL or other EU law enforcement agencies regarding persons suspected of involvement in cross-border criminal activities, facilitation of illegal immigration activities or in human trafficking activities'.[170]

This shift illustrates the centrality of data processing for the EU home affairs agencies. It does, in the meantime, raise a question about the standing of data protection in EU internal security policies. Here, concerns about FRONTEX' compliance with data protection safeguards have led to the authorisation of data processing activities. The assumption underpinning the reasoning of the EDPS in support of authorising the agency to process personal data – namely, that the absence of such provisions might lead to unlawful data processing by the agency – raises strong concerns as to the relation between the activities of EU home affairs agencies and rule of law principles such as those of accountability and transparency.

One last development needs to be scrutinised regarding EU agencies in charge of data processing activities in the AFSJ: the establishment of a European agency for the operational management of large-scale IT systems, on which Council and Parliament have recently found a political agreement.[171] The Commission initially submitted (June 2009) a legislative package composed of a proposal for a Regulation of the European Parliament and of the Council establishing the agency with a first pillar legal base, and a proposal for a Council Decision regarding the operational management of SIS II and VIS falling under Title VI TEU (third pillar). The package was re-submitted following the entry into force of the Lisbon treaty as a single amended proposal for a Regulation. According to the latest version of the Regulation (pending the approval of Parliament), the agency is to be responsible for the management of SIS-II, VIS and Eurodac (Article 1(0a)). It would take over the responsibilities of the Managing Authority established by the SIS-II and VIS Regulation, as well as the management tasks conferred upon the Commission by the Eurodac Regulation. The agency would also be tasked with the "preparation, development and operational management of other large-scale IT systems" (Article 1(0b)). This forward-looking remit demonstrates that the establishment of this agency echoes the outlook of policy-making regarding technology that have been highlighted so far. It will not only contribute to the proper management of existing systems, but will potentially serve as the platform to launch additional initiatives.

[170] Council of the European Union, *Strengthening the European external borders agency Frontex*, 2011, p. 2.

[171] Council of the European Union, *EU agency for large-scale IT systems*, 11337/11, 9.6.2011, Luxembourg. For the compromise text, see: Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Possible agreement with the EP*, 10827/1/11, 6.6.2011, Brussels.

One satisfaction tied with the establishment of the agency is the decision-making sequence, which has avoided two problematic temptations from the point of view of democratic accountability and data protection. The first one would have been to establish the agency as an executive agency, based on a decision by the European Commission. The choice of a regulatory body has enabled the participation of Parliament in line with its new attributions following the entry into force of the Lisbon treaty. The second temptation would have been to entrust the management of SIS II, VIS and Eurodac to EUROPOL and/or FRONTEX, an option that had been foreseen by the European Commission and that would have created tensions due to the interest manifested by the two bodies in the processing of personal data. Two issues of concern nonetheless remain in terms of data protection:

- The first one relates to the question of the architecture of data discussed in the previous section of this Chapter. Placing the three main databases at EU level under the remit of a single entity, in a context where EU policies regarding data processing emphasise the notion of interoperability, raises a few questions. The point was made by the EDPS in his December 2009 opinion on the Commission's initial legislative package, but is met in the current version of the proposed regulation by Article 1(0c) which states that the systems falling within the remit of the agency "shall not exchange data and/or enable sharing of information and knowledge, unless provided for in a specific legal basis". Technical function creep is ruled out, but the agency offers the possibility to enable interoperability, with all the reservations linked to this notion; and
- The possibility for the agency to prepare, develop and manage additional large-scale IT systems. The definition of what such systems might be is absent from the text as it currently stands, whereas this was a pending issue pointed out by the EDPS. Are large-scale IT systems limited to centralised databases on the model of SIS II, VIS and Eurodac? Will the agency be entrusted with the management of so-called decentralised data processing schemes such as the Prüm system or ECRIS?

The establishment of the agency for the operational management of large-scale IT systems, in sum, highlights two trends:

- The continued emphasis on technology, and particularly data processing, as a central component of EU AFSJ policies, and the increasing role of EU home affairs agencies as data controllers. The agency's forward-looking remit on the preparation and development of large-scale IT systems in addition to SIS II, VIS and Eurodac stresses the open-endedness of current policy practices in this area, a point that is also highlighted by the modification of the FRONTEX regulation; and
- The possibility for the European Parliament to play a role in the evolutions of the AFSJ. Both the modification of the FRONTEX Regulation and the establishment of the large-scale IT systems agency have seen the involvement of the European Parliament, in stark contrast with some of the other developments assessed in this chapter. The following chapter will discuss this matter more in-depth, but let us stress already here that the updating of the EU DPF is also an opportunity to examine how the EP can play a role in the increasing use of technology for law enforcement purposes, and one that can support the principles and values it has constantly upheld over the past decade in this framework.

3. THE EP'S ROLE IN FRAMING EU DATA PROTECTION AND PRIVACY POLICIES

KEY FINDINGS

- The EP has played a major role in the construction of the right to the protection of personal data as an autonomous fundamental right in the EU, and in its recognition in a legally binding instrument, namely the EU Charter. Until now, however, it has relied only very timorously on the specificity of this innovative right, owing to the lack of a comprehensive understanding of its nature or of political will (or both), generally framing the impact of data processing practices in terms of mere privacy infringements. Historically, the EP has been the main advocate of the adoption of EU legislation on the protection of personal data.
- The EP's contribution to the framing of EU data protection and privacy policies offers a picture of where institutional and substantial concerns are intrinsically linked. Many data protection and privacy controversies in which the EP has played an active role also mirror inter-institutional tensions, be it in relation to the applicable legislative procedure, the division of competences through 'comitology' or the powers linked to the conclusion of international agreements.
- There is no linear relationship between more involvement of the EP in decision-making, on the one hand, and a higher level of personal data protection granted to individuals, on the other. On the contrary, sometimes the strengthened participation of the EP in legislative procedures has led to a lowering of data protection and privacy standards.
- Over the years, one of the main priorities for the EP has been to call for the reinforcement of data protection standards in the field of police and judicial cooperation in criminal matters (the old EU third pillar). The EP has commonly portrayed this as a precondition for the deployment of a series of data processing initiatives that it eventually supported. The entry into force of the Lisbon Treaty has provided the EU with a new legal basis allowing for the adoption of a legal instrument on data protection to apply also in this field. It remains to be seen whether the EP will seize the opportunity to push still more vigorously for the strengthening of protection in the former third pillar, as demanded for so long.
- Another recurrent concern of the EP in the field of data protection, privacy and EU security policies has been the issue of profiling through predictive data-mining. The relations of the EP with other EU actors are intricate. It is relatively close to the 'liberty EU agencies' relevant in the data protection area, such as the WP29 and the EDPS, but it can also depart from their positions. The added value of the opinions of the FRA for the EP's stance in this particular field is not yet clear.
- Despite its formal commitment to the assurance and promotion of fundamental rights in the EU, as well as its different initiatives contributing to the assurance of the rights to data protection and privacy, the EP has not yet effectively questioned the factors underpinning the development of measures that threaten them the most: notably, the modern transformations of policing and their connection with AFSJ policies, and the progressive design of an increasingly opaque web of data exchanges among EU agencies and from these nodes to the authorities of the Member States, as well as third countries.

What has traditionally been the role of the European Parliament in shaping EU data protection and privacy policies, in particular in the AFSJ? What have been the EP's main concerns, and how has it proceeded to bring them to the fore? Has the entry into force of the Lisbon Treaty affected its position in these debates? This chapter examines the EP's

contribution to assuring the protection of personal data and privacy in the AFSJ, from the perspective of the continuous development of EU security policies having a heavy impact on these rights.

The chapter first focuses upon the initial steps of EP involvement in this area. Second, it describes the EP's positions and actions in the context of six substantive themes that have acquired major relevance over the years: the systematic processing of travel data for law enforcement purposes; the processing of financial data in the context of antiterrorism through TFTPs; the adoption and implementation of the DRD; the design of large-scale databases, such as the new Schengen Information System II (SIS II) and the VIS; the processing of personal data by FRONTEX, and the deployment of 'body scanners' at airports across the EU. In doing so, it studies the EP's relations with EU (liberty) agencies and bodies, the mechanisms relied upon by the EP to voice its concerns and the nature of such concerns. Third, the chapter discusses the different features of the EP's involvement in the area to assess their potential and their limitations.

3.1. The genealogy of the EP's involvement in data protection

The EP has historically played a major role in advancing the protection of personal data in the EU. It has been an active supporter of the adoption of EU legal instruments on personal data protection even when EU competence to legislate in the area was strongly contested, and has repeatedly fought for the establishment of a solid data protection legal framework across EU pillars; it has been an instrumental actor in the recognition of personal data protection as an autonomous fundamental right in the EU Charter, and consistently advocated the acknowledgement of its binding force. Moreover, it has systematically promoted the EU's accession to the ECHR, which protects individuals against the processing of data relating to them through its Article 8 on the right to respect for private life.

3.1.1. A background of fundamental rights defence and promotion

The support granted by the EP to the development of EU data protection must be put into the perspective of the EP's commitment to fundamental rights protection in the EU in general. This commitment originally translated into both supporting the adoption of an EU-specific catalogue of fundamental rights, on the one hand, and championing accession to the ECHR, on the other, as parallel but concomitant paths for reinforced safeguarding.

The EP was the initiator of the Joint Declaration signed on 5 April 1977 together with the Council and the European Commission, affirming that they would do their utmost to protect the fundamental rights enshrined in both the constitutions of the Member States and in the ECHR.[172] On 14 February 1984, the EP adopted a draft EU Treaty, also known as the 'Spinelli draft',[173] which foresaw a five-year period for the EU to take a decision on accession to the ECHR and to adopt its own declaration on fundamental rights.[174]

On 12 April 1989, a Declaration of Fundamental Rights and Freedoms was adopted by the EP. It listed what the EP regarded as the EU fundamental rights and freedoms derived from the Treaties establishing the European Communities (EC), the constitutional traditions common to the Member States, the ECHR and the case law of the CJEU. The list of rights did not include any reference to the protection of personal data, but under Article 6, it presented an inventive construal of the right to privacy, including an explicit mention of the right to identity.[175] On 10 February 1994, the EP endorsed a Resolution noting with

[172] Joint Declaration by the European Parliament, Council and the Commission concerning the protection of fundamental rights and the ECHR, Luxembourg, 5 April 1977, OJ C 103, 27.04.1977, pp. 1-2.

[173] Draft Treaty establishing the European Union (14 February 1984).

[174] Art. 4(3) of the Draft Treaty establishing the European Union (14 February 1984).

[175] Art. 6 of the Declaration established that: "1. Everyone shall have the right to respect and protection for their identity. 2. Respect for privacy and family life, reputation, the home and private correspondence shall be guaranteed."

satisfaction the work carried out by an internal committee, namely the Committee on Institutional Affairs, which had resulted in a draft Constitution for the EU with its own list of the 'human rights' perceived as being guaranteed by the EU. Such a list introduced a revised version of the 1989 Article 6 on the right to privacy, now expanded with a reference to judicial authorisation as a condition for surveillance by public authorities.[176] But there was still no mention of the right to the protection of personal data as such. Nevertheless, in 1998 the LIBE Committee mentioned almost incidentally in its Annual Report on respect for human rights in the EU that the right to the protection of personal data was a fundamental right "which States are required to uphold".[177]

The efforts to provide the EU with its own modern instrument of codified fundamental rights entered a new phase as work towards the Charter of Fundamental Rights of the EU was launched. In a Resolution of 16 September 1999, the EP welcomed the decision taken at the Cologne European Council to proceed with drawing up a draft Charter of Fundamental Rights, and explicitly highlighted "the need for an open and innovative approach to...the nature of the rights to be featured in it".[178] The EP was directly involved in the European Convention drafting the Charter with a delegation of 16 representatives. During the drafting period, the EP issued a Resolution underlining that the Charter should become a binding legal instrument[179] and that it should be "innovative in nature" by giving legal protection in respect of new threats to fundamental rights, for example from the field of information technology.[180]

The draft of the Charter was officially concluded on 2 October 2000, incorporating a full article on the protection of personal data (Article 8). On 8 October 2000, the EP Committee on Constitutional Affairs insisted on the position according to which the Charter should be incorporated into the Treaties and thus acquire binding force.[181] On 14 November 2000 the EP assented to the Charter draft, leading to its formal proclamation by the leaders of EU institutions on 7 December 2000 in Nice. This formal proclamation, however, did not grant the EU Charter any mandatory force. During many years, the EP regretted the EU Charter's unsettled status, calling for its content to be enforceable before the courts[182] and promoting a refined approach for considering throughout the legislative process the rights it recognises.[183] The entry into force of the Lisbon Treaty in December 2009 finally gave binding force to the text. Already in November 2009, in its Resolution on the Stockholm

[176] Art. 6 of Title VIII of the 1994 Draft Constitution, titled "Privacy", read as follows: "(a) Everyone has the right to respect and protection for his or her identity. (b) Respect for privacy and family life, reputation, the home and private communications shall be guaranteed. (c) Surveillance by public authorities of individuals and organizations may only take place if duly authorized by a competent judicial authority."

[177] European Parliament, *Annual Report of 2 December 1998 on respect for human rights in the European Union*, PE 228.192/final, 1997 § 23.

[178] European Parliament, *Resolution of 16 September 1999 on the establishment of the Charter of Fundamental Rights*, OJ C 54, 25.2.2000, p. 93, § 3.

[179] European Parliament, *Resolution of 16 March 2000 on respect for human rights in the European Union* (1998-1999) (11350/1999 - C5-0265/1999 - 1999/2001(INI)), A5-0050/2000, § 7(a).

[180] Ibid., § 7(h).

[181] European Parliament, Report of 8 October 2000 of the Committee on Constitutional Affairs on the impact of the Charter of Fundamental Rights of the European Union and its future status (2002/2139(INI)), PE 313.401.

[182] See, for instance European Parliament, *Resolution of 23 October 2002 on the impact of the Charter of Fundamental Rights of the European Union and its future status*, (2002/2139(INI)), C 300 E/432, 11.12.2003, pp. 432-437.

[183] In this sense: European Parliament, *Resolution of 15 March 2007 on compliance with the Charter of Fundamental Rights in the Commission's legislative proposals: methodology for systematic and rigorous monitoring*. The Resolution alludes to "*the protection of private life*" as one of the fundamental rights that could benefit from making a prior assessment of the impact of EU legislation (Recital I).

programme,[184] the EP unambiguously referred to "the fundamental rights dimension of data protection and the right to privacy".[185]

During all these years, the EP also called for the EU's accession to the ECHR.[186] In a Resolution of 15 December 1993 on the relations between the EU and the Council of Europe, it argued that it was "both desirable and necessary".[187] On 18 January 1994, it adopted an ad-hoc Resolution[188] calling for the Council to authorise the European Commission to negotiate with the Council of Europe on accession arrangements,[189] while underlining that this should be envisaged as complementing the adoption by the EU of its own Declaration of Human Rights and Fundamental Freedoms.[190] It was only with the Lisbon Treaty that the EU was finally to incorporate a legal basis allowing for the accession.

The EP's historical contribution to the promotion of fundamental rights was also marked by the creation of the Committee on Civil Liberties and Internal Affairs ('LIBE Committee') in 1992, as the Maastricht Treaty instituted the pillar structure of the EU and established a third pillar with a distinct intergovernmental nature. Since 1993, the LIBE Committee has produced numerous reports on the respect for human rights within and outside the EU, leading to EP resolutions on the subject. Additionally, the EP upheld the creation of the Fundamental Rights Agency (FRA) as an important element of a reinforced EU strategy for the assurance and protection of fundamental rights.[191]

3.1.2. The EP and the design of EU data protection

The EP can be described as the instigator of EU legalisation on the protection of personal data and one of its main architects. Historically, it was the first European institution to explicitly call for the European Communities to legislate on the subject – and for almost two decades was the only one.

Since the beginning of the 1970s, both the EP and the European Commission have been concerned with the dominance of non-European companies in the growing European market for data processing.[192] In 1973, the European Commission advised the Council to devise systematic support for the commercial development of data processing for commercial applications, while at the same time noting that 'social problems' were to arise from such a policy, and recommending that a series of public hearings on the matter be arranged.[193] In subsequent years, a Community policy in the area was indeed developed by the European

[184] European Parliament, *Resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme*, P7_TA(2009)0090.

[185] Idem, § 83.

[186] See also European Parliament, *Resolution on the impact of the Charter of Fundamental Rights of the European Union and its future status*, (2002/2139(INI)),23 October 2002, already mentioned.

[187] European Parliament, *Resolution of 15 December 1993 on relations between the Union and the Council of Europe*, OJ No C 20, 24.01.94, pp. 44-46, § 12.

[188] European Parliament, *Resolution of 18 January 1994 on Community accession to the European Convention on Human Rights*, OJ C 44, 14.02.94, pp. 32-34.

[189] Ibid., § 9.

[190] Ibid., § 13.

[191] See, in this sense: European Parliament, *Resolution of 26 May 2005 on promotion and protection of fundamental rights: the role of national and European institutions, including the Fundamental Rights Agency*, (2005/2007(INI)), P6_TA(2005)0208.

[192] See, for instance, European Commission, *The European Community and Data Processing -- Government Development Aids Permitted*, Information [Competition] 21/72, 1972

[193] See European Commission, Communication by the Commission of the European Communities concerning a Community policy for data processing: Information Memo P-63/73, November 1973: and European Commission, Community Policy on Data Processing: Communication of the Commission to the Council, SEC (73) 4300 final, 21 November 1973.

Commission and the Council, but with practically no reference whatsoever to the alluded 'social problems' related to the commercial expansion of data processing.[194]

In the meantime, different European and non-European countries had started to consider, draft or even adopt laws on personal data protection. In 1970, the first-ever law on data protection was enacted by the German Land of Hessen; 1973 witnessed the adoption of the first national legislation on data protection, in Sweden (the 'Data Lag') and 1974 was the year in which the US passed the Privacy Act.[195] Additionally, international and European organisations were energetically working towards the elaboration of ad-hoc legal and policy instruments: the Organisation for Economic Co-operation and Development (OECD) Council was to approve a Recommendation concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980; and the Council of Europe adopted its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') in 1981.

In contrast to this effervescence of global regulation, and much to the regret of the EP, the European Commission kept a distance from the issue. By 1975, the EP had already started to plea for the preparation of a directive on what was designated at the time as 'individual freedom and data processing'.[196] With a Resolution of 8 April 1976, the EP requested the European Commission to draft legislation on "the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing",[197] a right later to be known as the right to the protection of personal data. To work on the file, a Subcommittee on Data Processing and the Rights of the Individual had been set up by the EP Legal Affairs Committee, whereas the European Commission established a Working Party on Data Processing and Protection of Liberties. A new Resolution was adopted by the EP in May 1979, this time advocating the creation of a "genuine common market in data-processing", calling for the drafting of a Directive harmonising legislation on data protection, and listing principles to be used as basis for the effort.[198] The 1979 Resolution also introduced the idea that representatives of bodies responsible of data protection at the national level should work together to supervise the implementation of an EC data protection law[199] (a pioneering suggestion, which eventually led to the establishment of the WP29) and that the EP should chair such a committee[200] (a vision later abandoned).

Following the adoption of the Council of Europe's Convention 108, the European Commission asserted in 1981 that in its view, the Convention was an appropriate instrument for the purpose of creating a uniform level of data protection in Europe[201] and therefore no legislative proposal from its side was needed. The EP, however, on the basis of the limited number of Member States that complied with the instrument, was unconvinced by the argument, and in March 1982 the EP again expressed that it considered the adoption of a Directive worthy of consideration.[202]

---

[194] See, for instance, European Commission, *Community Policy for Data-processing*, COM(75) 467 final, Brussels, 1975

[195] Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, Dec. 31, 1974.

[196] European Parliament, *Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, OJ C 60, 13.3.75, pp. 48.

[197] European Parliament, *Resolution of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing,* OJ C 100, 3.5.76, pp. 27.

[198] European Parliament, *Resolution on the protection of the rights of the individual in the face of technical developments in data processing*, OJ C 140, 5.6.1979, pp. 34-38.

[199] Ibid., § 13.

[200] Ibid., § 14.

[201] European Commission, *Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data*, OJ No L 246, 29.8.1981, p. 31, Recital 5.

[202] European Parliament, *Resolution of 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing*, OJ C 87, 5.4.82, pp. 39-41.

On 18 July 1990 the European Commission introduced to the Council a first proposal for a Directive on the protection of personal data. Echoing previous EP suggestions, it foresaw the creation of a consultative organ at the EU level, composed of representatives of national DPAs. In July 1992 the European Commission presented a second proposal, this time taking into account that meanwhile the procedure to be followed had been changed by the Treaties, and the EP was to have co-decision competences. The proposal was consequently submitted for adoption to both the Council and the EP. Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data,[203] was finally approved on 24 October 1995.

The EP's involvement in privacy and data protection came to a climax on September 2001, with the adoption of a Resolution on a global system for the interception of private and commercial communications, known as ECHELON.[204] The Resolution asserted that the existence of such an interception system, operating by means of cooperation among the US, UK, Canada, Australia and New Zealand, had been proved beyond doubt, and that the degree of protection enjoyed by EU citizens against it could "hardly be said to be adequate".[205] It was based on a report on ECHELON adopted on 11 July 2001 that noted the recent proclamation of the EU Charter, but considering its limitations, took the view that "the only effective international instrument for the comprehensive protection of privacy" was the ECHR.[206] The report was the fruit of work by a Temporary Committee set up a year beforehand by the EP, prompted by a debate on a 1999 study[207] commissioned by STOA[208] at the request of the LIBE Committee, and presented at a hearing of same Committee on the subject of 'the European Union and data protection'.[209]

The terrorist attacks of 9/11 and the security initiatives that followed deeply affected privacy and data protection debates worldwide. In the EP, this translated inter alia into a strong focus on safeguarding these rights in the AFSJ, notably aimed at providing the area with a consistent level of protection of personal data despite the discrepancies between the EU legislation that applied under the former first and the third pillars. It also translated into the related question of how to regulate data transfers from the EU to third countries such as the US, when such transfers affect data that was originally collected for commercial purposes (and thus benefited from first-pillar data protection) but which have been subsequently processed for security purposes (and thus possibly falling under the third pillar).

Indeed, a major issue of debate at the EU level during the past decade has been the regulation of data protection in the ex-third pillar, namely regarding data processing in the area of police and judicial cooperation in criminal matters, as well as, until 1999, in relation to data processing related to freedom of movement issues and judicial cooperation in civil

[203] European Parliament and Council of the European Union, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, 23.11.1995, pp. 31-50.

[204] European Parliament, *Resolution of 5 September 2001 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*, (2001/2098(INI)).

[205] Ibid., § L.

[206] Temporary Committee on the ECHELON Interception System, Report of 11 July 2011 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI), Explanatory Statement, § 8(2).

[207] D. Campbell, "The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5", in STOA (ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, October 1999, PE 168.184.

[208] STOA (Scientific and Technological Options Assessment) is a department of the EP Directorate-General for Research.

[209] Coinciding with the (at the time) recent conclusion of the period granted to Member States to transpose the Data Protection Directive.

matters (in 1999, the Amsterdam Treaty shifted these competencies to the first pillar). This field had been left unregulated by the DPD, which explicitly excluded it from its scope of application. For many years, the EP insistently requested the adoption of a horizontal legal instrument for data protection in the third pillar, but with little success. In the third pillar, contrary to the first pillar, the Council had the possibility to legislate without the EP's support. This sidelining of the EP on data protection applicable to data processing related to police and judicial cooperation in criminal matters also affected the EP's role when data transfers to third countries for such purposes were authorised.

EP calls for the establishment of a comprehensive and coherent set of rules at the EU level for the protection of personal data processed in the areas excluded by the DPD could be traced back already to the first years following the adoption of such instrument, i.e. the end of the 1990s. The EP also put efforts in empowering DPAs in relation with third pillar policies, for instance by insisting during the legislative procedure leading to the adoption of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[210] (a first-pillar instrument, on the adoption of which the EP was involved through co-decision) on the fact that the EDPS should cooperate with any supervisory bodies established in the third pillar.[211]

In a Resolution adopted on 27 March 2003,[212] the EP explicitly called on the European Commission to come forward "as soon as possible" with a binding legal instrument relating to data protection in measures taken in the context of the third pillar to provide guarantees equivalent to those inherent in the DPD, and requested the Council to ensure that all major EU information systems were subject to first-pillar data protection.[213] In November 2003, the European Commission announced at the EP its intention to work on a proposal for a new legal instrument. In March 2004, the EP adopted another Resolution[214] with more appeals for "a comprehensive and trans-pillar European privacy and data protection regime", criticising "the extremely serious delays" that occurred in the area of third-pillar data protection. The EP insisted on the necessity of a legal instrument "binding in nature and aimed at guaranteeing in the third pillar the same level of data protection and privacy rights as in the first pillar",[215] and asserted that "in the long term, Directive 95/46/EC should be applied, following the appropriate modifications, to all areas of EU activity, so as to guarantee a high standard of harmonised and common rules for privacy and data protection".[216] In June 2005, a new Resolution endorsed by the EP[217] repeated "its call for common criteria for data protection in the security domain".[218]

---

[210] European Parliament and Council of the European Union, Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal of the European Communities, L 8, 12.1.2001, pp. 1- 22.

[211] See, in this sense, the amendments proposed in European Parliament, *Legislative resolution of 14 November 2000 on the proposal for a European Parliament and Council regulation on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data*, (COM(1999) 337 - C5-0149/1999 - 1999/0153(COD)), OJ C 223 8.8.2001, p. 73.

[212] European Parliament, *Resolution of 27 March 2003 on progress in 2002 in implementing an area of Freedom, Security and Justice*, (Articles 2 and 39 of the EU Treaty), P5_TA(2003)0126.

[213] Ibid., § 1(e).

[214] European Parliament, *Resolution of 9 March 2004 on the First Report on the implementation of the Data Protection Directive (95/46/EC)*, (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI)), P5_TA(2004)0141.

[215] Ibid., § 1.

[216] Ibid., § 2.

[217] European Parliament, *Resolution of 8 June 2005 on progress made in 2004 in creating an area of freedom, security and justice (AFSJ) (Articles 2 and 39 of the EU Treaty)*, P6_TA(2005)0227.

[218] Ibid., § 34.

On 4 October 2005, the European Commission finally introduced a Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[219] The EP adopted a legislative resolution on the proposal on 27 September 2006,[220] putting forward a series of amendments and calling on the Council to consult it again if it intended to modify the text substantially. In December 2006, as discussions at Council level appeared to be almost blocked, the EP voted a recommendation to the Council[221] in which it expressed extreme concern with the direction being taken by the debates, which appeared to imply a lowering of the level of protection granted by the initial proposal. The Council took the decision to consult again the EP, submitting to MEPs a Council text of March 2007. The EP adopted its opinion on the new draft on 7 June 2007,[222] suggesting several proposals for amendments, and regretting the lack of consensus in the Council on the application of the future legal instrument to data processing at national level.[223] In December 2007, the Council reached a political agreement on a new, significantly modified version of the proposal, and decided to consult the EP on the modified text. On 23 September 2008, the EP proposed a last set of amendments,[224] including an explicit reference to idea that the entry into force of the Lisbon Treaty would allow a strengthening of the provisions approved. The instrument was adopted by the Council on 27 November 2008.[225] As already anticipated in chapter 2, in the end, its content failed to satisfy the expectations of those aiming at ensuring a level of protection in the third pillar not too far from the first-pillar data protection.

On 6 July 2011, the EP, in its Resolution on the Commission Work Programme 2012,[226] stressed that it "believes strongly that the forthcoming proposals on a review of Directive 95/46/EC...should be ambitious, going beyond the insufficient protection offered by the Framework Decision on data protection in the former third pillar".[227] In its Resolution of the same day on a comprehensive approach on personal data protection in the EU,[228] the EP detailed that it

[219] European Commission, *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, COM(2005) 475 final, 04.10.2005, Brussels.

[220] European Parliament, *Legislative resolution of 27 September 2006 on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, (COM(2005)0475 – C6-0436/2005 – 2005/0202(CNS)), P6_TA(2006)0370.

[221] European Parliament, *Recommendation to the Council of 14 December 2006 on the progress of the negotiations on the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, (2006/2286(INI)), P6_TA(2006)0602.

[222] European Parliament, *Legislative Resolution of 7 June 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (renewed consultation)*, (7315/2007 – C6-0115/2007 – 2005/0202(CNS)), P6_TA(2007)0230.

[223] Ibid., § 5.

[224] European Parliament, *Legislative resolution of 23 September 2008 on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, (16069/2007 – C6-0010/2008 – 2005/0202(CNS)), P6_TA(2008)0436.

[225] Council of the European Union, Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350, 30.12.2008, p. 60–71.

[226] European Parliament, *Resolution of 6 July 2011 on the Commission Work Programme 2012*, P7_TA(2011)0327.

[227] Ibid., § 53.

[228] European Parliament, *Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union,* (2011/2025(INI)), P7_TA(2011)0323.

> [c]onsiders it imperative to extend the application of the general data protection rules to the areas of police and judicial cooperation, including processing at domestic level, taking particular account of the questionable trend towards systematic re-use of private-sector personal data for law enforcement purposes, while also allowing, where strictly necessary and proportionate in a democratic society, for narrowly tailored and harmonised limitations to certain data protection rights of the individual.[229]

The EP has also been active in other (non-third pillar) data protection and privacy debates, promoting the taking into account of these rights in various policies related to the internal market. For instance, on 15 June 2010 the EP adopted a resolution on the Internet of Things[230] in which it asserts that it firmly believes that protection of privacy constitutes a 'core value' in this domain, and that all users should have control over their personal data; and on 15 December 2010 it endorsed a Resolution on the impact of advertising on consumer behaviour[231] underlining how the development of new advertising practices is generating a range of problems that need dealing with in order to safeguard a high level of protection for users, and that targeted advertising can constitute a serious attack on the protection of privacy.

3.2. Contemporary controversies

In this section, six selected case studies are described in detail to explore how the EP has acted and reacted in a series of key files related to EU security policies with crucial implications for personal data protection and privacy. They aim at illustrating the ways in which the EP has been active in these policies, through which mechanisms and following which data protection and privacy priorities. These particular case studies have been chosen on the grounds of their political significance, but also because they each exemplify different aspects of the relevant institutional and substantive tensions nowadays, as well as those of the immediate past and (as seems foreseeable) near future.

3.2.1. PNR

PNR data is all the information collected by airline companies when passengers book airplane tickets: the name of the passenger, itinerary, contact details, eventual modifications of the booking, cancellation, etc. PNR data became the subject of international debates when, in 2001, the US put forward the possibility for law enforcement authorities to massively retrieve this information from airline companies, to store it and to process it using modern data-mining techniques in order to look for 'unidentified terrorist suspects', in the context of their post-9/11 events counterterrorism strategy. The US requested, in particular, access to PNR data of all passengers travelling to and from US territory, thus including all passengers of all EU–US flights. This demand obliged airline companies operating these flights from the EU to export personal data from the EU's territory to the US, despite this going against the strict rules on the limited conditions under which such data exports are authorised under EU law. The EU was later confronted by other similar requests from other third countries, such as Canada and Australia. Eventually, EU institutions started to discuss the possible establishment of a system for the routine storage and use of PNR data for law enforcement purposes in the EU. The EP has been active in the debates concerning all these initiatives.

- 2000: The Safe Harbour Agreement as a key precedent

[229] Ibid., § 6.

[230] European Parliament, *Resolution of 15 June 2010 on the Internet of Things (IoT)*, P7_TA(2010)0207, based on an own-initiative report adopted on a 4 May 2010 by the Committee on Industry, Research and Energy.

[231] European Parliament, *Resolution of 15 December 2010 on the impact of advertising on consumer behavior*, (2010/2052(INI)), P7_TA(2010)0484, based on an own-initiative report adopted on 8 November 2010 by the Committee on Internal Market and Consumer Protection.

Data transfers from the EU to third countries had already been a contentious issue long before 2001, generating a series of major inter-institutional tensions. According to the DPD, the basic principle applying in this field is that for transfers of personal data from the EU to any third country to take place, insofar as the DPD is applicable, that third country needs to have been officially recognised as providing 'adequate protection' for personal data on its territory in general terms.[232] If such is not the case, and as a way of derogation, transfers can be allowed on a series of other (limited) grounds, such as the unambiguous consent of the data subject or the necessity of the transfer for the performance of a contract, if required on public interest grounds.[233]

There has always been a wide consensus on the fact that the US does not provide, in general, 'adequate protection' to personal data in the terms required by the DPD. However, in order to facilitate EU–US data transfers, and thus also commercial relations between the two parties, the European Commission and the US Department of Commerce searched for a solution that finally saw the light as a series of arrangements allowing US companies to adhere to a set of data protection principles, known as the Safe Harbour principles, and, by doing so, to be officially considered as companies providing 'adequate (personal data) protection' and thus allowed to legally export personal data from the EU to the US, without any further formalities.

In order to formalise this Safe Harbour arrangements in compliance with EU law, the European Commission decided to adopt a Decision in accordance with the method foreseen in the DPD for declaring that a third country provides 'adequate protection' – but declaring, instead, that the protection granted by companies committed to the Safe Harbour principles was 'adequate'. This implied the obligation for the European Commission to follow a 'comitology' procedure,[234] which was thus observed.

'Comitology' procedures have been for many years a matter of dispute amongst EU institutions, especially as the EP has sometimes perceived them as a problematic way of limiting the scope of its legislative oversight on EU decision-making. A revision of the modus operandi of 'comitology' procedures had been introduced by the 1999 'Comitology' Decision,[235] which strengthened the EP power of scrutiny. In 2000, using for the first time ever such new powers, the EP adopted a disapproving Resolution[236] on the draft Decision presented by the European Commission, contesting the 'adequacy' of the level of protection given to personal data under the scheme, and calling on the Commission to closely monitor the implementation of the Safe Harbour Agreement. Despite this critical reaction from the EP, the European Commission went ahead and adopted the Safe Harbour Decision on 26 July 2000.[237] A year later, it introduced in the Decision a Recital stating that, in its view, the EP had never actually questioned its powers to adopt it, and thus had not, as a matter of fact, opposed its adoption in compliance with the 1999 'Comitology' Decision.[238]

- 2001: US authorities unilaterally impose obligation to transfer PNR data on EU companies

[232] Art. 25 of Directive 95/46/EC.

[233] See Art. 26 of Directive 95/46/EC.

[234] As established by Article 25(6) and Article 31(2) of Directive 95/46/EC.

[235] Council of the European Union, *Decision of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (1999/468/EC)*, OJ L 184, 17.7.1999, p. 23.

[236] European Parliament, *Resolution of 5 July 2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related frequently asked questions issued by the US Department of Commerce*, (C5-0280/2000 – 2000/2144(COS)), A5-0177/2000, OJ 2001 C 121/152.

[237] European Commission, *Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C*, (2000) 2441, OJ L 215, 25.8.2000, pp. 7–47.

[238] Corrigendum, OJ 2000 L 115/14 (2000/520/EC).

The decision of US authorities to demand access to PNR data on all passengers travelling to and from US territory, thus imposing on EU airline companies operating EU–US flights to export personal data from the EU territory to the US, raised the question of the legality of such data flows from the perspective of EU law. The transfers did not appear to be compliant with the DPD, as they were not based on any of the grounds allowed by its provisions on international data transfers. They could neither take place under the Safe Harbour Agreement, which was applicable not to EU but solely to US companies. In the light of this assessment, in 2003 the Council decided to authorise the European Commission to negotiate an agreement that would regularise the situation, by obtaining some commitments from the US authorities regarding the conditions of the processing of data. In accordance with the procedure selected to conclude the agreement,[239] once it had been negotiated by the European Commission, the Council could adopt it after simply proceeding to consult the EP, and regardless of the actual position of the EP, which was not granted any veto powers by the procedure. The Council could also establish a time limit for the EP to express its opinion, and if the time elapsed without a formal reaction from the EP, just go ahead with the signature of the agreement.[240] The European Commission eventually negotiated a legal instrument with US authorities, later known as the first EU–US PNR Agreement, and submitted it to the EP for consultation.

- 2004: A first EU–US PNR Agreement is adopted

The agreement was to be accompanied by a Decision of the European Commission asserting that the data transferred by the EU airline companies would benefit from 'adequate protection' in the US. The European Commission introduced a draft of this Decision in 2004,[241] in order to have it adopted through the 'comitology' procedure foreseen by the DPD, just as with the Safe Harbour Decision.

On 31 March 2004, making again use of its powers of scrutiny under the revised 'comitology' procedure already mentioned, the EP adopted a Resolution[242] opposing the European Commission draft measure. This time, it explicitly held that the European Commission had exceeded its powers because of the non-binding nature of US commitments on the use of the data transferred, and that the Decision might lower the protection granted by the DPD. It requested the European Commission to withdraw the drafted adequacy-finding Decision[243] and to submit a new one, unless it negotiated an international agreement satisfactorily guaranteeing protection, reserving the right to appeal to the CJEU if the European Commission was to adopt the proposed one.[244] The EP also pointed out that it reserved the right to bring an action in order to seek verification of the legality of the projected international agreement and, in particular, its compatibility with the protection of fundamental rights.[245] Additionally, it appealed for the European Commission to block any initiatives for establishing European centralised management of the PNR data,[246] which was an approach discussed at the time as a solution for some data protection problems linked to the measure.

[239] Art. 300 TEC.

[240] See Art. 300(3) TEC.

[241] European Commission, *Draft decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection*, (2004/2011(INI)).

[242] European Parliament, *Resolution of 31 March 2004 on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection*, (2004/2011(INI)), P5_TA(2004)0245.

[243] Ibid., §10.

[244] Ibid., §7.

[245] Ibid., §8.

[246] Ibid., § 6.

In April 2004, the Legal Affairs Committee of the EP voiced serious reservations about the procedure chosen by the Council and the European Commission for concluding the agreement with the US, suggesting that the instrument could actually constitute a modification of the DPD and, thus, entail the amendment of an act adopted through co-decision, which was one of the conditions obliging the Council not to simply consult the EP when wishing to conclude an international agreement, but to obtain its assent.[247] The question of whether the negotiated agreement could infringe the fundamental right of data protection enshrined in Community law, in particular Article 286 of the EC Treaty, was also discussed by the Committee. In the light of these concerns, the EP decided to refer the issue to the CJEU for advice, and to wait for such guidance before taking any formal position on the issue.

At the beginning of May 2004, the European Commission launched an urgent procedure to have its 'adequacy-finding' Decision rapidly adopted through the 'comitology' procedure., The Decision was indeed adopted despite the EP's will to wait for the CJEU's orientation.[248] On 17 May 2004, the Council made official the conclusion of the EU–US PNR Agreement.[249] The EP request for the Court's opinion became thus null and void.

On 25 June 2004, the EP President decided to ask the CJEU, on behalf of the European Parliament,[250] to annul the Council's Decision of 17 May 2004 on the conclusion of an agreement, and to appeal against the European Commission's Decision stating that the level of protection of data provided by the US was adequate.[251]

- 2005: Pending resolution by the Court, the EP disapproves of EU–Canada PNR Agreement

In 2005, the Council and the European Commission followed the same contested procedure to negotiate an agreement for the transfer of PNR data from the EU to Canada. On 7 July 2005, the EP adopted a Resolution[252] stating that it did not approve the conclusion of the agreement, on the basis that the approach adopted by the Commission and Council gave rise to the same reservations as those expressed regarding the EU–US PNR Agreement. The EU–Canada PNR Agreement was nevertheless eventually concluded.[253]

- May 2006: The CJEU annuls the challenged EU–US PNR Agreement

With a judgement of 30 May 2006,[254] the CJEU annulled both the Council's Decision on the conclusion of the EU–US PNR Agreement and the 'adequacy-finding' Decision of the

[247] As foreseen in Art. 300(3) TEC.

[248] European Commission, Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under document number C(2004) 1914), OJ L 235 , 06.07.2004, pp. 11-22.

[249] Council of the European Union, *Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security*, Bureau of Customs and Border Protection, OJ 2004 L 183, p. 83.

[250] And in the light of recommendations made on 16 June by the EP Legal Affairs Committee and the Conference of Presidents.

[251] Action for annulment under Article 230 of the Community Treaty. The European Data Protection Supervisor (EDPS) was eventually given leave to join the proceedings, supporting the EP.

[252] Council of the European Union, *Resolution on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data,* (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS).

[253] Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82, 21.03.2006, pp. 15-19.

[254] Court of Justice of the European Union (Grand Chamber), Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*, 30 May 2006

European Commission. The Court came to conclusion that the legal bases used to adopt them were inappropriate. The Council and the European Commission had regarded the transfers as being a first-pillar issue, falling under the scope of the DPD. The Court found, however, that the Commission's 'adequacy-finding' Decision and the Agreement applied to "processing operations concerning public security and the activities of the State in areas of criminal law",[255] falling outside of the scope of the DPD,[256] and therefore rendering ill-suited the use of a first-pillar legal basis[257] for the adoption of the agreement.[258] The annulled instruments were allowed by the CJEU to be in force until a new agreement was in place, and until 30 September 2006 at the latest.[259]

The judgement of 30 May 2006 was a victory for the EP in the sense that it repealed the contentious EU–US PNR Agreement, but it failed to provide any guidance on the compatibility of the instrument's content with fundamental rights. Moreover, by affirming the third pillar nature of this type of international agreements, it curtailed the powers of the EP on upcoming negotiations, and highlighted the negative repercussions of having disparate legislative procedures and heterogeneous data protection frameworks for the First and the Third pillar.

- *October 2006: Interim EU–US PNR Agreement*

Following the judgement of the CJEU, discussions on a new instrument were rapidly set in motion, but proved difficult. The Council and the European Commission opted to focus on the rapid conclusion of an 'interim' solution to enter into force by the September 2006 deadline fixed by the Court , allowing for more time for discussions on a more permanent agreement for the future.

On 7 September 2006, the EP adopted a Recommendation to the Council on the negotiations for an EU–US PNR[260] describing a series of requirements to be taken into account in the area, such as the purpose limitation principle.[261] The EP also expressed that, as a general principle, it considered "that the systematic collection of the data of ordinary citizens outside the framework of a judicial procedure or police investigation should remain forbidden in the EU"[262], and, despite not explicitly mentioning the technique of profiling, emphasised its concerns with the access to data to assess the possible match of individuals "against a theoretical pattern whether such a passenger might constitute a potential threat".[263] It also took the occasion to declare that the Council should not take advantage of artificial divisions between pillars, but should rather create a consistent EU cross-pillar data protection framework and ensure that any new agreement was concluded in association with the EP.[264]

On 11 October 2006, at a Plenary Session, MEPs were informed by a Council representative that consensus on a temporary agreement, to be valid until the end of July 2007, had been reached. The 'interim' agreement was officially signed on 19 October 2006. As the procedure was now framed under third-pillar rules, no assent of the EP was required.

---

[255] § 56 of the Judgement of 30 May 2006.

[256] By virtue of Art. 3(2) of the Data Protection Directive.

[257] Article 95(EC), as had been the case.

[258] § 67 of the Judgement of 30 May 2006.

[259] § 74 of the Judgement of 30 May 2006.

[260] European Parliament, *Recommendation to the Council of 7 September 2007 on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime* (2006/2193(INI)), P6_TA(2006)0354.

[261] Ibid., § 1. The 'push' system is opposed to the 'pull' system and refers to the modalities of data access by US authorities.

[262] Ibid., § 3.

[263] Ibid., Recital A.

[264] Ibid., § 1(i).

On 6 November 2006, an EU–US High Level Contact Group was set up in order to discuss privacy and personal data protection in the context of the exchange of information for law enforcement purposes, with the view of exploring the possible negotiation of an EU–US Agreement to generally allow the transfer of personal data from the EU to the US for such purposes.

- 2007-2008: A new EU–US PNR Agreement, an EU-AUS PNR Agreement, and EU-PNR is introduced

On 28 June 2007 the draft of a new EU–US PNR Agreement was concluded, to replace the 'interim' one. The new agreement was transmitted informally to the EP, which on 12 July 2007 adopted a Resolution on the subject.[265] The EP expressed that it regretted the lack of democratic oversight of the negotiations leading to such an agreement,[266] criticised its failure to offer an adequate level of personal data protection, and lamented the lack of clear and proportionate provisions as regards the sharing of information and its retention and supervision by DPAs,[267] calling on the national parliaments to examine the draft carefully in the light of these observations.[268] The EP also demanded a clarification on a reference contained in the draft agreement to the possible set up of an EU PNR system, access to which would supposedly also be granted to US authorities.[269] Finally, it put forward its intention to seek a legal appraisal of the agreement, inviting the WP29 and the EDPS to present opinions in this respect.[270] The Council formally adopted the new EU–US PNR Agreement on 23 July 2007.[271]

On 6 November 2007, the European Commission presented a proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes[272] in order to pave the way to the establishment of an EU PNR system based on the systematic collection, storage and processing of personal data of all passengers travelling by air to and from the EU, for the purpose of preventing and combating terrorist offences and organised crime. As the proposal concerned a third pillar legal instrument, i.e. a Council Framework Decision, it could be adopted without the involvement of the EP as co-legislator through the co-decision procedure. Nevertheless, as the text was extensively discussed in the Council, in September 2008 the Presidency decided to request an opinion on it from the FRA. The opinion was delivered in October 2008, and focused on compliance of the envisaged system with the right to respect for private life, the right to protection of personal data and the prohibition of discrimination.[273]

On 28 May 2008, the EU–US High Level Contact Group set up to discuss privacy and personal data protection in the context of transatlantic exchanges of information for law

[265] European Parliament, *Resolution of 12 July 2007 on the PNR agreement with the United States of America*, P6_TA(2007)0347.

[266] Ibid., § 2.

[267] Ibid., § 4.

[268] Ibid., § 5.

[269] Ibid., § 27.

[270] Ibid., § 31.

[271] Council of the European Union, *Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS)*, OJ L 204, 04.08.2007, pp. 16-25.

[272] European Commission, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, Brussels, 6 November 2007.

[273] European Union Agency for Fundamental Rights (FRA) (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 28 October 2008.

enforcement purposes produced its final report setting out some general principles on which consensus had been noted.[274]

In June 2008, the Council adopted a Decision on the conclusion of an agreement to transfer PNR data to Australia.[275] On 22 October 2008, the EP adopted a Recommendation to the Council[276] arguing that the procedure followed for the conclusion of such EU-Australia PNR Agreement lacked democratic legitimacy, as at no stage had there been any meaningful democratic scrutiny or Parliamentary approval. Furthermore, in the EP's view the agreement failed to meet EU and international data protection standards, or to comply with Article 8 of the ECHR, in particular with the requirements regarding purpose limitation. MEPs also stressed that, in the event of the entry into force of the Treaty of Lisbon, the EP should be associated on a fair basis with the review of all PNR international agreements.

A month later, on 20 November 2008, the EP endorsed a Resolution on the European Commission's proposal for an EU PNR system.[277] The EP regretted that the proposal had left many legal uncertainties with respect to its compatibility with the ECHR and the Charter, as well as its legal basis, raising questions as to its appropriate role in the legislative procedure,[278] and noted that similar concerns had been raised by the FRA, the EDPS, the WP29 and the recently set-up WPPJ.[279] The EP considered that it had to reserve its formal opinion until these concerns had been properly addressed. Nevertheless, regarding the substance of the proposal, it emphasised that the ECHR and the EU Charter require that any massive infringement of the right to the protection of personal data be legitimate and justified by a pressing social need, provided for by law and proportionate to the end pursued, which must be necessary and legitimate in a democratic society[280]. The EP also declared that the adoption of an adequate data protection framework under the third pillar should be regarded as an absolute precondition for the establishment of any EU PNR scheme.[281]

On 12 December 2008, a US–EU JHA Ministerial meeting asserted that, as the EU–US High Level Contact Group on privacy and personal data protection in the context of transatlantic exchanges of information for law enforcement had identified a wide range of common principles, the parties should aim at starting negotiations on a binding EU–US agreement as soon as possible.

- 2009: Resolution on profiling, Lisbon Treaty

On 24 April 2009, the EP adopted a Recommendation to the Council on the issue of profiling,[282] advocating the establishment of a legal framework providing a clear definition

[274] Council of the European Union, *Note from the Presidency to COREPER on the EU-US Summit, 12 June 2008: Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 9831/08, 28 May 2008, Brussels.

[275] Council of the European Union, *Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service*, OJ L 213, 8.8.2008, pp. 47-48.

[276] European Parliament, *Recommendation of 22 October 2008 to the Council on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service*, P6_TA(2008)0512.

[277] European Parliament, *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, P6_TA(2008)0561.

[278] Ibid., § 3.

[279] Idem.

[280] Ibid., § 8.

[281] Ibid., § 25.

[282] European Parliament, *Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control* (2008/2020(INI)), OJ C 184 E, 8.7.2010, pp. 119-125.

of profiling, whether through the automated mining of computer data or otherwise. Data-mining and profiling blur the boundaries between permissible, targeted surveillance and problematic mass surveillance, in which data are gathered because they are useful rather than for defined purposes, according to the Recommendation, which was based on an own-initiative report adopted on 31 March 2009 by the LIBE Committee.[283]
In December 2009, the entry into force of the Lisbon Treaty implied the collapse of the EU pillar structure, and redefined the EP role in the conclusion of international agreements. Moreover, it rendered the proposed Council Framework Decision for an EU PNR system of 2007 the obsolete, which led the Council to ask the European Commission to draft a new proposal.[284]

- 2010: The EP slows down progress on all PNR files

Taking into account the new applicable procedures, the Council submitted both an EU–US and an EU–AUS PNR Agreement to the EP, with a view to obtaining its consent for concluding the agreements. On 5 May 2010, however, the EP decided to postpone its vote on the request for consent to the instruments. Adopting a Resolution on the negotiations of agreements with the US, Australia and Canada,[285] the EP stated that the vote was postponed until the EP had fully explored the options for arrangements and whether they met the EP's concerns. In this sense, the EP required the European Commission to provide all the available relevant information and background documents and to ensure that MEPs were given full access to the negotiation documents and directives at all stages of the procedure, and that national parliaments were given access upon request.[286] It also asserted that any new legislative instrument should be preceded by a Privacy Impact Assessment, along with a proportionality test demonstrating that existing legal instruments were not sufficient.[287] The EP invited the Commission to present, no later than mid-July 2010, a proposal for a coherent approach on the use of PNR data for law enforcement and security purposes, establishing a single set of principles to serve as a basis for agreements with third countries,[288] and to request that the FRA provide a detailed opinion on the fundamental rights dimension of any new PNR agreement.[289] It also listed the minimum requirements for such model, including that of being in line with European data-protection standards, in particular regarding purpose limitation, proportionality, legal redress, the imitation of the amount of data to be collected and the length of storage periods.[290]

In response to the EP's request, on 21 September 2010, the European Commission presented a Communication on the EU external PNR strategy.[291] The Communication was part of a package of proposals on the exchange of PNR data, including also a set of recommendations for negotiating directives for new PNR agreements with the US, Australia and Canada, for the Council to authorise the opening of new negotiations. The Council welcomed the approach and pressured to European Commission to rapidly come forward with a new proposal for an EU PNR system.

[283] Submitted by Sarah Ludford (ALDE) on 19 December 2007.

[284] European Council, The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens, 2010, p. 19.

[285] European Parliament, *Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada*, P7_TA(2010)0144.

[286] Ibid., § 11.

[287] Ibid., § 5.

[288] Ibid., § 7.

[289] Ibid., § 8.

[290] Ibid., § 9.

[291] European Commission, *Communication from the Commission On the global approach to transfers of Passengers Name Record (PNR) data to third countries*, COM(2010) 492 final, 21.9.2010, Brussels.

On 11 November 2010, the EP reacted to the developments endorsing a new Resolution[292] in which it insisted on some previously expressed concerns, stressing the need to safeguard the protection of values described as "data protection, the right of informational self-determination, personal rights and the right to privacy"[293] and recalled its belief in the need to protect civil liberties and fundamental rights, among which it placed not only the rights to privacy and data protection (recognised in the EU Charter), but also the (German) right of informational self-determination.[294] The EP underlined the importance of the proportionality principle, reiterating its call to the European Commission to provide it with factual evidence of the necessity of the measures proposed, and indicated that it would only be able to give its consent to any agreements if fully informed on all PNR-related and relevant developments. It also reiterated its position that PNR data shall in no circumstances be used for data-mining or profiling, stating that the differences between the concepts of 'risk assessment' and 'profiling' in the PNR context need to be clarified.[295]

In December 2010, EU Justice Ministers approved the start of talks with the US on the possible negotiation of a transatlantic agreement on data exchange and data protection when cooperating to fight terrorism or crime.

- *2011: Progress resumes amid criticism*

In February 2011, the European Commission introduced a new proposal for an EU-PNR system, this time in the form of a proposal for a Directive.[296] It allegedly took into account the previous recommendations of the EP. On 12 April 2011, the Council Legal Service issued an opinion in which it came to the conclusion that, in the form proposed, the Directive restricted the right to respect for privacy and the right to protection of personal data to such an extent that it could in fact be challenged in Court, invoking the proportionality requirement pursuant to Articles 7, 8 and 52 of the EU Charter and the general principles of EU law.

Negotiations on the EU-PNR system continued at Council, where a majority of Member States appear to support the extension of the compulsory of collection of PNR data to internal EU flights. Nevertheless, some Member States asserted during the negotiations that they had faced difficulties in convincing their national Parliament of the necessity for collecting and processing PNR data as foreseen.[297]

In May 2011, the European Commission introduced a Proposal for a Council Decision on the conclusion of an EU–AUS PNR Agreement. During Spring 2011, the European Commission, on behalf of the EU, also negotiated with US authorities a new EU–US PNR Agreement. A Draft Agreement was eventually rendered public informally. On 18 May 2011, the Legal Service of the European Commission addressed a letter to DG HOME stating that there are grave concerns that Draft Agreement, on which the European Commission planned to inform the Council and the EP, was contrary to the right to the protection of personal data as enshrined in Article 16 TFEU and Article 8 of the EU Charter. The Legal Service explained that a number of elements put into question the proportionality of the measure, including the definition of "serious crime" in reference to the notion of "extraditable offence", the possible use of data "to ensure border security", the non-compliance with the principle of

[292] European Parliament, *Resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council to authorise the opening of negotiations between the European Union and Australia, Canada and the United States*, P7_TA(2010)0397.

[293] Ibid., Recital I.

[294] Ibid., § 1.

[295] Ibid., § 7.

[296] European Commission, *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, Brussels, 2 February 2011.

[297] Working Party on General Matters including Evaluation (GENVAL), *Summary of discussion on 11 May 2011*, 14 June, Brussels, p. 2.

purpose limitation due to the possibility to use data "if ordered by a Court", the long data retention period, the lack of judicial redress, and the lack of independent oversight.

In April 2011, the EP President had sent a letter to the FRA requesting an expert opinion on the Proposal for a Directive on the US–EU PNR and its compliance with the EU Charter. The FRA published its opinion in June 2011, identifying a series of problematic issues.[298] The FRA assessment focused on compliance with the right to non-discrimination, which the Impact Assessment of the Commission services had not mentioned, and on two broader fundamental rights issues, namely requirements for limitations of fundamental rights and effective supervision. The FRA stated that, "for the detection of indirect discrimination, it would be useful to create suitable aggregate statistics based on PNR data to detect discriminatory patterns and trends in the application of the PNR system; these statistics must, however, be created anonymously and in a non-identifiable manner in order to comply with EU data protection principles."[299] It also referred to the European Union Committee of the UK House of Lords 2008 statement according to which it had been persuaded by confidential evidence received from the Home Office that PNR data, when used in conjunction with data from other sources, could significantly assist in the identification of terrorists.[300]

3.2.2. TFTP

Just like debates on PNR data processing for law enforcement purposes, discussions on the possible processing of financial data of innocent individuals for 'terrorist tracking' were provoked by US use of such data in the context of its post-9/11 counterterrorism policy. The discussions among EU institutions eventually evolved to integrate also the establishment of a 'local' system in the EU.

- 2006: Access by US authorities to EU financial data through SWIFT revealed to the public

In June 2006, the media disclosed the existence of a TFTP, put in place by the US administration, which allowed US authorities to access financial data stored by a Belgian-based company working for thousands of commercial banks and institutions, SWIFT. It was revealed that SWIFT, which processes data on millions of financial transactions daily, relied on a server based on US territory and that the US Treasury Department's Office of Foreign Assets Control (OFAC) had issued administrative subpoenas requiring the US operating centre for SWIFT to provide access to data processed on that server. The revelation provoked major discomfort in the EU, as even the existence of the server in question appeared to be unknown to the authority that should have been notified of the transfers to possibly authorise them (i.e., the Belgian Privacy Commission).

On 6 July 2006, the EP endorsed a Resolution on the interception of bank transfer data from the SWIFT system by the US secret services,[301] stressing that the EU is based on the rule of law and that all transfers of personal data to third countries are subject to data protection legislation at national and European level, which provides that any transfer must be authorised by a judicial authority and that any derogation from this principle must be proportional and founded on a law or an international agreement. The EP took the occasion to request to the Council to urgently adopt the proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, by that time under discussion at Council level.[302] In this sense, the EP expressed its disappointment with the Council's unwillingness to overcome the legislative

[298] European Union Agency for Fundamental Rights (FRA) , *Opinion on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime* (COM(2011) 32 final) 14 June 2011, Vienna.

[299] Ibid., p. 10.

[300] Ibid., p. 15.

[301] European Parliament, *Resolution of 6 July 2006 on the interception of bank transfer data from the SWIFT system by the US secret services*, P6_TA(2006)0317.

[302] Ibid., § 9.

situation of the time, where two different procedural frameworks for the protection of fundamental rights applied.[303] The EP followed up the issue notably by organising a public hearing in October 2006.

On 14 February 2007, the EP voted a Resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues,[304] stressing that several agreements prompted by US requirements and adopted without any EP involvement had led to a situation of legal uncertainty with regard to the necessary data protection guarantees for data sharing and transfer between the EU and the US.[305] The EP explicitly referred to the critical opinions on the situation as expressed by the WP29 and the EDPS,[306] as well as to the US Congress and its reservations as regards the method of profiling and data-mining, described as consisting in accumulating in an indiscriminate manner larger and larger volumes of personal data.[307] It asserted that the EP and national parliaments should be fully involved in the negotiation of all international agreements that concern EU fundamental rights[308] of the EU, and again stressed the need for the adoption of a Framework Decision on the protection of personal data in the third pillar, to be comprehensive and ambitious in scope and to provide for data protection rules also covering the exchange of personal data with third countries.[309] In a Resolution on transatlantic relations adopted on 25 April 2007,[310] the EP manifested again its regrets on the fact that the PNR and SWIFT affairs had led to a situation of legal uncertainty with regard to the necessary data protection guarantees for data sharing and transfer between the EU and the US for the purposes of ensuring public security and, in particular, preventing and fighting terrorism.[311]

Eventually, an agreement was reached between EU and US authorities on the access to SWIFT data. On June 28 of 2007, a set of unilateral commitments on the part of the US Treasury was disclosed. In October 2007, SWIFT announced that a new network structure would be operational by the end of 2009, having as a consequence that the majority of the financial data that SWIFT had being delivering to the US Treasury Department's TFTP would no longer be made available through the same channel, unless new measures were undertaken.

- 2009: Transatlantic negotiations

To find a way to allow the US TFTP to continue consulting SWIFT data even if unrelated to US territory, transatlantic informal negotiations resumed in 2009. On 27 July 2009, the Council unanimously adopted negotiating directives for the negotiation by the Presidency, assisted by the European Commission, of an international agreement with the US to continue the transfer of SWIFT data to the US TFTP.

On 17 September 2009, the EP endorsed a Resolution on the envisaged agreement.[312] The EP declared that it was concerned that, with respect to the legal basis chosen for this envisaged agreement, the legal services of the institutions had expressed divergent opinions.[313] It underlined that any international agreement should as a very minimum

[303] Ibid., § 11.

[304] European Parliament, *Resolution of 14 February 2007 on SWIFT, the PNR agreement and the transatlantic dialogue on these issues*, P6_TA(2007)0039.

[305] Ibid., § 1.

[306] Ibid., § 2.

[307] Ibid., § 3.

[308] Ibid., § 8.

[309] Ibid., § 10.

[310] European Parliament, *Resolution of 25 April 2007 on transatlantic relations*, P6_TA(2007)0155.

[311] Ibid., § 9.

[312] European Parliament, *Resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing*, P7_TA(2009)0016.

[313] Ibid., § 6.

ensure a series of principles such as purpose limitation and proportionality. In addition, it envisaged the agreement as an interim agreement that should provide for the US authorities to be notified after the entry into force of the Lisbon Treaty, in order to negotiate then a new agreement under the new EU legal framework, involving the EP and national parliaments.[314] On 22 October 2009, the EP noted in a new Resolution[315] that an interim agreement on the transfer of financial data was being negotiated between the EU and the US which would be valid for an intermediate period through a sunset clause not exceeding 12 months, and that a new agreement, negotiated without prejudice to the procedure to be followed under the Lisbon Treaty, should have to fully involve the EP and national parliaments.[316]

In November 2009, the EU and US negotiators finally reached a consensus on a draft interim agreement[317] to allow US authorities to receive financial data stored in the EU by a designated provider in order to allow targeted searches for counter-terrorism investigations. On 30 November 2009, the Council signed the agreement, to be provisionally applied as from 1 February 2010. A proposal for a Council decision on the singing of the agreement was drafted. In December 2009, an MEP brought an application to the CJEU seeking the annulment of a Council decision refusing her access to an opinion of the Council Legal Service on the opening of negotiations on the agreement.[318]

- 2010: The EP refuses to consent to first agreement

Under the provisions of the Lisbon Treaty, entered into force in December 2009, the EP consent to the formal conclusion of the (already signed, and thus not further negotiable) interim agreement was required. In January 2010, the Chairman of the LIBE Committee consulted the EDPS on the issue, who replied that "not enough elements ha[d] been provided to justify the necessity and the proportionality of such a privacy-intrusive agreement".[319] On 1 February 2010, the provisional application of the TFTP agreement began. On 2 February 2010, the Legal Service of the EP warned that in its view the EP was not in a position to give consent to the agreement, notably because of the limited information received during the negotiations.[320]

On 11 February 2010, the EP adopted a legislative resolution on the agreement.[321] Much to the surprise of the Council and the US, the EP withheld its consent to its conclusion.[322] The EP requested the European Commission to immediately submit recommendations to the Council with a view to a long-term agreement with the US, stressing that any new agreement in this area should comply with the new legal framework established by the Treaty of Lisbon and the then already binding EU Charter.[323] The Resolution was adopted having regard to the recommendation of the LIBE Committee of 5 February 2010 on the same subject, which asserted that the agreement violated the basic principles of data

[314] Ibid., § 7.

[315] European Parliament, *Resolution of 22 October 2009 on the upcoming EU-US Summit and the Transatlantic Economic Council Meeting*, P7_TA(2009)0058.

[316] Ibid., § 63.

[317] Council of the European Union, *Draft agreement on SWIFT*, 15671/09.

[318] Court of Justice of the European Union, Case T-529/09, *In't Veld v Council,* 31 December 2009

[319] "Letter from the European Data Protection Supervisor (EDPS), Peter Hustinx, to the Chairman of the Committee on Civil Liberties, Justice and Home Affairs, Juan Fernando López Aguilar, Brussels, 25 January 2010.

[320] Legal Service of the European Parliament , *Legal opinion on: SWIFT (Conclusion of EU/US TFTP Agreement)*, 02.02.2010.

[321] European Parliament, *Legislative resolution of 11 February 2010 on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, P7_TA(2010)0029.

[322] Ibid., § 1.

[323] Ibid., § 2.

protection law, i.e. the principles of necessity and proportionality, among other legal issues.[324] The Recommendation also raised concerns regarding inter-institutional relations and, particularly, the inappropriateness of requesting the EP consent for the conclusion of the Agreement in conditions in which it was impossible for practical reasons for it to react before its the provisional application came into operation.[325] The first TFTP agreement, which had been in force for 11 days, was thus invalidated.

In the Stockholm programme, the European Council called upon the European Commission to "examine the possibilities to track terrorist financing within the Union".[326] In its Action Plan for the Programme, the European Commission announced the publication of a Communication on the feasibility of a European Terrorist Finance Tracking Program in 2011.[327]

- 2010: The EP accepts a second TFTP agreement

On 5 May 2010, the EP voted a Recommendation to authorise the negotiation of a second TFTP agreement.[328] It declared that it welcomed the new spirit of cooperation demonstrated by the European Commission and the Council and their willingness to engage with the EP in this area,[329] and requested that all relevant information and documents, including any underlying intelligence, be made available for deliberations in the EP, in line with the applicable rules on confidentiality, in order to demonstrate the necessity of the scheme in relation to already existing instruments. The EP also asked the European Commission to report regularly on the functioning of the agreement and to inform the EP fully about any review mechanism to be set up under the said agreement.[330] Furthermore, it reiterated its emphasis on the need for the agreement to respect the purpose limitation principle,[331] as well as the principles of proportionality and necessity.[332]

On 15 June 2010, the European Commission adopted a Proposal for a Council Decision on the conclusion of the second TFTP agreement.[333] It was manifest that the drafters had aimed at multiplying the explicit references to the fundamental rights that the agreement allegedly respected, even if they did not manage to always provide fully accurate references.[334] On 22 June 2010, the EDPS published an opinion stating that the new draft

[324] Ibid., § 3.

[325] Ibid., § 4.

[326] European Council, *The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens*, 2010, p. 25.

[327] European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Delivering an area of freedom, security and justice for Europe's citizens: Action Plan Implementing the Stockholm Programme*, COM(2010) 171 final, 20.4.2010, Brussels, p. 41.

[328] European Parliament, *Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing*, P7_TA(2010)0143.

[329] Ibid., § 11.

[330] Ibid., § 17.

[331] Ibid., § 6.

[332] Ibid., § 7.

[333] European Commission, *Proposal for a Council Decision on the signature of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, COM(2010) 317 final, 15.06.2010, Brussels.

[334] The proposal notably referred to "the protection of personal data under Article 8(2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms", even though Art. 8 ECHR refers not to the protection of personal data but to the right to respect for private life, and the right is established in Art. 8(1) ECHR, whereas Art. 8(2) ECHR only provides for the legitimate interferences with the right; and it refers to "the right to privacy with regard to the

included improvements but there were still major concerns, notably regarding data subject rights and oversight mechanisms.[335]

On 28 June 2010, the new TFTP agreement was signed.[336] On 8 July 2011, the Plenary voted in favour of a Resolution granting consent to the second TFTP agreement.[337] The Resolution was adopted having regard to a Recommendation adopted on 5 July 2011 by the LIBE Committee,[338] which underlined a series of improvements brought by the new agreement, such as the monitoring of the access to and extraction of data by US agencies by a European official, allegedly to prevent the possibility of data-mining and economic espionage; a more detailed regulation of the procedure regarding judicial redress for EU citizens; a more comprehensive right to rectification, erasure, and blocking; a more detailed regulation on transparency of the US TFTP and of the procedure regarding onward data transfers to third countries; and the clarification of the scope for fighting terrorism. The Recommendation was nevertheless accompanied by two Minority Opinions, one of which asserted that the new agreement did not meet the guarantees requested by the EP in its previous resolutions, and which was also critical of the supervisory role to be played by EUROPOL.[339] The approved TFTP agreement entered into force in August 2010.

- *2011: A debated implementation*

In November 2010, the EUROPOL Joint Supervisory Body, composed of representatives of national DPAs, conducted an inspection on EUROPOL's implementation of the TFTP agreement. The inspection led to the conclusion that EUROPOL's practice of accepting oral requests of data from the US rendered impossible any proper audit of compliance with its data protection obligations.[340]

At the beginning of 2011, tensions emerged as a member of the German Bundestag asked the German Federal Ministry of the Interior questions about the TFTP Agreement, but no answers could be obtained due to EUROPOL's refusal to provide information on its role in the execution of Article 4 of the Agreement (which configures the Agency as responsible for verifying the conformity of US requests for data) on the grounds that the questions touched upon a politically sensitive area.[341]

---

processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union", even if Art. 16 TFEU does not mention the right to privacy at all.

[335] European Data Protection Supervisor, *Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II)*, 22 June 2010, Brussels.

[336] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010.

[337] European Parliament, *Legislative resolution of 8 July 2010 on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program* (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE)), P7_TA(2010)0279.

[338] European Parliament, *Recommendation of 5 July on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program* (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE)), Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Alexander Alvaro), A7-0224/2010.

[339] Minority Opinion by J. Albrecht, R. Tavares, J. Sargentini, H. Flautre, T. Zdanoka and Cornelia Ernst.

[340] EUROPOL Joint Supervisory Body, *Report on the inspection of EUROPOL's implementation of the TFTP agreement, conducted in November 2010*, JSB EUROPOL inspection report 11-07, 1 March 2011, Brussels.

[341] Council of the European Union, *Note from German delegation to delegations on EUROPOL's role in the framework of the EU-US TFTP Agreement 1 and state of play of operational and strategic*

In accordance with the concluded TFTP agreement, its first review was to take place six months after its entry into force. In March was published the report relating to the joint review of the implementation of the agreement,[342] giving an overall positive picture of data protection compliance despite the existence of dissenting opinions.[343]

In July 2011, the European Commission published a Communication to advance in discussion towards the establishment of an EU TFTP.[344]

3.2.3. Data retention

The EP has also been particularly involved in the discussions related to the regulation of the retention of telecommunications data by communication providers and their making available of such data to law enforcement authorities.

- 2002: EU law grants Member States freedom to impose retention of 'traffic data'

The first explicit reference in EU law to the possibility of Member States to oblige communication providers to store telecommunications data and make it available for the purposes of law enforcement appeared in Directive 2002/58/EC (known as the e-Privacy Directive),[345] adopted by the EP and the Council under the co-decision procedure. Developing an exception already configured in the legal instrument that it replaced, namely in Directive 97/66/EC,[346] Directive 2002/58/EC recognised that Member States *might* impose on communications providers the obligation to store 'traffic' data and to ensure access to it to law enforcement authorities. As at the time no political agreement on the actual length of such possible retention could be reached, this issue was not harmonised further.

- 2004-2006: EP criticises data retention, but adopts DRD

In March 2004, the EP asserted in a Resolution[347] that, in its view, "Member States' laws providing for the wide-scale retention of data related to citizens' communications for law-

agreements of EUROPOL (specific focus: the agreement on exchange of personal data and related information that EUROPOL has with the US) - EU information policy on the TFTP Agreement, 6266/11, 8 February 2011, Brussels.

[342] Joint Review Team, EU/USA Agreement: processing and transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Program: the report relating to the joint review of the implementation of the agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. See also: European Commission, *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, 16.03.2011.

[343] See, notably: Breitbarth, P., *Letter to the Head of Delegation of the EU Joint Review Team TFTP*, 18 April 2011, Den Haag.

[344] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European terrorist finance tracking system: available options*, COM(2011) 429 final, 13.07.2011, Brussels.

[345] European Parliament and Council of the European Union, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ of the European Communities, L 201, 31.7.2002, pp. 37-47.

[346] European Parliament and Council of the European Union, Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal of the European Communities, L 24, 30.1.1998, pp. 1–8.

[347] European Parliament, First Report on the implementation of the Data Protection Directive (95/46/EC), 2004

enforcement purposes are not in full conformity with the European Convention on Human Rights".[348]

A first EU legislative proposal to render uniform among Member States such data retention obligations imposed on communication providers was tabled in April 2004. It took the form of a third pillar instrument, i.e. a proposal for a Framework Decision, submitted as a joint proposal by the four Member States (the UK, France, Ireland, and Sweden). For it to be adopted, the proposal needed to a unanimous vote at Council, but it did not require the approval of the EP, which had to be merely consulted.

On 27 September 2005, the EP adopted a Resolution[349] under the consultation procedure rejecting the proposal for a Framework Decision. The vote took place on the basis of a Report of 31 May of the LIBE Committee[350] stating that there were sizeable doubts concerning the choice of legal basis of the instrument and the proportionality of the measure, and that in reality it was also possible that the proposal contravened Article 8 of the ECHR. The report included an Opinion of the Committee on Legal Affairs, considering that content of the proposal should be split into two instruments, one falling under the first and the other under the third pillar.

In the meantime (on 21 September 2005), the EC had formally introduced a first pillar legal instrument for data retention, namely a proposal for Directive amending Directive 2002/58. The legal basis on which this proposal relied granted the EP the right of co-decision.

In October 2005, the UK Presidency informed the EP that it aimed at adopting a measure on data retention by the end of the year, regardless of its legislative form, and that the Council was open to discuss the possible adoption of a Directive, while keeping on the table the proposal for a Framework Decision. At a Conference of Presidents taking place soon after it appeared that the EP was also interested in reaching a compromise by the end of 2005.

On 24 November 2005, the LIBE Committee defined its position on the proposed Directive, opting to support the proposal with a limited series of amendments negotiated by the three major Political Groups. On 28 November, the LIBE Committee adopted a Report defending this endorsement of the Directive,[351] containing nevertheless a Minority Opinion stating the text seriously impinged on the fundamental rights of citizens.[352]

---

[348] Ibid., § 18.

[349] European Parliament, *Legislative Resolution of 27 September 2005 on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism* (8958/2004 – C6-0198/2004 – 2004/0813(CNS)), P6_TA(2005)0348.

[350] European Parliament, *Report of 31 May 2005 on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism* (8958/2004 – C6-0198/2004 – 2004/0813(CNS)), Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Alexander Nuno Alvaro), PE 357.618v03-00.

[351] European Parliament, *Report of 28 November 2005 on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)), Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Alexander Nuno Alvaro).

[352] Minority Opinion pursuant to Rule 48(3) of the Rules of Procedure, by Giusto Catania, Ole Krarup, Sylvia-Yvonne Kaufmann and Kathalijne Maria Buitenweg.

On 14 December 2005, the EP officially approved the proposal for a DRD, with a legislative Resolution voted under the co-decision procedure.[353] As complementary statements, the EP called on the European Commission to carry out an impact assessment study covering all internal market and consumer protection issues related to the instrument,[354] and took the opportunity to request the Council to swiftly adopt appropriate data protection rules for the third pillar.[355] The Resolution was adopted having regard to the mentioned Report of the LIBE Committee, whose rapporteur made a public statement pointing out that he did not agree with the outcome of the vote and that he would be withdrawing his name from the Report. On 15 March 2006, the DRD was formally adopted.[356]

- 2006-2009: Legal basis of the DRD upheld

On 6 July 2006, Ireland brought an action for annulment against the DRD, on the grounds that its legal basis was inappropriate. As the main purpose of the Directive is to facilitate the investigation, detection and prosecution of serious crime, including terrorism, Ireland considered it should have been a third pillar legal instrument. The case opposed thus Ireland to the Council and the EP, which were eventually to be supported inter alia by the European Commission and the EDPS. On 10 February 2009, the CJEU delivered its judgement for the case, upholding the first pillar legal basis of the DRD.[357]

- 2011: Problems recognised by European Commission

In April 2011, the European Commission published a report on the evaluation of the application by Member States of the DRD, and of its impact on fundamental rights.[358] It observed that some national Constitutional Courts had annulled the legal instruments transposing the Directive because of their non-compliance with fundamental rights. Based on its evaluation, the European Commission announced the future proposal of amendments to the text.

3.2.4. Large-scale databases

In this section is considered the development of the VIS are the SIS II, two large-scale databases which, together with Eurodac, are expected to be managed by the soon to be established European Agency for the operational management of large-scale IT systems. The place that these large-scale databases have in the wider EU data-processing patchwork and the challenges that the programmatic policy making characterizing their establishment and nature pose to data protection have been addressed in chapter 2. This section considers the position that the EP has played in relation to three different aspects of the debates surrounding them: a) the legislative design of the databases, and of the granting access to the data that they contain to law enforcement authorities; b) the question of the 'interoperability' of EU large-scale databases; and c) the creation of the above-mentioned IT Agency.

---

[353] European Parliament, *Legislative Resolution of 14 December 2005 on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)), P6_TA(2005)0512.

[354] Ibid., § 2.

[355] Ibid., §3.

[356] European Parliament and Council of the European Union, Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54-63.

[357] Court of Justice of the European Union, Case C-301/06, *Ireland v. European Parliament and Council of the European Union,* 10 February 2009

[358] European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM(2011) 225, 18.4.2011, Brussels.

a) The design of SIS II and VIS and access to their data

The EP has been involved in the legislative tailoring of these two databases through various paths, as the legal instruments relating to them have fallen under both the first and the third pillar (and the boundaries between them have changed over time).

The SIS is the largest database in the EU. In 2001,[359] the European Commission was given a mandate to develop an expanded version of it, SIS II, to come into force in March 2007. In 2003, the Council decided to include biometric data in the future SIS II. On 20 November 2003, the EP adopted a Recommendation to the Council on SIS II[360] expressing that the Council should ensure that any extension of the SIS was accompanied by the highest standards of data protection, paying particular attention to the human rights implications and dangers inherent in the inclusion of biometric data. The EP overtly objected to any possible exception of the purpose limitation principle, such as, for instance, grating to some authorities the possibility to use SIS data for purposes other than the purpose for which they had been originally introduced in the SIS, as already discussed by then by Council.[361] The EP, incidentally, also suggested that a detailed study should be undertaken about the feasibility of merging existing or future EU-wide databases through a single technical platform for a 'Union Information System', which should evolve to encompass future system needs in all relevant areas.[362] The Recommendation was adopted having regard to a Report adopted by the LIBE Committee on 7 November 2003, which included a Minority Opinion[363] where it was stated that "the discussed changes to the SIS have serious and alarming repercussions on the fundamental right of European citizens to data protection and privacy, creating a risk for abuse and legal vacuums".

In 2004, the Council established the VIS as a system for the exchange of visa data between Member States, and gave to the European Commission the mandate to prepare the technical development of VIS and to provide the required legislative basis.[364] The aim was to set up a central database and a system of exchange of information concerning short-stay visas, and thus to lead to the storage in a centralised database and to exchanges of data, including biometric data, concerning a vast number of persons. To define the exact purpose, functionalities and responsibilities for the VIS, and to establish the conditions and procedures for the exchange of visa data between Member States, a Regulation was drafted.

The VIS Regulation was to be complemented by another legal instrument, adopted under the third pillar, in order to grant access to VIS to internal security authorities, including EUROPOL. In November 2005, the European Commission presented a proposal for a Council Decision for this purpose.[365] On 7 June 2007, the EP adopted a legislative resolution on the proposal,[366] incorporating amendments related to the protection of personal data, in particular to ensure purpose limitation, and the rights of the individual. The EP portrayed as a necessary prior condition for the adoption of the instrument the strengthening of third-

[359] Council of the European Union, Regulation (EC) No 2424/2001.

[360] European Parliament, *Recommendation to the Council of 20 November 2003 on the second-generation Schengen information system (SIS II)*, P5_TA(2003)0509.

[361] Ibid., § 1.

[362] Idem.

[363] Of Marco Cappato and Maurizio Turco, adopted pursuant to Rule 161(3) of the Rules of Procedure.

[364] Council of the European Union, *Decision 2004/512/EC establishing the Visa Information System (VIS)*, (CNS/2004/0029)

[365] Jay, R., *Data Protection Law and Practice*, London, Sweet & Maxwell, 2007, p. 732.

[366] European Parliament legislative resolution of 7 June 2007 on the proposal for a Council decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by EUROPOL for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

pillar data protection.[367] The instrument granting access to VIS to EUROPOL was finally adopted as Council Decision 2008/633/JHA.[368]

The EP was also involved in the legislative procedure for the amendment of the Regulation as regards the use of the VIS under the Schengen Borders Code.[369] This took place under 'ordinary' co-decision procedures, allowing for a full involvement of the EP, which supported the strengthening of data protection and procedural rights.

The European Commission had introduced a legislative package for SIS II in 2005. It was composed of different proposals, with different legal bases: a proposal for a Council Decision contained specific provisions regarding the use of SIS II data for supporting police and judicial cooperation in criminal matters,[370] and a Regulation was to set the rules on the processing of SIS II data supporting the implementation of policies linked to the movement of persons.[371] The complex negotiations, which took place through 'trialogue' meetings, led to a final compromise text, reached between the EP, the Commission and the Council on 27 September 2006. The compromise position leading to an adoption at first reading was adopted at the plenary sitting of 25 October 2006,[372] proving the relative success of EP's determination for the strengthening of data protection provisions for SIS II. The outcome was however much more mitigated in relation with EP initial concerns concerning the use of biometrics and the harmonisation of grounds for listing.

A major concern for the EP during the recent years has been the troubled implementation of both SIS II and VIS, as they have been significantly delayed, and are still not operational – even though VIS is expected to start operating in autumn 2011. In October 2004, the European Commission had launched the implementation of SIS II and the VIS by signing a contract for their development. The EP was notably called to back up the extension of the European Commission's mandate to ensure the implementation of SIS II.[373] On 22 October

[367] European Parliament, *Recommendation to the Council of 14 December 2006 on the progress of the negotiations on the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, § 1(q).

[368] Council of the European Union, *Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by EUROPOL for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, OJ L 350, 30.12.2008, pp. 138-149. The resolution was adopted on the basis of a Report by the LIBE Committee in which support to the Council Decision was linked to the commitment by the Council to provide in the short term a new data protection instrument for the third pillar (Report on the proposal for a Council decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by EUROPOL for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, Rapporteur: Sarah Ludford, 21.05.2005).

[369] See, notably: European Parliament, *Legislative resolution of 2 September 2008 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code* (COM(2008)0101 – C6-0086/2008 – 2008/0041(COD)), P6_TA(2008)0383.

[370] European Commission, *Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*, COM(2005) 230 final, Brussels, 31.05.2005.

[371] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II)*, COM(2005) 236 final/2, Brussels, 23.08.2005.

[372] European Parliament, *Legislative resolution of 25 October 2006 on the proposal for a Council decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*, P6_TA(2006)0447.

[373] See, in this sense: European Parliament, *Legislative resolution of 24 September 2008 on the draft Council decision on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)* (12059/1/2008 – C6-0188/2008 – 2008/0077(CNS)), P6_TA(2008)0441.

2009, the EP adopted a Resolution on progress of SIS II and VIS[374] noting the slow advance, and stressing that MEPs should be kept constantly informed of the state of play as regards the deployment of both databases.

b) The 'interoperability' notion and large-scale databases

Since 2004, both the European Council and the Council called upon the European Commission to submit proposals for enhanced interoperability and synergy among European databases. The step was finally undertaken by the European Commission in 2005 with a proposal[375] that focused on the "interoperability" between VIS, SIS and Eurodac, describing such notion as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge", and asserting that the concept was "technical rather than...legal".[376]

The EP has not manifested over the years any particularly coherent position on this issue. As already advanced, in 2003 it voted in favour of studying the feasibility of merging existing or future EU-wide databases through a single technical platform.[377] In June 2005, however, an EP Resolution[378] laconically stated that the EP alerted "the Council to the risks posed by the interoperability of information systems".[379] A Proposal for a Recommendation to the Council on interoperability and synergies among European databases in the AFSJ[380] was introduced in 2006, calling for a political debate on the notion, but did not go forward.

By the end of the 2000s, discussions on the notion of 'interoperability' were progressively abandoned by EU institutions, which appeared to focus instead on stocktaking, in particular by listing and examining the information systems already in place or in the pipeline. In its Resolution on the Stockholm programme of 16 November 2009,[381] the EP expressed concern with the launching of any additional border management instruments or large-scale data storage systems, pointing out that no additional tool should be developed until those already existing were not fully operational, safe and reliable, and calling for a thorough assessment of the necessity and proportionality of any new instruments.[382] In July 2010, the European Commission published a Communication on information management in the AFSJ[383] in which it declared that principle of purpose limitation, one of the basic data protection principles, "appears to be a core factor in the design of EU-level information management measures", but "with the exception of" SIS, SIS II and VIS.[384] The EP did not react to this finding according to which one of the central EU data protection principles is not respected by what are to become the most extensive databases of the EU.

---

[374] European Parliament, *Resolution of 22 October 2009 on progress of Schengen Information System II and Visa Information System*, P7_TA(2009)0055.

[375] European Commission, *Communication from the Commission to the Council and the European Parliament: On improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597, 24.11.2005, Brussels.

[376] Ibid., p. 3.

[377] European Parliament, Recommendation to the Council of 20 November 2003 on the second-generation Schengen information system (SIS II), § 1.

[378] European Parliament, *Resolution 8 June 2005 on progress made in 2004 in creating an area of freedom, security and justice (AFSJ)*.

[379] Ibid., § 34.

[380] European Parliament, *Proposal for a Recommendation to the Council of 8 June 2006, by Alexander Alvaro, on behalf of the ALDE Group on interoperability and synergies among European databases in the area of justice and home affairs*, PE 374.607v01-00.

[381] European Parliament, *Resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme.*

[382] Idem, § 72.

[383] European Commission, *Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, 20.7.2010, Brussels.

[384] Ibid., p. 22.

c) The IT agency

Just as it started refraining from using the expression of 'interoperability of information systems', the European Commission began to sketch out the creation of an Agency that would de facto give flesh to such feature: in June 2009, it introduced a proposal for the establishment of an agency for the operational management of large-scale IT systems in the AFSJ,[385] the core function of which will be the management of SIS II, VIS and Eurodac, as well as upcoming IT systems in the AFSJ (to be determined). The proposal was modified in 2010 to change its legal basis, following the entry into force of the Lisbon Treaty.[386]

In October 2010, an orientation vote took place in the LIBE Committee and a mandate was given to the Rapporteur to negotiate on the proposal in 'trialogue' meetings with representatives of the European Commission and of the Council, with the view to reaching an agreement at first reading. During the negotiations, discrepancies emerged between the Legal Services of the EP, on the one hand, and of the Council and the European Commission, on the other, the EP Rapporteur agreeing to accept the solution supported by the Council and the European Commission for the sake of compromise.[387] On 5 July 2011, the EP adopted a legislative resolution[388] on the amended proposal for a Regulation, granting support to the initiative, even if proposing a series of amendments that reinforce its right to be informed by the new Agency and that detail a series of data protection provisions, notably on the responsibilities of the EDPS. In its Resolution of 6 July 2011 on the Commission Work Programme 2012,[389] the EP called on the European Commission "to complete the establishment of the SIS II system, VIS and Eurodac, as well as the new IT agency".[390]

3.2.5. FRONTEX and personal data processing

FRONTEX was created in 2004 with the aim of coordinating and assisting Member States' action in the surveillance and control of the external borders of the EU. For many years there was limited debate on whether data processing carried out by FRONTEX presented particular risks in terms of the assurance of personal data protection, the main question being, at the time, whether FRONTEX as such was responsible for the processing personal data of individuals identified during 'joint operations' carried out by national authorities under its umbrella, or whether such data processing was the sole responsibility of the national authorities involved. The original FRONTEX Regulation did not have any specific provisions on personal data processing, the Agency being nevertheless subject to Regulation (EC) 45/2001 when processing personal data in the exercise of its activities falling under EC law.

---

[385] Formally, split into two proposals: European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, COM(2009) 293 final, 24.6.2009, Brussels; and European Commission, *Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty*, COM(2009) 294 final, 24.6.2009, Brussels.

[386] The two mentioned texts were replaced by: European Commission (2010), Amended Proposal for a Regulation (EU) No .../... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2010)93 final, Brussels, 19.03.2010.

[387] Council of the European Union, *Note from the Presidency to the Mixed Committee at the level of Senior Officials on Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice: Possible agreement with the EP*, 30 May 2011, Brussels, p. 4.

[388] European Parliament, *Legislative resolution of 5 July 2011 on the amended proposal for a regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice* (COM(2010)0093 – C7-0046/2009 – 2009/0089(COD)), P7_TA(2011)0304.

[389] European Parliament, *Resolution of 6 July 2011 on the Commission Work Programme 2012*

[390] Ibid., § 50.

More recently, however, the issue of personal data protection and FRONTEX took a new dimension as the European Commission embarked in supporting the reinforced integration of EU instruments related to 'border management', including FRONTEX, as well as EUROSUR (the European Border Surveillance System) and a number of possibly upcoming systems relying on the massive processing of data related to individuals, with the view of the gradual establishment of a European integrated border management system. In light of these developments, the EP expressed on 18 December 2008[391] its concern "that third-country nationals may lack adequate means to monitor whether personal information on them gathered in the planned 'system of systems' of the EU is handled in accordance with the principles of data protection law applicable in the Union", and called on the European Commission to clarify to what extent personal data processed in this area would be made available to third countries.[392]

In February 2010, the European Commission presented a Proposal for a Regulation amending the existing provisions on FRONTEX.[393] The EC explicitly departed from the recommended options in the Impact Assessments preceding the draft, by disregarding suggestions to allow FRONTEX to carry out data processing activities for the purpose of the fight against criminal networks organising illegal immigration, and preferring instead to frame any new competences related to the processing of personal data by the Agency in the wide context of the EU strategy for information exchange.[394]

In March 2011, the LIBE Committee had an orientation vote on the proposed measure as discussed in the Council, which had notably modified the text in order to explicitly allow the transmission of personal data from FRONTEX to EUROPOL. The orientation vote supported such transmission, although only if to take place on a case by case basis. In June 2011, the Council and the EP reached a political agreement on the proposal, negotiated in 'trialogue' meetings between the Council Presidency, the EP and the European Commission. The new rules incorporated strengthened provisions for the protection of fundamental rights, including the establishment of a Consultative Forum on Fundamental Rights and the designation of a Fundamental Rights Officer; and reinforced tasks for the agency as regards risk analysis (i.e. to regularly assess the capacity of member states to face upcoming challenges at the external borders). They also included the possibility to transfer on a case by case basis personal data to EUROPOL and other EU law enforcement agencies regarding persons suspected of involvement in cross-border criminal activities, facilitation of illegal immigration activities or in human trafficking activities, and ad-hoc data protection provisions for such transfers.[395]

In its Resolution of 6 July 2011 on the Commission Work Programme 2012,[396] the EP asserted that it "shares the idea that FRONTEX will play a major role in border control management and welcomes the agreement on the modification of its legal framework to enable it to be more effective in terms of its operational capacity on the external border".[397]

---

[391] European Parliament, *Resolution of 18 December 2008 on the evaluation and future development of the FRONTEX Agency and of the European Border Surveillance System (EUROSUR)* (2008/2157(INI)), P6_TA(2008)0633.

[392] Ibid., § 19.

[393] European Commission, *Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX),* (COM(2010) 61), 24.2.2010, Brussels.

[394] Idem, p. 4.

[395] See: European Parliament, *Draft report of Simon Busuttil (PE450.754v01-00) on the proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) (Amendment 255: Consolidated text resulting of a compromise between the rapporteur, the shadow rapporteurs, the Council and the Commission)*, 2010/0039(COD), 6.7.2011.

[396] European Parliament, *Resolution of 6 July 2011 on the Commission Work Programme 2012*

[397] Ibid., § 52.

3.2.6. Body scanners

The last selected case study refers to the authorisation by EU institutions of the deployment in EU airports of screening machines originally known as 'body scanners', and eventually re-baptised by the European Commission as 'security scanners'.

- 2008: The EP stops the European Commission

The EU's legal framework for aviation security lists various screening methods and technologies that Member States can allow in their airports for passengers' screening. On 5 September 2008, the European Commission proposed to the Council and the EP a draft Regulation that was to include in the list a mention of 'body scanners' to automatically screen passengers. On 23 October 2008, however, the EP adopted a Resolution[398] denouncing the fact that the European Commission had advanced the draft measure through a 'comitology' procedure; in its view, the draft measure was far from being technical and, taking into account its serious impact "on the right to privacy, the right to data protection and the right to personal dignity",[399] it needed to be accompanied by strong and adequate safeguards. The EP notably set a three-month deadline for the European Commission to carry out an impact assessment relating to fundamental rights, and to consult the EDPS, the WP29 and the FRA on the subject.[400] As a first response, the European Commission agreed to withdraw the scanners from the original legislative proposal. Body scanners, nevertheless, were eventually put in place in several European airports, allowed by different Member States as trial measures.

- 2010: The European Commission reformulates proposal, with the support of the EP

In June 2010, the European Commission adopted a report on body scanners, then re-baptised as 'security scanners', which proposed an assessment of their compliance with fundamental rights.[401] Its essential argument was that the fundamental rights concerns raised by the machines, and in particular regarding compliance with personal data protection requirements, could be solved by technical adjustments of the products.[402] The European Commission noted, concretely, that it was technically possible to produce instead of real images of the bodies only a 'mannequin' image, which could be considered as not being data relating to any 'identified' or 'identifiable' person, and thus not 'personal data' in the sense of EU data protection law. This fact had been put forward to the European Commission by a manufacturer of body scanners that had changed their design in response to the EP Resolution of October 2008.

In a Resolution voted on 6 July 2011,[403] the EP expressed it support for the European Commission to add 'security scanners' to the list of authorised screening methods, under some conditions and after "the impact assessment that the European Parliament requested in 2008 has first been carried out which demonstrates that the devices do not constitute a risk to passenger health, personal data, the individual dignity and privacy of passengers and the effectiveness of these scanners".[404] The key condition for the EP was that "all security scanners should make use of a stick figure to protect passengers' identities and to

---

[398] European Parliament, *Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection*, P6_TA(2008)0521.

[399] Recital D of European Parliament, *Resolution Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection*.

[400] § 1 of Resolution P6_TA(2008)0521.

[401] European Commission, *Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports*, 15.6.2010, Brussels.

[402] Ibid., p. 12.

[403] European Parliament, *Resolution of 6 July 2011 on aviation security, with a special focus on security scanners* (2010/2154(INI)), P7_TA(2011)0329.

[404] Ibid., § 9.

ensure that they cannot be identified through images of any part of their body".[405] It also called for the European Commission to disregard the 'comitology' procedure and fully involve the EP in this field through co-decision.[406]

The Resolution was voted having regard to a report of the Committee on Transport and Tourism and the opinions of the Committee on the Environment, Public Health and Food Safety and the LIBE Committee. The report notably expressed satisfaction with the assessment of the European Commission in its 2010 Communication.[407] On the contrary, the LIBE Committee had detailed a long series of requirements that it considered necessary for any impact assessment on which could be grounded the decision to deploy the use of body scanners, to cover

> inter alia, the fundamental rights aspect of body scanners, the proportionality and necessity, taking into account the added value for the fight against terrorism, the costs incurred as a result of the acquisition, installation and operation of body scanners and the possible health risks to passengers and staff members, in particular vulnerable passengers and staff members, also having regard to the opinions of the European Union, international and national human rights and DPAs, such as the EDPS, the WP29, the FRA, the World Health Organisation and the UN Special Rapporteur on the Protection of Human Rights while Countering Terrorism.[408]

3.3. Analysis of the EP's involvement

The recalling of the historical involvement of the EP and the description of six selected recent controversies have illustrated the fact that the EP has been engaging in the assurance of the privacy and personal data protection in the EU through a number of legislative and non-legislative mechanisms, defending various priorities, and with the support or the resistance of different actors. This section describes the crucial features of such involvement, from a wider perspective.

3.3.1. Institutional aspects

For many years, the EP's contribution to the assurance of personal data protection in the AFSJ has been characterised by an overlapping of institutional and substantial concerns. Both issues are actually deeply interlinked and it could be argued that the EP has granted much attention to a strengthening of its own role in the EU institutional framework in general, and in the AFSJ in particular, for the purpose of better promoting and protecting fundamental rights, including the protection of personal data.

It is a well-known fact that all through its history the EP has been particularly active to advance and to defend its competences under the Treaties. The controversies described confirm that, in the pre-Lisbon Treaty era, the EP has regularly fought to strengthen its legislative role, be it by aiming at clearly circumscribing the scope of application of 'comitology' procedures; by reacting against what has sometimes been perceived as 'venue shopping' by the Council (or the possibility to play with the some arbitrary boundaries between the First and the Third pillar); or by asserting its prerogatives in relation with the conclusion of international agreements. The EP, significantly, has even instigated legal action to advance in this direction, even if not always with the expected results, as illustrated by the 2006 PNR judgement.

---

[405] Ibid., § 31.

[406] Ibid., § 56.

[407] European Parliament, *Committee on Transport and Tourism, Report of 1 June 2011 on aviation security, with a special focus on security scanners* (2010/2154(INI)), Rapporteur: Luis de Grandes Pascual, A7-0216/2011.

[408] European Parliament, *Opinion of the LIBE Committee for the Committee on Transport and Tourism on aviation security with a special focus on security scanners* (2010/2154(INI)), 27.04.2001, Rapporteur: Judith Sargentini, § 21.

It appears, however, that there is no linear relationship between a reinforced involvement of the EP in decision-making and a strengthened EU legal protection of personal data. The EP has over the decades been instrumental in some key advances of the EU data protection legal framework – its contribution to the recognition of right to the protection of personal data as a fundamental right in a legally binding EU Charter testifies of its achievements. But there are also some concrete examples that would tend to suggest that the EP support for a high level of personal data protection in the EU is negatively affected by the expansion of its competences. It was the case with the adoption of the DRD, for instance: the EP formally rejected a third pillar instrument on data retention, but made a u-turn on its substantial concerns as soon as the chosen instrument was changed, and its legislative role transformed.

In the light of this qualification, and as the Lisbon Treaty has partially solved some of the institutional tensions that had been vehemently criticised by the EP, it remains to be seen whether the recent institutional advances are to translate in fully corresponding substantive advances. An example of a debate into which the EP has already applied the new, post-Lisbon formal mechanisms at its disposal is the conclusion of international agreements, for instance regarding the US TFTP agreements. The EP'd refusal to assent to the first TFTP Agreement gave a strong signal to other institutions, and to the US negotiators, on the EP's intention to stand firmly for the protection of the fundamental rights of the individual, such as privacy and the protection of personal data. In contrast, the assent given to the second TFTP Agreement, transmitted a much more ambivalent signal. The real added value of the 'improvements' on which the EP grounded its change of position is subject to debate, and in any case they did not appear to satisfy the totality of previous EP concerns, and certainly not the concerns of relevant actors such as the EDPS.

In any case, the progress achieved with the entry into force of the Lisbon Treaty appears as not being sufficient in itself to allow the EP to ensure that privacy and the protection of personal data are duly taken into account at all stages of decision-making, especially insofar as the AFSJ is concerned. Coming back to issue of international agreements, the obligation for the Council to obtain the assent of the EP in an increased number of circumstances is an important institutional breakthrough for the EP, but, nevertheless, it still circumscribes the EP input to a very specific moment in time (the conclusion of the agreement), and to a highly specific question (whether to accept or to refuse an already negotiated agreement). The challenge becomes then for the EP to be able to use this veto power in order to expand its participation upstream, for instance by insisting on the need for MEPs of being kept informed on the development of negotiations leading to the draft of agreements, and by warning of the scrutiny to come at the moment of the assent request,[409] as well as downstream, by trying to get incorporated into the agreements mechanisms that could allow for EP action in case of dissatisfaction with the implementation and execution of the agreement, for example.

3.3.2. Substantive concerns

The recurrent overlap of institutional and substantive concerns in the EP and their implications for privacy and data protection issues related to the AFSJ does not facilitate the identification of the specific concerns of the EP regarding EU policies in the area. Moreover, the EP acts more often than not reactively, in response to initiatives or decisions undertaken by the European Commission and the Council, as opposed to proactively. Therefore, any inventory of the points at issue more that are explicitly highlighted by the EP on a regular basis (which should inevitably include, for instance, the principles of

[409] In its Resolution on the Commission Work Programme 2012, for instance, the EP "calls on the Commission to respect EU data protection when negotiating with third countries, stressing that Parliament will carefully scrutinise all proposals, including EU-PNR and an EU system for extraction of financial data and any EU PNR agreements with third countries (with negotiations currently underway with the US, Canada and Australia) for their compliance with fundamental rights" (European Parliament, Resolution of 6 July 2011 on the Commission Work Programme 2012, § 53).

proportionality, and the purpose limitation principle)[410] is to leave undecided the question of whether these points are, per se, the major issues for the EP in relation with privacy and data protection in the AFSJ, or whether they have simply happened to be the privacy and data protection principles more frequently threatened in the AFSJ by the Council and the European Commission.

As has been highlighted in this study, an issue that has been put repeatedly high on the agenda by the EP is the question of the level of personal data protection in the area of police and judicial cooperation in criminal matters (data protection in the ex-third pillar). It was actually the EP that pushed for this file to be addressed by European Commission and the Council, and, despite its limited powers in the third pillar, it has again and again referred to its importance also when discussing other data protection and privacy issues, from international agreements to first pillar legal instruments, in many occasions trying to frame it as a necessary pre-condition for the adoption to different EU data processing measures.

A search for the distinct privacy and data protection concerns of the EP leads in any case inevitably also to the issue of profiling already discussed in chapter 2 above. The EP has been the only major EU institution that has put on the table the need to address profiling and its consequences for the assurance of fundamental rights in the AFSJ. This stance is fully consistent with the position of the Council of Europe, which recently adopted a recommendation on the subject.[411] This, as we have previously argued, stands in contrast with the positions taken by the Council and the European Commission, which have systematically resisted to do so, to the extent of even avoiding the use of the very term 'profiling'.

Profiling, like many other data protection and privacy issues, is actually a horizontal matter that has been addressed by the EP both in regards to behavioural advertising (under ex-first pillar rules) and in relation with police and judicial cooperation in criminal matters (ex-third pillar). In its Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the EU,[412] the EP pointed out "that profiling is a major trend in the digital world, owing not least to the growing importance of social networks and integrated internet business models; calls on the Commission, therefore, to include provisions on profiling, while clearly defining the terms 'profile' and 'profiling'".[413]

This is not to say, however, that there might be at the EP a fully coherent approach to profiling. In another Resolution adopted the same day,[414] and in spite of divergent positions embraced in the context of PNR agreements with third countries and TFTP, the EP "(c)alls on the Commission and Member States to develop an integrated risk-analysis system for passengers who may with good reason be suspected of being a security threat and for

[410] In addition to the cases already discussed, can be mentioned, as another recent example of the EP support for the purpose limitation data protection principle, its involvement through co-decision in the legislative process to lead to a Directive on the cross-border exchange of information on road safety (see, notably European Parliament, Legislative Resolution of 6 July 2011 on the Council position at first reading with a view to the adoption of a directive of the European Parliament and of the Council facilitating the cross-border exchange of information on road safety related traffic offences (17506/1/2010 – C7-0074/2011 – 2008/0062(COD), P7_TA(2011)0325).

[411] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 23 November 2010.

[412] European Parliament, *Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union*, (2011/2025(INI)).

[413] European Parliament, *Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union*, § 18.

[414] European Parliament, *Resolution of 6 July 2011 on aviation security, with a special focus on security scanners* (2010/2154(INI)), P7_TA(2011)0329.

checks on luggage and cargo, based on all available, reliable information, in particular that provided by the police, intelligence services, customs and transport undertakings".[415]

Another striking feature of the EP approach to privacy and data protection issues is that, despite its notable contribution to the recognition of personal data protection as a fundamental right in the now legally binding EU Charter, it has relied only very timorously on the specific nature of this right, and on the mandatory strength of the instrument. The EP seems indeed to be (still) much more familiar with the requirements of Article 8 of the ECHR on the right to respect for private life, and the Strasbourg case law thereof, than with the content of Article 8 of the EU Charter on the protection of personal data, and the Luxembourg case law about it. Confirming the EP's awareness with Article 8 of the ECHR can be mention the attention it grants to the issue of proportionality, that it has often linked to issues of transparency. As evidence of its more limited acquaintance with the specificities of Article 8 of the EU Charter, can be mentioned the absence of references to the requirement of Article 8(3) concerning independent supervision, for instance, in particular of its endorsement of EUROPOL as a legitimate actor to assess compliance with the access requests by US authorities of EU financial data.

Perhaps more crucially, the EP has failed to effectively challenge the factors underpinning the deployment of policy initiatives that threaten the rights to personal data protection and privacy in the EU. Despite questioning the proportionality and necessity of specific data processing measures, it has not yet convincingly addressed the links between contemporary transformations of policing, current discussions on future EU-wide information exchange models, and massive data processing practices supported in the context of the 'EU integrated border management'. In this sense, and in spite of some punctual warnings on the implications of these developments, the EP is ultimately not opposing a series of steps towards the design of a decentralised but dense network of data transfers which establishes EUROPOL, FRONTEX and other EU agencies such as the IT agency as major nodal points, and the law enforcement and intelligence authorities of Member States, but also of third countries, as associated components.

[415] Ibid., § 4.

4. NEW DATA PROTECTION PRINCIPLES AND ELEMENTS FOR THE EU SECURITY ENVIRONMENT

KEY FINDINGS

- EU data protection rules in security and law enforcement matters are currently fragmented. Police and judicial cooperation in criminal matters are excluded from the scope of the DPD. The DPFD adopted in 2008 only applies to cross-border data processing. It provides for exemptions to all established principles on data protection, and is flanked by a number of sector-specific rules adopted in the legal instruments related to the SIS, EUROPOL, EUROJUST and the Prüm Decision.
- The proposals tabled by the European Commission for a comprehensive legal framework, which have been partially endorsed by the EDPS, the WP29 and the European Parliament, envisage the possible extension of this framework to police and judicial cooperation in criminal matters.
- The imminent accession of the EU to the ECHR is expected to benefit the consideration of data protection principles. Although no explicit mention of the right to data protection is made in the text of the ECHR, the ECtHR has strongly linked data protection principles to the development of the right to privacy, as set out in Article 8 of the Convention. The ECtHR has issued extensive case law in the field, rigorously applying the criteria of the necessity and legitimacy of the processing. In addition, it is not restricted in examining AFSJ data processing by any of its statutes. Even before the accession takes place, however, EU institutions must ensure that the level of protection granted to individuals does not restrict or adversely affect human rights as recognised in the ECHR and as interpreted by the ECtHR case law.
- From a law-making point of view, two conceivable ways forward may be identified at this stage: i) either a new, single, comprehensive, standard-setting text will be introduced that will set the general rules for all personal data processing within the EU; or ii) processing not related to police and judicial cooperation in criminal matters, on the one hand, and processing in such fields, on the other, shall remain separate within the EU, through the continued existence of the DPD and the DPFD respectively, properly amended in the post-Lisbon environment. Although the merits and drawbacks of each option are elaborated, either option matters little as far as effective personal data protection is concerned: what matters is that power configurations and the identified challenges to data protection are dealt with and controlled, regardless of the legal means through which this goal is achieved.
- Concerning the *profiling society environment*, specific emphasis should be placed on the foreseeable orientations in data processing for security purposes to ensure that the data protection framework is robust and long lasting. The new DPF should develop a set of legal principles governing profiling in the EU's AFSJ. A definition of profiling should be included in the revised framework. This definition should also include the types of profiling that should be definitely prohibited under all circumstances and solid legal safeguards for those considered legitimate. The first type of profiling to be expressly prohibited is that which uses sensitive personal data as part of its basis. The second prohibition for profiling in the AFSJ should be on the use of unlawfully acquired data. Lastly, the profiling logic needs expressly to adhere to the general data protection principles, particularly that of fair and lawful processing.
- With regard to the *contemporary networking society*, the principles of transparency and openness are equally central at times of providing a concrete response to the challenges posed by AFSJ data processing policies, systems and practices.

Nevertheless, so far law enforcement processing has been granted a wide margin for exceptions. Because transparency mechanisms such as the notification system or the right to information and access or even the oversight by an independent authority could be said to hinder police work, substantial derogations have been granted in favour of such processing. The amended EU DPF needs to make explicit reference to these principles. Their implementation in practice might require changing the structure of coordination and cooperation among DPAs with competences for supervising data processing practices in the AFSJ (or further strengthening and developing the role of the current WP29) or reversing the burden of proof in data protection litigation in favour of data subjects.

- The principle of accountability is of central importance in AFSJ personal data processing. To create added value in the amended EU DPF, this principle needs to address such questions as how to reconcile the need for specificity with a general principle and how to resolve the issue of scalability or proportionality. After all, the requirement for the introduction of accountability checks in AFSJ processing is particularly important given the actual, perhaps unrecognised, role of individual consent; increased accountability checks for data controllers warrant the efficient protection of individual rights.
- With respect to AFSJ data processing, the DPF in effect enables individuals to seek redress against law enforcement agencies that have unlawfully processed their data. Yet this right may ultimately prove useless if individuals are not afforded the proper means to build up and prove their case. This seems to be a nearly impossible task under the EU DPF in a practical sense. Individuals need to collect evidence and establish jurisdiction – tasks that are difficult to accomplish and potentially expensive. Similar difficulties met in the DPD context have led to discussions about introducing a 'closest to home' individual right of redress. Such a right ought to be extended in AFSJ processing as well.
- Because the EU DPF review process is ambitious in scope, it needs to remain focused on primarily addressing the basic contemporary issues in data protection. In personal data processing in the AFSJ, it could make use of existing data protection means or those that are newly devised and presently under consideration (mostly in the DPD review context).

- The list of the fair information principles, as developed in the text of the DPD, needs to be extended to cover AFSJ processing as well.

- New ideas currently elaborated in the DPD review context, such as the introduction of DPIAs and the implementation of privacy-by-design system architecture could prove of particular value for data protection purposes in AFSJ processing as well. The role of national DPAs, while monitoring and controlling AFSJ personal data processing, needs to be strengthened in the amended EU DPF. The introduction of a central coordination mechanism of supervisory authorities in the AFSJ, such as the WP29, is crucial for data protection purposes.

- Comprehensive provisions on data protection and the EU Charter should be integral to the legal mandates of all EU home affairs agencies, requiring full compliance with the principles of purpose limitation, purpose specification and rights for the data subject to access and correct the personal data held by agencies. Legal provisions must be accompanied by a robust supervisory mechanism that would ensure the practical delivery of these common principles and standards. The above-mentioned establishment of an independent, central, coordinating authority for AFSJ processing compliance with data protection and privacy in the EU would constitute the proper approach for attaining this goal.

4.1. Introduction

What is the current legal framework for data protection in AFSJ[416] personal data processing and what framework *could* be created in the near future? This chapter addresses these two questions, taking into account the lack of regulatory clarity of the new EU DPF under construction. The chapter borrows some of the ideas developed in the current review process of the 1995 DPD. It ponders whether some of the new ideas pertaining to this instrument (not related to AFSJ personal data processing under the former third pillar) are useful for regulating future AFSJ personal data processing and going beyond the limited scope of the 2008 Data Protection Framework Decision (DPFD, 2008/977/JHA) – a more recent text that can hardly be looked at as little more than a starting point for a more comprehensive regulation. The chapter assumes that there will be a reform of the DPFD alongside the ongoing review process of the DPD. Although this reform is not officially on the EU's law reform agenda, it does occupy some part of it, appearing to be a more or less unexpected side effect of the DPD review process. This chapter defends the view that reform of the DPFD is needed for the substantive reasons below.

In section 4.2, this chapter discusses the multitude of existing regulatory texts (of various legal statuses with no straightforward interrelation), the case law that introduces more finely constructed criteria, and the extensive documentation (consultations, guidelines, opinions) of yet unidentified, or even unidentifiable, power that in effect make up the EU's DPF regulatory patchwork in AFSJ personal data processing today. In practice, they all add up to a system that is extremely complex and difficult to follow for the protection of the (by now fundamental within the EU) individual rights to data protection and privacy.

The complexity of the system was probably to be expected, given the pillar structure characterising AFSJ cooperation in the pre-Treaty of Lisbon environment. Commercial data and other non-security-related processing was distinguished from data processing in the area of police and judicial cooperation in criminal matters, and each was regulated by different instruments, with a more visionary and general regulatory approach with regard to the former. Security data processing largely did not attract much legislative interest at the EU level until the 9/11 events. After that, and the subsequent acts of political violence in some EU capitals, security-related personal data processing gained exponentially in importance and today is regulated by a plethora of not always fine-tuned regulatory instruments.

Still, as explained in chapter 1 of this study, in the post-Lisbon landscape new options have been created for individual data protection, such as the accession of the EU to the ECHR, while the relationship between already familiar notions like privacy and data protection is currently undergoing a process of redefinition.

Meanwhile, the distinction between 'commercial' and 'security' personal data processing has mostly proven to be schematic. The boundaries between the processing of personal data for security purposes, particularly when originally collected for commercial purposes, despite important relevant case law, remain mostly blurred.[417]

---

[416] This chapter uses expressions such as 'data processing in the field of police and judicial cooperation' and 'AFSJ personal data processing' without making any distinction.

[417] See for instance PNR-related processing, that was found security-related despite the fact that data are collected by airline carriers for commercial purposes (see Papakonstantinou, V. and De Hert, P., "The PNR Agreement and Transatlantic anti-Terrorism Co-operation: No Firm Human Rights Framework on either Side of the Atlantic", Common Market Law Review 46 (2009: 885-919), while the retention of telecommunications data, equally collected by telecommunications providers for commercial purposes, have been judged as commercial processing (as established by the Court of Justice of the European Union in its Case C-301/06, *Ireland v. Parliament and Council*). On the other hand, it remains yet unclear how the 'depillarisation' emerging from the Lisbon Treaty shall affect personal data protection. For the time being, as put by the LIBE Committee (2010), it appears that

Security-related processing allegedly presents a series of unique characteristics that may make specialised regulations data protection necessary.[418] For instance, law enforcement agencies thrive on 'hearsay', and thus not on personal information that has been data quality-certified. Or they need to keep data forever if possible and correlate them incessantly. Or suspects need not have complete access to their files or even be informed that they are under police scrutiny until they are charged with a crime. Or the potential future uses for police information are unforeseeable. All of the above perhaps impose a special, accommodating regime of data protection for such processing.

During the EU DPF amendment process, two issues need to be clearly distinguished and dealt with separately: the law-making options and the real data protection issues at hand. Because discussions have often focused particularly on the need for a single regulatory instrument for data protection in the EU and how to achieve it, the need to adequately identify and deal with the current challenges in data protection is at risk of going unnoticed. In this context, it is submitted that the law-making options are ultimately less relevant to the actual data protection purposes; what is actually needed is to address the issues in an adequate way from the data protection perspective, regardless of the means for doing so.

In any event, with regard to the law-making options, the DPF review process needs to choose from two mutually exclusive options: whether to produce a single data protection instrument to regulate all and any personal data processing in the EU, or to maintain the current scheme of the DPD and the DPFD, properly amended in the post-Lisbon environment. The first option undoubtedly creates a much-needed, comprehensive environment of legal certainty for data subjects and data controllers alike. That notwithstanding, it will be demonstrated that in many cases a more effective law-making option would be to maintain and update the current DPD and DPFD system, because the required differentiations due to the special needs of each type of processing shall probably make a single instrument complicated and difficult to follow. On the other hand, the distinction between commercial and security processing remains far from straightforward. Particularly in the contemporary AFSJ environment, whereby law enforcement agencies routinely ask for and are granted access to datasets assembled in commercial-processing circumstances, the line between the two types of processing is blurred. The DPD and the DPFD, if maintained, shall always be found in conflict as to which is applicable each time.

With regard to the current dilemmas of data protection in AFSJ processing (which stem directly from those identified and examined in detail in chapter 2) that need to be dealt with during the DPF amendment process, this chapter discusses the necessity of addressing security-related profiling. More specifically, it looks at the need to create an environment of transparency and openness, the principle of accountability for law enforcement processing and individual access to justice.

The amendment process of the EU DPF perhaps appears over-ambitious in scope. It needs to include an update of the DPD, dating from the early 1990s, to the new Internet reality. It also needs to create a coherent and comprehensive system in AFSJ personal data processing. Each of these tasks would have been enormous to complete. Taking them up simultaneously risks disappointment or even failure. That is why the redefinition of today's

---

> [t]he working methods and 'mentalities', as well as political ambitions, for actors like FRONTEX are to become closer to 'old-third pillar' activities and ways of working (internal security matters) and even second pillar ones (external security/foreign affairs), which as we have seen above allow them to expand their degree of autonomy and margin of manoeuvre by avoiding democratic, political and legal accountability and the shadows of nationalism. …[T]he old third pillar spirit is not only very much present but it is also now contaminating other (formerly considered) first pillar areas.

See the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies FRONTEX, EUROPOL and the European Asylum Support Office, 2011, p. 98.

[418] After all, the "specific nature" of the judicial cooperation in criminal matters and police cooperation fields has been acknowledged in the Lisbon Treaty Declarations (21).

data protection tools or the employment of existing ones is indispensable during the DPF amendment process. In this context, this chapter examines the fair information principles, DPIAs, privacy by design and privacy-enhancing technologies (PETs), as well as the roles of national DPAs and the WP29.

4.2. Data protection in police and judicial cooperation in criminal matters: The EU's regulatory patchwork and role of the ECHR

The process for the review of the EU regulatory framework for data protection cannot be taken out of its institutional, legal context. The environment within which it takes place is at present one of increased complexity, as described in chapter 1. The Lisbon Treaty abolished the pillar system and formally turned the right to data protection into a separate fundamental right, through Article 8 of the EU Charter, distinct from the right to privacy. In addition, it enabled the EU to accede to the ECHR. In effect, the amended regulatory instrument, whenever released, shall essentially constitute the first attempt to incorporate the profound institutional changes brought by the Lisbon Treaty to the European data protection field. In the meantime, data protection regulations in the EU, especially with regard to security processing, proliferate. Relevant provisions may be found in various dedicated instruments or in those only incidentally related to data protection.

This section presents the state of play on police and judicial cooperation in the context of the upcoming revision of the EU data protection framework. It examines the position discussed by the European Commission in its 2010 Communication on the issue and surveys the stances adopted by other EU bodies and institutions: EU DPAs and particularly the EDPS, the Council and the EP. In addition, the potential effects on EU data protection arising from the EU's forthcoming accession to the ECHR are discussed, as well as the new articulation between the right to data protection and the right to privacy. Finally, the law-making options at this point are elaborated, mentioning the notions of the networking society and the profiling society.

4.2.1. The EU DPF: State of play

4.2.1.1. The Commission's approach to data protection in police and judicial cooperation in criminal matters

Police and judicial cooperation in criminal matters occupy a specific position in the field of data protection. The initial legislation on data protection was introduced, starting in the 1960s, in view of the growing reliance of state administrations on computer systems that enabled the massive and automated processing of personal data. During the 1980s and 1990s – when the DPD was adopted – the main preoccupation shifted towards the processing of personal data by private bodies for commercial purposes. Adopted after the entry into force of the Maastricht Treaty, Directive 95/46/EC reflected both these concerns and the specific institutional set-up of the EU. It dealt accordingly with first-pillar processing, while processing performed by judicial, police and security services (in the framework of the former third pillar) was explicitly left out.[419]

While the DPD set standards for commercial processing, no such EU standards existed in the field of police and judicial cooperation. This type of personal data processing gained in importance after 9/11. The terrorist attacks in several EU capitals further strengthened the request by security agencies, both within and outside the EU, to be provided with more extensive and efficient means to massively process the personal information of individuals

[419] Art. 3.2 excludes activities falling outside of Community law as well as "processing operations concerning public security, defence, State security […] and the activities of the State in the area of criminal law".

in order to facilitate their work.[420] Because of the favourable political and social environment,[421] such means were granted.

The DPFD was adopted on 30 December 2008. Until that time, standards were set rather by the Council of Europe's Convention 108 as amended by Protocol 181 and Recommendation No. R(87) 15 of 17 September 1987. Further elements of data protection derived from the sector-specific measures adopted in the legal instruments on the SIS, EUROPOL, EUROJUST and the Prüm Decision, among others.[422] Data protection regulations for security-related processing were thus not introduced in the anticipated order: rather than first introducing an instrument of general application, setting the principles and elements for any and all security-related processing, to be followed by sector-specific regulations for each different type of processing, quite the opposite took place.

Originating from an agreement between the Council and the Parliament following the concerns voiced by the latter during the adoption of the 2006 DRD, the DPFD was adopted after a long and protracted negotiation. The Council's Multidisciplinary Group on Organised Crime (MDG) led the final drafting process, which resulted in a significant rewriting of the Commission's original proposal and the marginalisation of DPAs. As a result, the legal instrument adopted gives priority to the concerns of judicial, police and security services. Commentators note in particular that the scope of the DPFD is limited to cross-border processing,[423] leaving aside the question of domestic processing, and more importantly, provides for exemptions from every single data protection principle.[424] Owing to these limitations, the DPFD has not played the standard-setting role that the DPD has acquired with regard to the commercial processing of data. In addition, since no supervisory body (mirroring, for instance, the WP29) has been set up in the DPFD,[425] the data protection principles featured in the instrument have not been streamlined into EU policy-making on establishing new data processing schemes and systems.

The position adopted by the European Commission in its proposals for revising the EU DPF with regard to police and judicial cooperation draws from the observation of the shortcomings of the DPFD. Three reasons for these shortcomings are highlighted in its Communication:

- The DPFD only applies to the cross-border exchange of personal data within the EU, thus leaving out domestic processing of personal data.
- It "contains too wide an exception to the purpose limitation principle",[426] and does not provide sufficiently for the possibility of distinguishing between different

[420] See, for instance, the Data Retention Directive, Preamble, 10.

[421] See *The Economist* series on Terrorism and Civil Liberty back in 2007, in particular, Civil liberties: Surveillance and Privacy, 27.09.2007.

[422] The implementation of these rules is supervised by distinct bodies, including the Schengen joint supervisory authority (under Art. 115 of the Schengen Convention), the EUROPOL JSB (under Art. 24 of the EUROPOL Convention), the EUROJUST JSB (under Art. 23 of the EUROJUST Decision).

[423] The limitation of the scope of the DPFD to cross-border exchanges was introduced at the behest of a number of Member States and associate countries, including the Czech Republic, Denmark, Ireland, Malta, Sweden and the United Kingdom, as well as Iceland and Switzerland. See de Hert and Papakonstantinou (2009), for a more detailed analysis of the drafting process of the DPFD and of its contents from a data-protection perspective as well as de Hert and Bellanova's (2009) briefing note on behalf of the LIBE Committee (De Hert, P. and Bellanova, R., *Data Protection in the AFSJ: a system still to be fully developed?*, LIBE Committee, 2009.

[424] Very briefly, these core principles – initially promoted by the first data protection legislations adopted in the 1960s and 1970s by European countries – include the principle of fair and lawful collection and use of data and data quality principles such as the principal of proportional collection and processing of personal data, the principle of data security, and the purpose specification principle.

[425] It was considered in the Commission's initial proposal, but was edited out in subsequent rewritings of the instrument.

[426] European Commission, *Communication on a comprehensive approach on personal data protection in the European Union,* 2010, p. 13.

categories of data ('hard' data based on facts and 'soft' data based on opinion, hearsay or assessment) and data subjects (convicted persons, suspects, victims, witnesses and so forth).

- It "does not replace the various sector-specific legislative instruments for police and judicial cooperation in criminal matters adopted at EU level".[427]

Particularly the latter form the patchwork of regulations for data protection when it comes to data processing in the AFSJ. A list of initiatives regarding data systems developed for security purposes within the EU are provided in chapter 2 of this study. Here it is enough to note that each of the 25 EU data-exchange mechanisms, as well as their underlying regulations at the Member State level, have been for the most part developed independent of the DPFD (or for the same purposes, the DPD). The DPFD expressly abstains from submitting sector-specific regulations for its principles,[428] thus failing to assume the role of a standard-setting instrument.

In light of these identified shortcomings, the European Commission's proposals are threefold:

- the EU legislator should "consider the extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters, including for processing at domestic level while providing, where necessary, for harmonised limitations to certain data protection rights of individuals";[429]
- the possibility of introducing "specific and harmonised provisions in the new general data protection framework, for example on data protection regarding the processing of genetic data for criminal law purposes or distinguishing the various categories of data subjects (witnesses, suspects, etc.)" should be examined;[430] and
- finally, the need to align sector-specific rules with the new, general, data protection framework should be assessed in the long term. The extension of the general framework on data protection to police and judicial cooperation in criminal matters would not preclude, however, the persistence of such sector-specific rules (in application of the *lex specialis* principle).[431]

The key issue regarding the revision of the EU DPF in the field of police and judicial cooperation in criminal matters from the European Commission's perspective thus appears to be the establishment of general standards of data protection that would be common to the areas currently covered separately by the DPP and DPFD and sector-specific rules. Commissioner Viviane Reding has confirmed this recently in an address to the European Privacy Platform of the European Parliament: "the Commission can now consider extending the general data protection rules to the areas of police and judicial cooperation in criminal matters. Limitations to rights in this area would need to comply with the general rules, and be clearly defined and proportionate."[432]

4.2.1.2. The position of EU DPAs

The position of the EDPS and EU DPAs on EU data protection in the field of police and judicial cooperation in criminal matters echoes this perspective. If the revised instrument on data protection is to be comprehensive, the EDPS[433] considers that it should include police and judicial cooperation and do away with the restriction established in Article 3(2) of the DPD. One argument to support this point, besides the problems encountered in the implementation of the DPFD, is that the distinction between the processing of personal data by private and public data controllers in this domain is increasingly irrelevant – for example in the case of the processing of PNR data or financial data as discussed in chapters 2 and 3 of this study. It should also have direct effect on domestic processing, which would give

[427] Ibid., p. 14.

[428] See Art. 28 of the DPFD.

national DPAs the same remit they enjoy with regard other data controllers. The EDPS further recommends these specific measures:

- regarding the quality of data, mechanisms for periodic verification and rectification of data, specific provisions to distinguish between data and files based on facts ('hard data') and on assessments ('soft data') and to distinguish among categories of data subjects (suspects, victims, witnesses, etc.), and specific provisions for the processing of the data of non-suspects;
- regarding particularly sensitive data, such as biometrics and genetic data, specific provisions to ensure that their use is limited to cases where no other option is available; and
- regarding the exchange of data, specific conditions for the transfer of data to non-competent authorities and private third parties as well as for the collection of data from private third parties for law enforcement purposes.

The position of the EDPS echoes that of other DPAs. The European Data Protection Commissioners' Conference has repeatedly stressed the need for a comprehensive EU DPF, which would include police and judicial cooperation in criminal matters and observe fully the principles spelled out in Convention 108 and its additional Protocols and Recommendations.[434]

4.2.1.3. The position of the Council and the European Parliament

The Council adopted its Conclusions on the comprehensive framework for data protection at the ministerial JHA meeting of 24-25 February 2011. The main elements of these conclusions on data protection in the field of police and judicial cooperation in criminal matters are the following:

- The Council acknowledges, in line with the European Commission's position, that "the inclusion of provisions on data protection in the field of police and judicial cooperation in criminal matters in the new framework, should be considered, taking due account of the specific nature of these fields and of the evaluation of the implementation of Framework Decision 2008/977/JHA", without prejudice to the possibility of adopting sector-specific legislation in this area.[435]
- The conclusions further highlight a number of specific points, including the need to reinforce the "special protection of sensitive data" and the devising of "specific provisions" for the processing of biometric and genetic data (including the possibility of establishing special impact assessments on privacy).

[429] Idem.

[430] Idem.

[431] See Papakonstantinou and de Hert (2009), op. cit.

[432] Commissioner V. Reding, "Your data, your rights: Safeguarding your privacy in a connected world Privacy Platform "The Review of the EU Data Protection Framework", Brussels, 16 March 2011, SPEECH/11/183, 16.03.2011, p. 3.

[433] European Data Protection Supervisor, *Opinion on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union"*, 14.01.2011.

[434] See the declarations adopted by the Conference in Edinburgh (April 2009), Prague (29-30 April 2010) and Brussels (5 April 2011).

[435] Council of the European Union, *Conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union*, 24-25.02.2011, p. 3.

- They finally express support for "a more harmonised role of DPAs", including in the area of police and judicial cooperation in criminal matters.[436]

The LIBE Committee of the European Parliament has recently adopted a *Report on a comprehensive approach on personal data protection in the European Union*.[437] In two working documents tabled in March 2011,[438] the rapporteur highlighted two points in relation to police and judicial cooperation in criminal matters:

- The first concerns a general principle, according to which

> a reasonable and modern data protection law has to find a balance between several, equally important factors: the individual freedom (of choice and will), the need to maintain internal and external security, the right to informational self-determination and the right to privacy. …Finding this balance should nevertheless be based on the insight that an effective and rapid exchange of data is indispensable for guaranteeing security nationally and globally. It may allow for the state to enable all other fundamental rights and to fulfil all necessary administrative tasks.[439]

  On this issue, however, the EU Charter establishes in its Article 6 a right to liberty *and* security of person; liberty and security go together, and cannot arguably be balanced against one another. Therefore, the rights deriving from data protection principles cannot be balanced against a 'right to security', although there can be – as argued by the European Parliament's rapporteur – restricted and strictly defined exemptions to these rights.[440]

  Furthermore, framing the rights of personal data protection as an obstacle to security can only be self-defeating for data protection.[441] There are, in this regard, a number of controversies regarding the relation between security and data protection. In the above-mentioned opinion, the EDPS points out that while

> data protection was quite often wrongly characterised as an obstacle to fully protecting the physical security of individuals…[a] strong framework of data protection can sharpen and strengthen security. On the basis of principles of data protection – when applied well – controllers are obliged to ensure that information is accurate and up to date, and that superfluous personal data that are not necessary for law enforcement are eliminated from the systems.[442]

  This is incidentally acknowledged by the Council Conclusions on the comprehensive data protection framework, which stress that "the EU is firmly committed to protecting the fundamental rights and freedoms of its citizens as well as protecting their security; that privacy and security are possible and that there is no need to choose between being free and being safe".[443]

- A second specific point is made about police and judicial cooperation where the rapporteur embraces the position of the Commission and the EDPS, considering

[436] Ibid., p. 6.

[437] European Parliament, *Report on a comprehensive approach on personal data protection in the European Union* (2011/2025(INI), A7-0244/2011, 22.6.2011.

[438] Voss, A., *Working Document 1 on a comprehensive approach on personal data protection in the European Union, European Parliament*, PE 460.637, 15.03.2011; Voss, A., *Working Document 2 on a comprehensive approach on personal data in the European Union*, PE 460.638, 15.03.2011.

[439] Voss, A., *Working Document 1*, p. 3.

[440] On the issues raised by the 'balance' metaphor, see the final reports of the ELISE (FP5) and CHALLENGE (FP6) projects.

[441] See the results of the ELISE (FP5) and CHALLENGE (FP6) projects, as well as the work conducted in the INEX (FP7) project.

[442] European Data Protection Supervisor, Opinion of 14 January 2011, p. 7.

[443] Council of the European Union, *Conclusions on a comprehensive approach on personal data protection in the European Union*, p. 2.

> that "there must be an extension of the application of the general data protection rules to the areas of police and judicial cooperation, including for processing at the domestic level while allowing for restricted and harmonised limitations to certain data protection rights of individuals".[444] The specific point on police and judicial cooperation is reiterated in the final report, which "considers it imperative to extend the application of the general data protection rules to the areas of police and judicial cooperation, including processing at domestic level, taking particular account of the questionable trend towards systematic re-use of private-sector personal data for law enforcement purposes". Limitations to data protection rights should be "strictly necessary and proportionate" as well as "narrowly tailored and harmonised". Reflecting this logic, the notion of a 'balance' between security and data protection has been removed from the final version of the report.

This position would address some of the issues engendered so far by the exclusion of former third-pillar and security matters from the scope of general EU data protection law. Extending the revised data protection framework to include police and judicial cooperation in criminal matters would ensure that it lives up to the criteria of 'comprehensiveness' and would set up legally binding standards in an area where, as shown in the rest of this chapter, policy-making and processing practices have sorely lacked overall guidance.

4.2.2. The added value of EU accession to the ECHR

The distinction between the right to privacy and the right to protection of personal data is primarily made in the EU Charter on Fundamental Rights.[445] The conceptual elements to be taken into consideration when speaking about 'privacy' and 'data protection' have been clarified in chapter 1 of this report. Suffice here to repeat that privacy is traditionally defined as the ability of an individual to be left alone, out of public view, free from surveillance or interference from others (individuals, organisations or the state) and in control of information about oneself.[446] One can distinguish the ability to prevent intrusion in one's physical space ('physical privacy', for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ('informational privacy'). The concept of privacy therefore overlaps but does not coincide with the concept of data protection. The right to protection of personal data protects all personal data, even when there is no strong link with privacy. The right to privacy (at least in the view of the European Court on Human Rights) only protects personal data in cases where a link with 'private life' may be identified (even if 'private life' is to be construed, according the Strasbourg Court, in a wide sense).

On the other hand, no explicit mention of the right to data protection is made in the text of the ECHR. Instead, its Article 8 merely states that

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[444] Voss, A., *Working Document 2*, p.2

[445] See de Hert, P. and Gutwirth, S., "Data Protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action", in S. Gutwirth et al., *Reinventing data protection?* Dordecht: Springer Science, 2009, pp. 3-44.

[446] Definition by the European Data Protection Supervisor (EDPS) retrieved from the EDPS official website: (http://www.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Dataprotection/Glossary/pid/84#privacy). The idea of privacy originates from the famous article by Samuel Warren and Louis Brandeis titled "*The Right to Privacy*" (*Harvard Law Review*, Vol. 4 No. 5, 1890).

Although the ECHR does not include any mention of a right to data protection, the ECtHR has developed it from the right to privacy, as outlined in its Article 8. In effect, the ECtHR has developed criteria to assess whether an issue of data protection touches upon the right to privacy, while also applying the criterion of the necessity of processing.[447] So far, there is little evidence that this approach creates drawbacks for data protection purposes. On the contrary, as demonstrated in the analysis that follows, recent case law suggests strong sensitivity on the part of the ECtHR to data protection concerns.

Where the Strasbourg Court has acknowledged that data protection is also a privacy issue, it has granted some of the guarantees foreseen in data protection legislation. For instance, this has been the case with regard to a right of access to personal files,[448] the purpose limitation principle[449] and the necessity of having independent supervisory authorities in the context of the processing of personal data.[450]

An important implication of the ratification of the Lisbon Treaty for European data protection is that it enables the EU to accede to the ECHR. This accession is expected to take place in the near future.

The practical results of such accession remain to be seen. Yet of particular importance for the purposes of this chapter is that once accession is completed, the ECtHR shall not be restricted in judging AFSJ cases by the Lisbon Treaty. By contrast, the CJEU faces substantial restrictions in the Treaties environment when deciding upon AFSJ data processing. Article 276 TFEU states that

> [i]n exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

Such limitations shall not apply to the ECtHR, which is therefore expected, once accession is completed, to go further and deeper than the CJEU while assessing AFSJ processing operations.

On the other hand, apart from future case law, ECtHR decisions that have already been issued have benefited data protection purposes owing to the Court's strong insistence on the application of the necessity and legality criteria. The *Marper* case can be mentioned here as an illustration of the former, and *Liberty* as an illustration of the latter. We return to both cases below.

---

[447] See also De Hert, P. & Gutwirth S. "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", Gutwirth S. et al. (eds), Reinventing Data Protection?, Springer Science, 2009; De Schutter, Olivier, "*Vie Privée Et Protection De L'individu Vis-À-Vis Des Traitements De Données À Caractère Personnel*", R.T.D.H., 2001, pp. 148 et seq.

[448] European Court of Human Rights, *Gaskin v. UK*, 10454/83, 7 July 1989, Application No. 10454/83; European Court of Human Rights, *Antony & Margaret McMichael v. UK*, 24 February 1995, Application no. 16424/90; European Court of Human Rights, *Guerra et al. v. Italy*, 19 February 1998, application no. 14967/89; European Court of Human Rights, *McGinley & Egan v. UK*, 09 June 1998, application no. 21825/93 and 23414/94.

[449] European Court of Human Rights, *Peck v. UK*, 28 January 2003, application no. 44647/98, § 62; European Court of Human Rights, *Perry v. UK*, 17 July 2003, application no. 63737/00, § 40; European Court of Human Rights, *P.G. & J.H. v. UK*, 25 September 2001, application no. 44787/98, § 59. In more detail, see Brouwer, E., op. cit., pp. 138–139.

[450] European Court of Human Rights, *Klass v. Germany*, 06 September 1978, application no. 5029/71, § 55; European Court of Human Rights, *Leander v. Sweden*, 26 March 1987, application no. 9248/81, §§ 65–67; European Court of Human Rights, *Rotaru v. Romania*, 04, May 2000, application no. 28341/95, §§ 59–60. See in detail Brouwer, E., op. cit., pp. 143–144; ECtHR, Gaskin v. UK, 10454/83; European Court of Human Rights, *Z. v. Finland*, 25 February 1997, application no. 22009/93.

With regard to AFSJ data processing in particular, the accession of the EU to the ECHR would mean that the case law of the Court of Strasbourg in this field would apply, while defining what is "necessary in a democratic society".[451] In the *Marper* case,[452] the ECtHR found that "an interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'".[453] Subsequently, the Court went on to further define these criteria, which any type of security-related processing will have to meet in order for it to be found legitimate in a democratic society. This important list will be applicable to all the data collection systems examined in chapter 2 and listed in Annex 1 of this report, regardless of whether their operation is governed by specialised provisions for data protection. Yet given their number (more than 25 initiatives recorded so far) and their method of implementation, it is unlikely that they would all meet the above necessity criterion.

4.2.3. Law-making options: A singular, comprehensive framework or the DPD and DPFD?

From a conceptual point of view, given the contemporary structure of EU data protection and the opportunity presented by the ratification of the Lisbon Treaty and the Commission Communication on the amendment of the legal framework for data protection, there are two conceivable ways forward from a law-making point of view: 1) either a new, single, comprehensive, standard-setting text will be introduced that will set the general rules for all personal data processing within the EU; 2) or commercial and security-related processing shall remain separate within the EU, through the continued existence of the DPD and the DPFD respectively. Apparently, both of the latter instruments will have to be properly amended in order to adhere to the (by now fundamental) rights to data protection and privacy. Nevertheless, it is submitted that either option matters little in practice as far as effective personal data protection is concerned: in effect, what matters is that power configurations are dealt with and controlled, regardless of the legal means through this is achieved.

A new, single regulatory instrument replacing both the DPD and the DPFD and forming a unitary basis of data protection within the EU would perhaps appear to be a rational option at this point. The DPD has run its course, successfully, for the past 15 years but by now it perhaps appears outdated within a processing environment based on such notions as cloud computing, social networking websites and location-based services. On the other hand, the DPFD failed to assume the role of a standard-setting text for data processing in the AFSJ and perhaps has no *raison d'être* in the post-Lisbon Treaty environment. The replacement of both instruments by a single, unifying document would constitute a reasonable option, which would take into account both public expectations and the fact that security and non-security personal data processing have become increasingly difficult to distinguish and separate within the AFSJ. Such an instrument could help bring much-needed clarity to the

[451] Application of this criterion while limiting "certain data protection rights of the individual" is also accepted in the EP *Report on a Comprehensive Approach on Personal Data Protection in the European Union*, Committee on Civil Liberties, Justice and Home Affairs, A7-0244/22.06.2011, 6.

[452] *European Court of Human Rights, S & Marper v. UK, 4 December 2008, application n. 30562/04 and 30566/04*.

[453] Para. 101; see also Guild E, *Global Data Transfers: the Human Rights Implications*, CEPS INEX Policy Brief No. 9/May 2009; Guild E, *The European Union after the Treaty of Lisbon, Fundamental Rights and EU Citizenship*, Global Jean Monnet/European Community Studies Association, World Conference 25-26 May 2010, CEPS Liberty and Security in Europe; González Fuster, G., De Hert, P., Ellyne, E. & Gutwirth, S., *Huber, Marper and Others: Throwing new light on the shadows of suspicion*, INEX Policy Brief, N. 11, June 2010.

field, assist individuals in the protection of their rights, create legal certainty and warrant a degree of harmonisation at the Member State level.[454]

Still, although the introduction of a new, single, regulatory instrument to replace both the DPD and the DPFD would probably be a reasonable option, it could prove unrealistic in practice. A series of legal issues affecting its release can be foreseen.[455] Article 16 TFEU acknowledges a right to data protection, but as highlighted in chapter 1, this is subject to a few exceptions. For instance, Declaration 21 states that "specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the TFEU may prove necessary because of the specific nature of these fields". In addition, certain Member States have inserted reservations in the text of the Treaty, reserving for themselves the right to act differently in the sectors concerned. Finally, pursuant to Article 10 of Protocol 36 TFEU on transitional provisions, all acts adopted before the entry into force of the Lisbon Treaty shall be preserved until the acts are repealed, annulled or amended. This means in practice that the review of the EU DPF process will have to include in its agenda the simultaneous repeal and replacement of both the DPD and the DPFD. The different procedures involved in such a task greatly complicate the construction of a new, single regulatory instrument for data protection in the EU.

On the other hand, the DPD and the DPFD could continue regulating data processing within their respective fields, of course properly amended to reflect changes in the post-Lisbon environment. This option would most likely include an updating of the DPD to address contemporary processing challenges and an extension of the DPFD scope to cover all security-related processing. The DPFD relationship with other data systems operating in the AFSJ would also have to be clarified, equally towards the introduction of common standards and rules for each different data processing mechanism.

The merits and shortcomings of this option are quite obvious. It is a realistic approach, given institutional, time and budgetary constraints. Because it is merely a projection of a model already in effect, it constitutes a self-evident option that will probably be operational within a short period of time through relatively little effort and resources. On the other hand, the maintenance of what is essentially a reflection of the pillar-system data protection framework would do very little to address the regulatory patchwork issue. This is particularly the case in relation to security-related processing, and it would leave individuals alone in their struggle to protect their personal data, while also not considering the routine blending of security and commercial personal data processing in the AFSJ.

Nevertheless, as demonstrated in the preceding chapters of this study, an excessive elaboration of the regulatory options available at this point risks developing into an end in itself, and thus diverting attention away from the data protection issues at hand. AFSJ data processing circumstances are ever changing, in order to address a security problem within the EU, regardless of whether it is real or perceived. Data processors, in the form of power configurations that process personal data for security-related purposes, have transformed in the past few years into two formations:

- *The networking society*. Personal data processing for security-related purposes has become a network phenomenon. Data processors come in various forms, including EU organisations, national governments, law enforcement agencies and private parties. Access is requested, and customarily granted, to a multitude of datasets, assembled under various circumstances and otherwise put to unrelated uses. As shown in chapter 2, 'networked' data processing follows largely from the disagreements between these different data processors as to how the data should

[454] The form of such an instrument remains to be decided – the EDPS from its part suggested the release of a Regulation particularly in order to achieve harmonisation among Member States (see EDPS, Opinion of 14 January 2011, p. 15).

[455] See particularly Hijmans H., Scirocco A., *Shortcomings in EU data protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?* Common Market Law Review, 46, 2009, p. 1516.

be processed and used. Processing takes place essentially behind closed doors, leaving no space for transparency or accountability.

- *The profiling society*. As discussed in chapter 2, profiling has gained exponentially in importance and wide use within the AFSJ context, but its legal treatment largely lags behind. All data systems currently in effect in the AFSJ allow for, by not explicitly prohibiting, collected personal data to be put to similar uses. Some profiling is indeed to be expected and may even prove useful with regard to the drafting of security policies in the AFSJ. Even so, specific rules need to be introduced on the type of profiling that is to be permitted (and the relevant conditions) and the type of profiling that should be prohibited at all times (particularly when using sensitive information).

Each notion is further elaborated in the following sections, alongside the appropriate new principles required to adequately address the challenges identified in chapter 2 of this study. From this viewpoint, the actual form of the EU DPF is ultimately irrelevant. Rather than expounding at length upon the regulatory means through which to achieve the data protection ends, it would be preferable for these efforts to focus on defining the latter, at least within the AFSJ data processing environment, in order for the updated DPF to take them into consideration regardless of its ultimate format. Nevertheless, the analysis that follows demonstrates that perhaps a more effective law-making option would be for the EU DPF amendment process to introduce multiple regulatory texts for formerly third-pillar processing, than a single comprehensive and all-encompassing instrument. Distinctions would unavoidably have to be made in such a single instrument, owing to both the special needs of security-related processing and the different development stages of commercial as opposed to security processing (for instance, no controlling mechanisms exist in the latter while in the former the discussion is to impose some of the more bureaucratic ones already in place). Such differentiations would probably make a single data protection instrument for all processing in the EU complicated and difficult to follow.

4.3. Data protection concerns within the AFSJ data processing context

As argued above, security-related processing presents unique characteristics and responds to special needs that differentiate it from any other type of personal data processing. The question of whether these circumstances impose a separate regulatory framework (in the form of an amended DPFD or other) or whether they may be accommodated by way of sector-specific exemptions in the text of a single regulatory instrument (in the form of an amended DPD or a regulation or other) is ultimately not of much concern for data protection purposes.

Instead, what is of importance is that the main concerns of data processing in the AFSJ are explicitly addressed and appropriately dealt with in whatever legal form the amended EU DPF ultimately assumes. The dilemmas stemming from the increased processing of personal data for law enforcement purposes in EU AFSJ policies have been discussed in detail in chapter 2 of this study. In this section we focus on the common elements of the legal basis and the principles that should be developed to satisfactorily respond to these concerns, in particular the following:

- the regulation of profiling for security purposes;
- the requirement for transparency and openness with regard to the processing done by law enforcement agencies;
- the principle of accountability and its interrelation with individual consent in the AFSJ context; and
- individual access to justice in the AFSJ context.

These legal dilemmas are raised practically on a daily basis, in the AFSJ context and commercial processing alike, because data protection is intrinsically connected to information technology as an unchallenged policy option for programmatic policy-making. Until the latter finds its proper place in modern societies, data protection shall inevitably have a restricting role.

4.3.1. The profiling society: Using profiles to facilitate security in the AFSJ

The specific challenges that profiling presents for individuals in the law enforcement context and their relationship with dataveillance and proactivity have been analysed in section 2.3 above. The fact that the relevant regulatory response so far has been surprisingly limited has equally been highlighted in the same analysis. In effect, the EU documents that attempt to come to terms with profiling from a data protection viewpoint only consist of a recommendation by the European Parliament,[456] which suggests two definitions for profiling and asks for the establishment of a set of criteria for assessing the lawfulness of current and foreseen profiling activities. On the other hand, the Council of Europe has issued a recommendation[457] on profiling, attempting to make the general provisions of Convention 108 concrete in the relevant processing context.

Notwithstanding the lack of a firm definition, neither of the documents specifically deals with profiling performed by law enforcement agencies, although they refer to it incidentally. Nevertheless, profiling operations in the AFSJ are qualitatively and quantitatively different from any other type of profiling,[458] and as such ought to be treated in an explicit way.

The DPFD and the DPD do not deal with profiling expressly but rather incidentally refer to it, by way of automated decisions on individuals. In this context, in its Article 7 the DPFD states that

> [a] decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.[459]

The DPD wording is quite similar (Article 15):

> 1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
>
> 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

[456] European Parliament, *Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control* (2008/2020(INI)).

[457] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010.

[458] In this context, it should also be noted that, as of January 2010, the new EUROPOL-EUROJUST agreement regulates EUROJUST participation in EUROPOL's analysis work files (see also Boehm, F., Information Sharing in the Area of Freedom, Security and Justice – Towards a common standard for data exchange between agencies and EU information systems (forthcoming).

[459] In the DPFD context it should also be noted that profiling operations shall most likely qualify for the 'prior checking' criteria as well (see Preamble, 32).

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

These provisions treat automated decision-making on the basis of personal data processing in a more or less similar way. With regard to profiling, they both seem to require a special law that will set the conditions under which it is to be allowed.[460] From this standpoint, it appears irrelevant whether a single or multiple regulatory documents were produced after the EU DPF review process was completed, given that specialised legislation distinguishing between profiling conducted for commercial and that conducted for security purposes needs to be introduced at a later stage. Consequently, the current framework is merely a start for the regulation of profiling, laying down only broad and minimum requirements for data protection.

On the other hand, profiling is being introduced in EU regulations at an accelerating pace and is increasingly conceived as a key component of the EU's AFSJ policies.[461] As demonstrated in section 2.3, notwithstanding differentiations in terminology, profiling may be found at the basis of several processing activities for EU law enforcement (for instance, in the VIS or PNR), because it is intrinsically connected to the trend towards a generalisation of data processing in view of the development of "a stronger focus on the prevention of criminal acts and terrorist attacks before they take place". Nevertheless, in all the above cases, although special attention is given to the organisation of the profiling processing *per se*, no mention whatsoever is made of the data protection safeguards that need to be implemented at the same time for the protection of individuals. This may be illustrated, for instance, by the latest EU *Proposal for a Directive on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*.[462] In this proposal, although procedures for the "assessment of passengers" form the basis of the relevant processing, its single article on data protection (Article 11) says nothing about the conditions under which such processing is to take place.

Consequently, today profiling operations in the AFSJ context are gaining in importance, yet without this development being followed by effective and adequate data protection regulation. It is only lately that new ideas for the regulation of profiling from the data protection perspective are emerging – for instance, the Council of Europe Recommendation asks for the use of PET[463] system architecture or specific guidance with regard to the individual's right to information in the profiling context.[464]

What is of importance, therefore, is the formulation of principles that should govern profiling in the AFSJ. Very little concrete guidance has been given so far about the principles governing profiling operations run by law enforcement agencies. No one really knows the collections of data from which they draw their conclusions, the logic of the

[460] See also European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, pp. 17, 18.

[461] Profiling, or the drafting of "risk assessments" and "risk analyses" has also been listed under "some of the activities performed by FRONTEX, EUROPOL and EASO as foreseen in their legal remits or as developed through informal (de facto) practices are at odds or present a more sensitive relationship with specific fundamental rights provisions foreseen in the EU Charter" – see European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies FRONTEX, EUROPOL and the European Asylum Support Office*, 2011, p. 108.

[462] European Commission, *Communication on a comprehensive approach on personal data protection in the European Union*, 4.11.2011.

[463] In its Article 2.2, see also 4.4.3.

[464] In its Article 4.

processing or the actions undertaken by security agencies on the basis of their findings. To date, transparency and openness about the instances of processing have been lacking, and thus the analysis that follows also covers this type of processing. But the requirements for transparency and openness for profiling operations may be derived directly from Article 8 of the ECHR:[465] applying ECtHR reasoning, data processors running profiling operations need to indicate with sufficient clarity the scope and manner of such operations, as well as set out in a form accessible to the public any indication of the procedure to be followed for the correlation of personal information.[466]

In addition to transparency and openness, the amended EU DPF needs to firmly establish what type of profiling is definitely prohibited under any and all circumstances. Profiling in the law enforcement sector is qualitatively different from profiling run by corporations for example. The latter may at worst lead to exclusion from information and social isolation and stagnation. The former can lead to a direct infringement of a series of fundamental human rights, ultimately affecting human dignity. Identifying in advance what type of profiling is allowed may prove an impossible task – and one that law enforcement agencies would reject in principle. The amended EU DPF therefore ought to focus on the types of profiling to be expressly prohibited and foresee detailed safeguards for those profiling operations that are considered legitimate, also in line with ECtHR's case law:[467]

- The first type of profiling to be expressly prohibited in the amended EU DPF is that which uses of sensitive personal data as part of its basis. Profiling using ethnicity, religion, political or philosophical beliefs and other sensitive information as defined in the DPD, may lead to unfair results affecting nothing less than human dignity and probably lead to categorisations that offer little for law enforcement purposes. A positive exemption, therefore, needs to be introduced to the text(s) of the amended EU DPF regulating AFSJ data processing. To date, both the DPD and the DPFD leave space, by way of derogations,[468] in their respective texts for such profiling. This is a loophole that needs to be explicitly addressed during the EU DPF amendment process.
- The second prohibition for profiling in the AFSJ should be on the use of unlawfully acquired data. This is perhaps a self-evident exclusion. Even so, owing to the envisaged extensive use of profiling by law enforcement agencies and the general trend to include as many datasets as possible in the relevant processing in order to formulate a possibly complete picture, clear guidance as to what datasets may be correlated at each time needs to be provided in the amended DPF.
- Lastly, the profiling logic needs expressly to adhere to the general data protection principles, particularly that of fair and lawful processing. In this vein, the outcome of profiling operations may not lead to unlawfully categorising individuals. And the processing criteria may not be discriminatory or unlawful. This may also appear a self-evident suggestion – after all, profiling is a personal data processing operation that largely falls within data protection limits and Articles 6 and 3 of the DPD and the DPFD respectively, each requesting *lawful* processing. Still, given that both texts

[465] See Gonzalez Fuster G., Gutwirth S., Ellyne E., *Profiling in the European Union: A high-risk practice*, CEPS INEX Policy Brief No. 10, June 2009, p. 5.

[466] See European Court of Human Rights*, Liberty and others v. the United Kingdom*, 1 July 2008*,* Application no. 58243/00.

[467] Particularly, *Marper* (see above, under 4.2.4), *Liberty*, and also with regard to non-discrimination the CJEU case of *Huber*, discussed in R. Van Brakel and P. De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', *Journal of Police Studies*, 2011, vol. 20(3), nr. 20, 163-192; González Fuster, G., De Hert, P., Ellyne, E. & Gutwirth, S., op. cit., p. 8.

[468] In the text of the DPD by way of Article 8.5, even if the general exemption of Article 3 (on its scope) was overlooked. In the text of the DPFD, in the, largely inadequate for the protection of sensitive data in general, Article 6.

allow room for exemptions, a relevant inclusion in the amended EU DPF appears necessary.

4.3.2. The networking society: Transparency and openness in security systems

The principles of transparency[469] and openness are essential parts of the EU DPF,[470] particularly in the DPD context; in practice, all the elements are intended to operate in a transparent and open way, thus enabling continual scrutiny by all the parties concerned.

The principles of transparency and openness are particularly important in the data protection field. Processing operations do not take place in public; neither are their results felt immediately by the individuals concerned, in order for them to respond accordingly. On the contrary, the processing of personal data takes place behind closed doors or rather within automated systems, without the millions of individuals whose data are being processed being present or even aware that such processing takes place. In addition, the results of such processing in the majority of cases do not lead to direct action, positive or negative, for the individuals concerned, but are stored in computer systems for future use. These circumstances, especially when it comes to security-related processing, may at the least lead to frustration or even unlawful infringement of individual rights. In the real world, individuals may come across a decision that affects them (for instance, being unable to enter a country applying border controls) and be unaware of the findings from processing operations that have been used to formulate such a decision. Thus, the task of safeguarding their rights is made impossible: individuals do not know that their data have been processed unless they are faced with a (negative) decision against them. Only then do they have reason to start enquiring about what happened. Security agencies may always refer to national interest while refusing to reply to similar requests. For this impossible task individuals need all the help they can get.

The EU DPF already takes account of the needs for transparency and openness as far as the data processing particulars are concerned.[471] To this end, the notification system or the dedicated individual rights to information, access and objection or even its enforcement mechanism, through independent agencies, could be noted. All these checks aim at strengthening the inherently weak position of individuals while protecting their right to data protection.

Law enforcement processing, however, has been granted a wide margin for exceptions, as evidenced in the text of the DPFD. Because a notification system or the right to information and access or even the oversight by an independent (non-police) authority could potentially hinder police work, substantial derogations have been granted in favour of such processing. This approach shall probably need to be re-evaluated during the processing of the amended EU DPF.

The lack of transparency and openness in AFSJ processing is particularly felt in the architecture of data processing examined in section 2.3 above and in the *networking society* context. By now, personal data processing for security-related purposes has become a network phenomenon. Data processors come in various forms and legal statuses, including EU organisations, national law enforcement agencies and private parties. So far, the EU DPF has in effect enabled a web or patchwork of personal information exchanges

[469] On the general principle of transparency see section 1.3.2 above.

[470] The principle of transparency discussed here is broader than the “increasing transparency for data subjects” analysis included in the Commission Communication (2.1.2), in that the principle elaborated here is intended to operate at multiple levels, being addressed to all data protection participants, rather than placing specific obligations upon data controllers (ultimately, merely expanding the individual right to information). On the other hand, the EDPS finds it perhaps more important to reinforce the existing Directive provisions dealing with transparency (see EDPS, Opinion of 14 January 2011, op. cit., p. 74).

[471] See European Data Protection Supervisor, Opinion of 14 January 2011, p. 72.

among them, whereby access is requested and customarily granted to a proliferation of data systems (section 2.2 above), ranging from passenger to telecommunications records. In its basis lies the DPFD, governing personal data processing "transmitted or made available between Member States", in a way that leaves room for broad exemptions.

The amended EU DPF hence needs to explicitly make reference, in the text of the relevant instruments, to the principles of transparency and openness. These should operate at multiple levels. They need to apply to data controllers (and data processors) and to the processing operations themselves. They also need to apply to the enforcement mechanisms for data protection from the perspective of both the data subject and the data controller. Such enforcement mechanisms need to remain open and transparent to citizens and to any third party with an interest in enquiring about their operation and effectiveness.

Equally, because processing in the AFSJ has lacked a central coordination body, such an agency should be established under the amended EU DPF in order to warrant the implementation of these principles among Member States.

As argued above, while profiling is not evidence but rather 'probabilistic knowledge', it is still used in criminal investigation procedures. The principles of transparency and openness should thus ultimately lead to a reversal of the burden of proof in favour of individuals in those cases when presenting evidence in court in defence of their rights is made impossible due to the processing executed by data controllers. Even in ex-first pillar, commercial processing, individuals may be handicapped while accessing evidence of their data being (unlawfully) processed, because of either legal exemptions in favour of data controllers or system architecture restrictions. These difficulties are expected to increase exponentially when it comes to AFSJ personal data processing. A reversal of the burden of proof would mean that it would be data controllers that will need to convince the court that their processing was lawful, instead of individuals having to present solid (often inaccessible) evidence substantiating their claims. Such a reversal would after all be in line with fundamental case law by the ECtHR (also in view of the imminent accession of the EU to the ECHR). In effect, the Court has recognised the inability of an individual to prove his or her case in front of national courts, but concluded that "to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the [data controller's] record keeping at the material time".[472]

Finally, the principles of transparency and openness invite discussions about a right of individuals to be notified after the AFSJ-related processing of their personal data is completed (evidently, without any need for further investigation).[473] Such a right has been elaborated by the ECtHR in the context of Article 8 of the ECHR.[474] It would include law enforcement agencies notifying all those individuals whose data have been processed for security-related purposes without their knowledge, even though no further actions were required after conclusion of the relevant processing, bearing in mind that the results of such processing have not been deleted from the relevant systems. In such an event, an individual has the right to know that unknowingly s/he has been subjected to such treatment, regardless of the absence of any immediate results from it.

4.3.3. The principle of accountability and the role of consent

The various conceptual elements pertaining to the principle of accountability have been outlined in chapter 1 of this study. In the data protection context, the introduction of a principle of accountability for data controllers is being identified as a law-making option that will enhance the effectiveness of the amended EU DPF and provide real protection to

[472] European Court of Human Rights, *K.U. v. Finland*, 2 December 2008, application no. 2872/02.

[473] See also De Hert P, Boehm, F., *The rights of notification after surveillance is over: Ready for recognition?*, Human Rights in the Digital Era Conference, University of Leeds, 16 September 2011.

[474] See, for instance, European Court of Human Rights, *Shimovolos v. Russia,* 21 June 2011, application no. 30194/09.

individuals. This is by no means a new idea in the field, however. Discussions on the principle of accountability date back to 2009, when the WP29 first listed it among its recommendations to achieve more effective implementation.[475] This idea was subsequently further elaborated and formulated into material suggestions in 2010.[476] Hence it appears that so far the principle of accountability has been discussed as a useful addition with respect to DPD amendment process. This section argues that it is additionally necessary to outline this principle in AFSJ processing.

In broad terms, the principle of accountability places upon data controllers the burden of implementing within their organisations specific measures to ensure that data protection requirements are met while executing their processing of personal data. Such measures could include anything from the introduction of a data protection officer to implementing DPIAs or employing privacy-by-design system architecture. Consequently, if viewed within the DPD review context (personal data processing for commercial reasons), the principle of accountability would perhaps add little to the present EU DPF, particularly if perceived as an alternative to some requirements for compliance with rules, because data controllers are in any case responsible for observing the data protection rules.[477]

Nevertheless, this is not the case when it comes to AFSJ personal data processing. As demonstrated in the previous chapters,[478] particularly chapter 2, all the 25 personal data processing systems in the AFSJ and the related regulatory instruments have been primarily assembled to help law enforcement agencies. None of these initiatives was introduced placing the individual or the judge at its epicentre. Their provisions, although specifying the particulars of each data processing system, are abstract when it comes to the details for implementing the right to data protection – which evidence to use, in which court to file a lawsuit or against which law enforcement agency to file a lawsuit. The principle of accountability would involve clear responses to the above questions. From the individual's point of view, the principle of accountability in the AFSJ context means enabling effective protection of the right to data protection in front of (or against) the competent authorities.

The principle of accountability in AFSJ personal data processing also requires the introduction of adequate controlling mechanisms. Security-related processing lacks transparency and openness, and at times effective controlling mechanisms. The DPFD, with its limited scope, falls short in establishing independent authorities either at the Member State or EU level with the required competences to effectively monitor and control personal data processing. A central coordinating group, such as the WP29, is equally missing from security-related processing. If the principle of accountability were translated into concrete measures to be implemented by security agencies, it would facilitate the monitoring tasks of the reorganised controlling authorities and thus its introduction in the amended DPF could be of some use. Indeed, for the principle of accountability to find its way into the new regulatory environment,[479] it needs to address such difficult questions as how to reconcile the need for specificity with a principle of a general nature and how to resolve the issue of scalability or proportionality. In other words, it needs to specify which criteria shall determine the adequacy of measures implemented by data controllers.[480] In this context, it

[475] Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168, 01.12.2009.

[476] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, 13.07.2010.

[477] See for instance Art. 6.2 of the DPD.

[478] See also European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), op. cit., p. 101.

[479] A development also favoured by the Council (see Szabo Endre Gyozo, *New principles – in the light of the discussions within the Council Council conclusions on the Commission's Communication*, presentation held during the *International Data Protection Conference*, Budapest, 16-17 June 2011).

[480] See Hijmans, H., *Principles of Data Protection: Renovation Needed?,* presentation held during the *International Data Protection Conference*, Budapest, 16-17 June 2011.

has been suggested that its added value lies in its possibility to function as a general obligation to demonstrate results, while giving freedom to data controllers as to the means they employ.[481]

Because a principle of accountability in the data protection context would involve different measures for different data controllers, a single data protection instrument to be produced during the DPF amendment process would need to make several distinctions. If viewed from the perspective of personal data processing for commercial purposes, a principle of accountability could mean a reduction in the data controllers' bureaucratic burden. In this vein, the Commission Communication suggests that "[t]his [principle of accountability] would not aim to increase the administrative burden on data controllers, since such measures would rather focus on establishing safeguards and mechanisms which make data protection compliance more effective while at the same time reducing and simplifying certain administrative formalities, such as notifications".[482] On the other hand, in the AFSJ environment, where there are no controlling mechanisms for similar procedures, a principle of accountability would operate in exactly the opposite way, actually increasing the relevant legal requirements placed upon data controllers. From this point of view, although of no importance for data protection purposes, a more effective law-making option would perhaps be multiple regulating texts coming out of the EU DPF amendment process.

The requirement for the introduction of accountability checks in AFSJ processing is particularly important given the actual, if perhaps unrecognised, role of individual consent in security-related personal data processing.

Individual consent, despite having a central role in the EU DPD relating to ex-first pillar, commercial processing,[483] is practically missing in AFSJ data processing. In the text of the DPFD, consent is generally perceived to relate to Member States (consenting to various uses of personal data transmitted to other Member States) and not to individuals. The same is true for other, security-related, personal data processing instruments: individual consent is nowhere requested or taken into consideration. It is because of this important omission that individual consent is examined here and not in the analysis in the next section of this chapter, where certain adjustments to the current EU DPF are discussed. Individual consent is an important omission of the regulatory framework for AFSJ-related data processing that needs to be viewed more as a data protection issue, whose implications concern the entire field of security-related personal data processing, rather than as a simple insertion into the resulting document(s) from the EU DPF review process.

It could be claimed that the omission of individual consent from AFSJ data processing is inevitable, given the special characteristics of security-related processing. From the individual's perspective, consent must be generally perceived as prejudiced by the need to perform an act or a task: for instance, to enter a country, board an airplane or have a passport issued. In all these cases a requirement for the consent of individuals concerned to process their data would probably be hypocritical, because individuals have no alternative but to comply. Individual consent may be applicable in ex-first pillar, commercial processing, whereby individuals may simply opt not to acquire a product or a service. When it comes to basic activities of human life, however, consent is burdened by necessity.

Although any reference to individual consent is missing in the regulatory texts of the present EU DPF in the AFSJ, seemingly to safeguard the interests of both data subjects and data controllers, such omission is superficial and misleading. In effect, individual consent is

[481] Ibid.

[482] In 2.2.4.

[483] In fact, it constitutes one of the legal bases in order for processing of personal data to be allowed. The requirement for consent should allow an individual to make sure that his or her data is processed only in the manner that was specified during its collection when consent was obtained. In order to warrant the individual right to data protection, the DPD requires that consent be "freely given, specific and informed".

missing only at the moment when law enforcement agencies process personal data found in their systems. Yet the origins of such datasets are not always security-related. Security agencies have access to and may process information applying the DPFD or other security-related data protection instruments[484] that has been gathered by private parties during routine, commercial processing. This occurs for instance with telecommunications data, which may be processed through the DRD. In other words, if one follows the path to the origins of data processed in the AFSJ context in the EU, it is likely that such origins will not always lie in the same AFSJ environment.[485] And if this is the case, then security agencies may well process data because data subjects unknowingly consented to their data being collected by other actors in the first place.

That is why individual consent matters in AFSJ data processing too. Its complete omission so far has been harmful to the individual right to data protection. The amended DPF would benefit from a single regulatory text, where the distinctions and extensive work on individual consent found in the DPD would also apply automatically to AFSJ data processing. Moreover, this text should be founded on the premise that dispensing with consent is not possible unless it can be justified on the grounds set out in Article 8.2 ECHR and that the justification will be in respect of the specific collection and use of data. Any subsequent use of data for any other purpose must once again be checked to satisfy the justification test. The test against whether the data use is 'necessary in a democratic society' should not just take place once the data is collected, but every time the data is accessed, shared, transmitted, etc.

In addition, not all aspects of policing need to be kept secret. It is a generalising and probably wrong regulatory approach to treat any and all security-related processing as a special type of personal data processing, therefore granting blanket exemptions to such important data protection principles as the requirement for individual consent (or for the same purposes the right to be informed). Certain categories of law enforcement processing would not be put at peril if these principles were also recognised in the AFSJ processing context; such categories could include, for instance, the routine and widespread processing of data on persons who hold weapons permits or the field of administrative policing.

In any event, even within the ex-first pillar, commercial processing environment the difficulties of warranting a free, specific and informed individual consent have been extensively identified in the Commission's Communication.[486] In the AFSJ context, the explicit inclusion of individual consent among the requirements of lawful data processing would probably be contested by law enforcement agencies. The inclusion of accountability checks for data controllers is thus the only way to ensure that security agencies remain accountable for processing performed by their respective organisations.

4.3.4. Access to justice: A 'closest to home' individual right of redress?

The noted lack of transparency, openness and accountability so far in AFSJ personal data processing directly affects the individual right of access to justice. Because law enforcement agencies are able to process data behind closed doors and exchange datasets among themselves practically seamlessly and with very few controlling or even monitoring mechanisms, individuals are hindered in effectively protecting their rights whenever infringed, in and out of courts. Indeed, even being aware that their rights to data protection have been infringed is practically impossible for individuals, given the limited rights

[484] See also Boehm, F., op. cit., "personal data exchange is not only limited to AFSJ agencies, it is also taking place between European information systems and the AFSJ agencies".

[485] See also European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, p. 6.

[486] Under 2.1.5, whereby it is stated that requirements on consent should be clarified so as to make it easier to know what is required in order to allow individuals to be able to make a truly informed consent.

afforded to them during the data collection and processing stage. In practice, individuals commence their struggle in and out of courts to protect their rights only if an adverse external action has been taken against them by a security agency (denial of entry into a country or security screening, etc.); otherwise, they may never know that they were subjected to unlawful data processing practices in the AFSJ context.

The right of access to justice, although an illustration of the actual implementation of the principles of accountability, transparency and openness in AFSJ personal data processing, deserves special attention while elaborating upon the amendment of the EU DPF, because of its grave, direct significance for individuals.

The DPFD leaves it to Member States to introduce judicial remedies in favour of data subjects:

> [w]ithout prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject shall have the right to a judicial remedy for any breach of the rights guaranteed to him by the applicable national law. (Article 20)

In addition,

> [a]ny person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision shall be entitled to receive compensation for the damage suffered from the controller or other authority competent under national law. (Article 19.1)

Therefore, in AFSJ data processing the DPF does in effect enable individuals to seek redress and even collect money from those law enforcement agencies that have unlawfully processed their data. Their right of access to justice is effectuated through administrative and judicial processes, in which they can sue directly and which expressly involves monetary indemnity. Yet it does not seem to allow for the possibility of class-action lawsuits, an option that should be made available to individuals.[487]

Nevertheless, all these measures are ultimately useless if individuals are not afforded the proper opportunity to build up and prove their case. This seems to be a nearly impossible task under the EU DPF at present. Data subjects do not need to give their consent in order for their data to be processed by security agencies. They may also not be informed of such processing if a security agency so requires (see Article 16.2 of the DPFD). The same applies to their right to access their data, which may likewise be restricted for a series of reasons (see Article 17.2 of the DPFD).

Things are more difficult for individuals if processing is performed by third countries. Various bilateral agreements for PNR data processing allow third countries (the US, Australia and Canada) to process personal information originating in the EU. This option is present in the text of the DPFD as well. The usual mechanism for EU citizens in this case is that they are afforded those means of redress that are available to the processing country nationals. Despite its *prima facie* fairness, this measure is actually impossible to put into practice. To do so, EU nationals will have to enquire with officials and take up judicial action in a foreign country and under a foreign jurisdiction. This procedure will be a costly and difficult to follow, if not a discouraging experience altogether.

Jurisprudence is also an important factor. The DPFD seems to require that an individual sue the security agencies of another Member State, if his or her rights are infringed while processing within its scope takes place.[488] In other words, a national of a Member State whose data have been transmitted by the security agencies of that Member State to those of another Member State, where unlawful data processing has taken place, will ultimately

[487] See European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, op. cit., p. 32.

[488] See its Article 19.2.

have to sue in front of foreign courts applying foreign ('national') law.[489] This is a practical difficulty that hinders the individual right of access to justice in the AFSJ.

Similar difficulties met in the DPD context (caused most notably by social networking websites and cloud computing) have led to discussions during the EU DPF amendment process about introducing a 'closest to home' individual right of redress.[490] This would enable data subjects to seek redress in front of the courts that are closest to their home, in this way affording them practical and reasonable opportunities to defend their fundamental right to data protection.[491] An extension of such a right in the AFSJ context, regardless of whether through a single regulating document or the respective specialised provisions, would substantially assist individuals while protecting their rights within a processing environment that in any case provides them relatively few guarantees.

4.4. The EU DPF amendment process: Lessons from the DPD amendment discussions on common principles and basic legal elements

The EU DPF amendment process is ambitious in scope. On the one hand, it aims at updating the DPD, which has constituted the basic principle-setting text in the EU for the past 15 years, for the new processing environment. On the other hand, it aims at bringing unity and comprehensiveness in AFSJ data processing, which remains fragmented, piecemeal and perhaps over-accommodating to the needs of law enforcement agencies. In parallel, it also needs to decide upon the law-making means it shall employ. It needs to choose whether to amend the existing instruments (the DPD and the DPFD) for the post-Lisbon environment, thus maintaining an increasingly indistinguishable separation between security and commercial personal data processing, or to merge them into a single, all-regulating, data protection instrument – a task that would also require a decision upon the form of such an instrument (a directive? a regulation? other?). It would have been a success to complete either of these tasks adequately during the EU DPF amendment process; taking all of them up at once would require bold, perhaps groundbreaking, decision-making.

In view of these difficulties, it has been submitted that the EU DPF review process ought to primarily focus on addressing the main, contemporary, data protection concerns studied in this report. To further assess the practical consequences of the principles of transparency, openness, accountability and necessity analysed above, this last section of chapter 4

[489] The DPFD is not applicable at national level; therefore, each Member State is free to apply whichever application on security-related personal data processing it wishes.

[490] The Article 29 Data Protection Working Party has already attempted to introduce similarly protective criteria since 2002 (see its Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites – Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, WP 56, 30.05.2002), admittedly adopting a rather creative reasoning (see Moerel, L., *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?*, International Data Privacy Law, 2011, Vol. 1, No. 1, pp. 28-46). However, the Council's position attempts to keep equal distances in this matter (see Council Conclusions, op. cit., p. 14).

[491] In the same context, the EURODAC system takes notice of where the "input" of the data was performed (see Art. 13, Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 361, 15.12.2000). The Eurodac system enables Member States to identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union by means of comparing fingerprints. Although the Eurodac system consists of a Central Unit within the Commission, equipped with a computerised central database for comparing fingerprints, it is up to the Member State of "origin" (input of personal information) to ensure that data protection regulations are observed.

borrows from the current EU DPF framework certain ideas that could find application in the AFSJ data processing field. Despite the identified need to perhaps regulate the AFSJ field separately, this section aims at examining the current DPD review process in order to single out those ideas that are particularly useful and relevant to the DPFD review process to come. In other words, the question addressed in the following analysis is what can be learned for AFSJ data processing from the DPD review process underway.

Therefore, this fourth section focuses on the means of data protection. Essentially, these are either drawn from the present data protection arsenal of the DPD or they are suggested as useful additions to it. In this regard, the application of the fair information principles in the AFSJ environment are discussed together with DPIAs and privacy-by-design system architecture, and suggestions are given for a new role for national DPAs and for the WP29 in the amended EU DPF.

4.4.1. Fair information principles

The fair information principles are a basic element of the EU and indeed the global data protection model. They have a history of more than 40 years and have been included, beyond the EU, in various international and regional instruments, such as Convention 108, the OECD guidelines or the UN guidelines.

As far as the EU DPF is concerned, the fair information principles are laid down primarily in Article 6 ("Principles Relating to Data Quality"), and also in Articles 16 ("Confidentiality of Processing") and 17 ("Security of Processing") of the DPD.[492]

An important observation with reference to the DPD text is that there are no exceptions whatsoever to the application of the fair information principles on any personal data processing.[493] Still, it should be noted that not each principle in the list has been received with the same enthusiasm by data controllers within or outside the EU. For instance, the confidentiality and security of processing principles or the principle on the accuracy and

[492] Article 6.1: Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Article 16: Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17.1: Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

[493] Apart from "journalistic, artistic or literary" purposes (freedom of expression); to this list it has been, perhaps convincingly suggested, that "social research" (or "research" in general) purposes be added as well (see, for instance, Erdos, D., Systematically handicapped? Social research in the data protection framework, *Information & Communications Technology Law*, Vol. 20 No. 2, June 2011, pp. 83-101, and also the EDPS Opinion of 14 January 2011, p. 53 – however, identifying a different challenge in the same freedom of expression context).

updated status of the data stored constitute self-evident principles to which any well-intentioned data controller, regardless of whether a corporation or a law enforcement agency, would find it hard to object.

Nevertheless, that is not the case with the purpose-specification principle. According to the relevant provisions, "personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". The limitation of such "further processing" has frequently raised substantial objections from the personal data processing industry and security agencies alike, each for its own purposes. For their part, security agencies would generally prefer not to be forced to observe restrictions on how best to handle their data (for example, in processing pertaining only to a single crime and not to any other potentially criminal activity in the future by the same individual).

The above helps explain the profoundly different approaches between the texts of the DPD and the DPFD on this issue.[494] Although the requests of security agencies were ultimately accommodated in the text of the DPFD, it is not evident whether such potentially unlimited processing is in agreement with the individual right to data protection.

This difference of approaches needs to be resolved in favour of individuals and the protection of their personal data. To this end, it should become explicit in the text of the amended EU DPF, regardless of its ultimate format, that the unequivocal version of the fair information principles included in the DPD and not the DPFD version[495] ought to find uniform application in all personal data processing in the AFSJ.

4.4.2. The role of 'soft law': DPIAs[496]

Self-regulation has often been suggested as a useful instrument for data processing regulation.[497] Self-regulation, however, is viewed differently in different parts of the world. Outside the EU, and most notably in the US, self-regulation is frequently used as a regulatory alternative. Within the EU's formal framework for data protection, self-regulation is mostly meant as an institutional accessory (meaning, under the control of DPAs) to the application of data protection, through the release of case-specific regulations for certain processing categories (direct marketing, credit, etc.). The most commonly seen methods to achieve this are specialised codes of conduct.

This 'soft law' model has proven useful over the years, and indeed in some cases, such as international data transfers, it is formally counted as part of data protection regulation.[498]

In this context, a lot of attention has been drawn recently to the potential merits of DPIAs.

A DPIA[499] may be defined as a systematic process for evaluating the potential effects on privacy and data protection of a project, initiative, proposed system or scheme and for finding ways to mitigate or avoid any adverse effects.[500] It is fair to say that the DPIA originates from the positive experience of environmental, regulatory and social impact

[494] See for instance the Framework Decision Article 3.2.

[495] See also European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, pp. 2 and 6.

[496] The authors would like to thank Dariusz Kloza for his useful input.

[497] See European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, p. 31.

[498] See Art. 25 of the DPD.

[499] 'Privacy Impact Assessment' (PIA) outside the EU.

[500] Wright, D., *Should privacy impact assessments be mandatory?*, Communications of ACM, July 2011 (forthcoming).

assessments, commenced in the 1960s. The idea grew and developed in a number of common law countries (e.g. the US, the UK[501] and Australia) in the mid-1990s.

If we were to summarise briefly the advantages of conducting a DPIA, it would be pointed out that it primarily allows the identification and management of risks, the avoidance of loss of reputation and unnecessary costs. Opponents would probably view DPIAs as a regulatory burden, an unnecessary cost and a cause of delays (especially when it is mandatory).

The concept of the DPIA recently ascended very high on the EU's agenda. First, in January 2010 the Commission published a report on new privacy challenges,[502] in which it overviewed DPIA policies around the world and briefly analysed the pros and cons of DPIAs. This report stated that "it is much easier to produce privacy-friendly systems if data protection issues are considered early in their design stage".[503] Second, the European Parliament, in its resolution in May 2010 on PNR, stated that "any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test".[504] Third, the need for public authorities and industry to better assume their responsibilities by means of DPIAs was explicitly addressed by Commissioner Reding in July 2010.[505] Also, the WP29 in February 2011 endorsed a DPIA for RFID (radio frequency identification) applications.[506]

The Commission Communication expressly states that to highlight data controllers' responsibility, an examination will be made of whether to include "in the legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases".[507] These cases could include, inter alia, the processing of sensitive data or those for which "the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance". In view of the potentially harmful personal data processing conducted in the AFSJ environment, DPIAs could prove a useful accessory, particularly in light of the principle of accountability – for instance, analytical impact assessments could be useful in detailing the particulars and assessing the risks prior to conducting profiling operations. In the same vein, DPIAs could also include an analysis of the 'necessity of the processing' test, which should be present in all AFSJ data processing operations. After all, it is suggested that should this have been the case, the 25 EU data-exchange mechanisms currently existing or under consideration, as described in section 2.2 of this study, would not all have qualified under the test.

---

[501] The UK was the first country in Europe to develop a PIA manual in 2007. Cf. Information Commissioner's Office, *Privacy Impact Assessment Handbook*, Version 2.0 (2009) (http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf).

[502] European Commission, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Final Report*, 20 January 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

[503] Ibid., p. 50.

[504] European Parliament, *Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada*, P7_TA(2010)0144, 5 May 2010.

[505] Commissioner V. Reding, "Towards a true Single Market of data protection", SPEECH/10/386, Meeting of the WP29 on the "Review of the Data protection legal framework", Brussels, 14 July 2010 (http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386).

[506] Article 29 Data Protection Working Party, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, WP 180, 11 February 2011. This issue dates back to a 2009 Commission's recommendation on DPIA requiring the industry and other stakeholders to develop a DPIA framework for RFID. The first proposal, submitted in March 2010, presented a good starting point, but it did not gain the full support of the Working Party. The revised proposal, submitted in January 2011, eventually got its acceptance.

[507] See 2.2.4.

4.4.3. Privacy by design – Privacy-enhancing technologies

Privacy-by-design system architecture is no newcomer in the data protection field: in fact, Recital 46 of the DPD states that

> whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing.

No connection to such system architecture or to the obligations placed upon data controllers in the text of the DPD was made, leaving the notion of privacy by design merely a general guideline: data controllers ought to design systems that take into consideration data protection concerns.[508]

Such system architecture must be proportional to the type of processing. The same Recital adds that "these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected". Thus, although privacy concerns must be kept in consideration while designing new processing systems, the measures to be undertaken must be proportionate to the state of the art, costs and the risks posed by the relevant processing. Evidently, because processing in the AFSJ context may prove sensitive to individual rights, while the origins of datasets involved in such processing may not always be law enforcement sources,[509] the relevant systems ought to incorporate security mechanisms that are proportionate to such risks.

The Council Recommendation on profiling encourages the use of privacy-by-design systems, particularly in the form of PETs, in the relevant processing:

> Member States should encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their planning stage, notably through the use of privacy-enhancing technologies. They should also take appropriate measures against the development and use of technologies which are aimed, wholly or partly, at the illicit circumvention of technological measures protecting privacy (Article 2.2).

In the same way, the Commission Communication connects PETs and the privacy-by-design system architecture, and under the principle of accountability analysis, suggests "further promot[ing] the possibilities for the concrete implementation of the concept of Privacy by Design".[510] Its idea is that "the principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal". Hence, the discussion is whether to upgrade a general guideline, as set out today in the text of the DPD, into a firm obligation for all data processors, regardless of whether they are involved in AFSJ or other personal data processing. Although it is likely that PETs and privacy by design will gain in importance in the text of the new EU DPF, their regulatory implementation will have to address substantial concerns, namely how to justify specificity within abstract legislative texts with regard to the actual technological measures to be applied in different processing systems.[511]

---

[508] It should be noted that the notion of privacy by design is broader than the notion of Privacy by Default (on examples of the latter, for instance internet browser settings and facebook settings, see also Hijmans H., op. cit.).

[509] See also European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, p. 6.

[510] Under section 2.2.4. See also European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, p. 35.

[511] See Hijmans H, op. cit.

Decisions on system architecture, and whether to implement privacy by design or install PETs, are important – especially given the multitude of data processing systems deployed or under development. Networked convergence and 'data-sharing by default', through the application of the principles of availability and interoperability, threaten the individual right to data protection in the context of the networking and profiling society. If, however, systems that provide for immediate information exchanges have acquired by default privacy-by-design architecture or extensively use PETs, translating data protection provisions into technical measures that are programmed to automatically intervene whenever individual rights are infringed, then an added safeguard for individual data protection would become available in the AFSJ processing sector.

4.4.4. National DPAs

In the EU DPF, national DPAs are intended to constitute the main instrument of data protection enforcement within their respective jurisdictions.[512] To this end, they have been equipped with independent status and significant material resources. DPAs will require substantial strengthening, however, if both of the claims above are to remain relevant.[513]

A "main instrument of data protection enforcement" means that DPAs are responsible for ensuring effective implementation of their respective national acts on data protection within their jurisdiction. There are several means to achieve this: investigative powers, powers of intervention and the power to engage in legal proceedings.[514] Yet all of the above powers refer to DPAs as a self-sufficient instrument: it is for the DPA to decide who to control and when to intervene in and out of courts. Nevertheless, the practice is quite different. Individuals, in addition to asking for assistance from their DPAs, are most likely to bring their case in front of courts, either to achieve monetary indemnity paid to themselves or to win an unequivocal and case law-formulating victory. In all relevant litigation, national DPAs only rarely intervene in favour of data subjects, despite being empowered by law to do so[515] (maybe as a result of politics or lack of resources). Still, it is in exactly this litigation that DPAs ought to be involved by definition, supporting individual rights whenever infringed. National DPAs should be explicitly reminded of their role as assistants to individuals in and out of courts, regardless of whether in an AFSJ or e-commerce context, in the text of the amended DPF.

Security-related processing traditionally has a much-troubled relationship with DPAs. Evidently, security agencies would prefer for their activities to lie outside the monitoring of DPAs, or if that is not possible, for the relevant regulatory framework to give to DPAs as few intervention powers as possible. At the EU level, EUROJUST has installed its own monitoring mechanism, keeping away from general schemes controlling data protection. In addition, the relationship between DPAs and the intra-EU PNR processing system still remains to be seen in the text of the relevant directive currently under development.

The DPFD, for its part, appoints national supervisory authorities (in its Article 25), which may coincide with those already established by the DPD.[516] In this way, a harmonising effect at least at the Member State level is indeed achieved, although this by no means constitutes the norm in AFSJ processing, given the patchwork of data protection regulations and mechanisms in effect. After all, an EU monitoring mechanism, such as the WP29, is still missing in security-related processing.

---

[512] See European Commission, *Communication on A comprehensive approach on personal data protection in the European Union*, 2.5.

[513] European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, p. 44.

[514] See Art. 28 of the DPD.

[515] See, for instance, Article 25.2(c) of the DPFD.

[516] See DPFD Preamble, 34.

A more effective and comprehensive monitoring mechanism is indispensable, in order for the EU DPF provisions to be implemented in practice. Unless an independent coordination body is granted the power to run checks and impose penalties on any type of processing within its jurisdiction, regardless of whether it is for security or commercial purposes, the new regulatory framework will be toothless and shall ultimately afford very little protection to individuals. As far as concrete measures for the AFSJ sector are concerned, under the amended EU DPF the DPAs should be allowed direct access to law enforcement datasets, when in their own judgment (and not that of the agencies concerned) security-related interests will not be put at peril. Such access would be particularly useful and relevant in the event of old, archived data. DPAs should also be made competent in the event of disputes to recommend a remedy or even to impose a solution assisting individuals while protecting their rights.

4.4.5. A new role for the WP29

The role of the WP29 has proven indispensable for EU data protection over the years. The WP29 has become the main body for consultation and harmonisation on data protection issues within the EU. In addition, it has frequently taken a proactive role as a privacy watchdog, identifying difficulties and recommending policies in cutting-edge technologies or newly-released business models. Its essential role while assessing the data protection level of third countries, in view of data exports from Member States, cannot be overstated.

Even within the DPD data processing context, the lack of a formal office for harmonisation within the EU, to which national DPAs could refer whenever they find it appropriate, is deeply felt. In the AFSJ context, no similar group of any legal status exists, as relevant provisions have failed to remain in the text of the DPFD. This important shortcoming needs to be addressed in the amended EU DPF.

On the other hand, the WP29, despite its central role, remains more or less a closed office, to which access (and appointment) is given only to its privileged members, the DPAs. Yet its harmonisation role would be considerably enhanced if it were also accessible to other parties in data processing (data controllers and data subjects) that may have a vested interest in a unified implementation of data protection rules across the EU.

In this light, the role of the WP29 should be strengthened, if not as an enforcement mechanism itself, most definitely as a central, permanent, open office for the furthering of data protection and privacy purposes in the EU.[517]

[517] See also the European Commission, *Communication on a comprehensive approach on personal data protection in the European Union*, 2.5; the European Parliament, *Report on a comprehensive approach on personal data protection in the European Union*, p. 43. The EDPS however "questions the fact that the Commission (and more specifically the Unit) is at the same time member, secretariat and addressee of the Working Party's opinions" (143); he also suggests that the way in which he and the Working Party cooperate could be fine-tuned (152 ff).

5. CONCLUSIONS AND RECOMMENDATIONS

5.1. Conclusions

This study has examined the new challenges facing the political, legal and technical aspects of the future EU framework for the protection of personal data in the AFSJ. It has explored the relationship between data protection and privacy on the one hand, and data processing for security purposes in law enforcement policies and amongst EU-level agencies on the other, in the context of the revised legal framework on data protection to be launched by the European Commission before the end of 2011. The study identifies a set of common principles and standards upon which the new EU legal framework and the EP's position should be built in the post-Treaty of Lisbon landscape.

The protection of personal data currently enjoys unprecedented value and status in the EU. It is recognised as an autonomous fundamental right in the now legally binding EU Charter. It is also acknowledged in the new (post-Lisbon) Treaty framework, which provides an express legal basis for the establishment of a comprehensive legal instrument for data protection, covering both the former first and third EU pillars. The announced review of the EU's legal framework for data protection must take these pivotal changes as a starting point, and aim at substantiating and ensuring a genuine impact of the fundamental right to the protection of personal data across all policy areas, including the EU's AFSJ.

Even if the post-Lisbon Treaty framework decidedly reinforces the formal status of the right to the protection of personal data in the EU, the assurance of this fundamental right is still actually rather precarious. This is especially true as far as the AFSJ is concerned, and notably the field of police and judicial cooperation in criminal matters (corresponding to the old third pillar). The vulnerability of the right to data protection stems from various challenges linked to the unrelenting deployment of measures relying on the massive processing of data related to individuals. In particular, this study has identified and examined a number of issues connected with the growing reliance on security technology, especially the processing of personal data for law enforcement purposes in the AFSJ, focusing mainly on the following three:

- There are general concerns tied to the development of EU policy-making in the AFSJ. EU decision-making practices consider technology an unchallenged policy option and are increasingly programmatic in nature. The default position is information exchange or 'data sharing by default'. Yet little attention has been paid to assessing the impact, proportionality and necessity of these policies and systems. EU policy-making has been 'programme driven' rather than 'evidence driven', and technical solutions have been systematically pursued in a way that has been detrimental to the quality, accountability and transparency of decision-making. There are multiple conflicting programmes, which see different groups of actors pursuing separate negotiations on their own priorities. New initiatives and large-scale IT systems are tabled and launched without proper consideration of projects already underway, leading to a situation in which it is extremely difficult to establish who is processing the data of whom, for which purpose, with whose consent and through which procedures. These developments can lead to an overemphasis on the technical elements of data processing to the detriment of legal and political considerations.
- In addition there are specific issues linked to the transformation of law enforcement activities in relation to technology and what we call 'the networking and profiling society'. Current law enforcement activities are premised upon the generalisation of data processing, purpose (un)limitation (function creep) and an increasing emphasis on prevention, anticipation and a proactive (intelligence-based) approach to policing. The logics of dataveillance, proactivity and profiling can generate frictions with core 'fair information principles' of data protection law, such as proportionality, necessity, purpose limitation, consent and access.

Profiling, as a form of pattern recognition enabling the identification of previously unknown persons based on assumptions about their behaviour in the future, is problematic insofar as it relies on the massive processing of personal data and additionally does not constitute evidence. As such, the growing reliance on profiling can entail not only major interferences with the right to personal data protection and the right to privacy, but also a reversal of the presumption of innocence and a challenge to the proper functioning of the criminal justice system. These practices and technologies also negatively affect key elements of the fundamental rights included in the EU Charter, the ECHR and the case law of both the CJEU and the ECtHR, and stand in an awkward relationship with the principles of adequacy, proportionality, transparency and access to justice.

- Finally, these dilemmas arise not only from the practices of national law enforcement authorities, but are also increasingly of relevance for EU home affairs agencies, as well as inter-agency cooperation. Bodies such as EUROPOL and FRONTEX have become 'data controllers' in their own right in the past ten years, in some cases without the proper legal framework to do so. In the absence of direct operational responsibilities, access to personal data has become a key area for the senior management of EU home affairs agencies, reinforcing the trend towards increased dataveillance in EU law enforcement activities. EU home affairs agencies are therefore becoming central actors (data controllers) in personal data exchange and processing.

These trends entail considerable ramifications for sound and efficient policy-making principles, including the Union's obligations in the field of fundamental rights to data protection and privacy as envisaged by the EU Charter. What can and should be the role of the EP in this evolution, in accordance with its traditional position and new capabilities?

The EP has traditionally called for the urgent reinforcement of the level of protection of personal data in this area, despite resistance from the Council and more recently interested parties such as EUROPOL. The EP has given much attention to strengthening its own role in the EU institutional framework in general, and in the AFSJ in particular, for the purpose of better promoting and protecting fundamental rights, including the protection of personal data. The Treaty of Lisbon has brought about changes in this respect, which have strengthened the role of the EP in decision-making in the AFSJ, and opened up new possibilities for improving the level of protection of personal data. Their advent thus represents a major opportunity for the EP to prove that it can indeed be used for the sketching of EU policies that effectively guarantee fundamental rights in a broad sense, and specifically the protection of personal data, and brings about the responsibility for the EP to substantiate its traditional position in the area.

The EP has played a decisive role in formally recognising the protection of personal data as a fundamental right of the EU, as well as in the construction of the EU legal framework for the data protection. Despite persistent limitations to its institutional powers over many years, it has managed to ensure some progress in the level of protection granted to individuals by the EU legal framework, and to block, restrict or at least retard some EU security initiatives that seriously threaten the fundamental rights to privacy and to the protection of personal data in the AFSJ.

The entry into force of the Lisbon Treaty provided the EU with a legal basis allowing for the adoption of a new instrument for 'cross-pillar' data protection, and solved various institutional issues perceived as an obstacle to the establishment of a comprehensive legal framework for the protection of personal data. The EP has already made use of some of its recently acquired powers for the advance of EU privacy and personal data protection, even if possibly not to their full extent. It is nonetheless unclear whether the EP has yet realised the full implications of the binding force acquired by the EU Charter, and thus of its groundbreaking Article 8 on the protection of personal data – particularly that it imposes on EU institutions the obligation (as opposed to the possibility) to fully substantiate the assurance of this emergent right throughout EU law.

As evidenced by this study, however, there is no linear relationship between more involvement of the EP in decision-making, on the one hand, and a higher level of personal data protection granted to individuals, on the other. Sometimes, the strengthened participation of the EP in legislative procedures has led to a lowering of data protection and privacy standards. The EP seems unable (or perhaps unwilling) to question and oppose some of the factors obstructing the assurance of EU fundamental rights in the AFSJ, such as the continuous development and implementation of new practices in data processing. Struggles and controversies over data processing for law enforcement purposes in the AFSJ have limited the possibility for the EP to address or resist all EU security initiatives with strong implications for the rights to personal data protection and privacy, and actively supported some measures without making sure that they were accompanied by fully effective and satisfactory safeguards.

The promotion of data protection and privacy should continue to be key policy priorities for the EP in its new role as co-legislator in these areas. A change in its traditional, pro-data protection approaches would jeopardise its legitimacy in this dynamic field of the AFSJ. The EP has been the most active EU institution in underlining the importance of accurately understanding the implications of profiling and contemporary data-mining practices for the fundamental rights of individuals, especially when these techniques are deployed in the context of security and law enforcement policies. The EP should therefore remain vigilant in the face of the possible adoption of any EU security measures and systems based on profiling, and sustain its calls for a debate on the need to approve detailed EU provisions on the subject.

One of the major current challenges for the EP is to work towards a satisfactory mainstreaming of personal data protection in the AFSJ – to find a way to reconcile the early and effective consideration of data protection and privacy concerns with programmatic policy-making, which tends to systematically view technology and personal data processing as undisputed policy options. The updating of the EU's DPF is also an opportunity to examine how the EP can play a role in the increasing use of technology for law enforcement purposes in the EU's AFSJ – where it should still support the principles and values it has upheld over the past decades to ensure its legitimacy as an actor in this policy domain.

The fundamental right to data protection should not only function as a 'requirement' to be complied with when the actual policy decision on the deployment of data processing measures has been already taken. It should also serve to effectively preclude the adoption of massive data processing or new policies and systems. Framing the right to personal data as an obstacle to (be balanced against) security can only be self-defeating for data protection and fundamental freedoms and rights more generally. Data protection should not be considered solely as a set of safeguards needed to match technical developments. It should provide a framework within which technical developments take place when these have been proved necessary, proportionate and compliant with fundamental rights. A strong data protection framework should be the premise or starting point of any security-related measure, mechanism or practice in the EU. This would be the best (and only) way to ensure security. The EU's objective is to build an area of freedom and justice as much as an area of security. The EP should reassert the centrality of data protection and privacy as a point of departure and continual process in data processing policies and decision-making arrangements in the EU's AFSJ.

The consolidation of the EU right to personal data protection must not take place to the detriment of other rights and principles. Just as it is crucial for EU institutions to fully apprehend the requirements derived from the right to the protection of personal data, it is equally important for the EU not to disregard, because of an overemphasis on this right, assurance of the right to privacy or any other fundamental right recognised in the EU Charter, the ECHR or common constitutional traditions of Member States. Through its case law on the right to privacy, the ECtHR has provided critical knowledge on how to assess the compatibility of contemporary surveillance (data processing) measures in the light of human rights standards. In this sense, it also needs to be noted that the EP benefits from the guidance of two major consultative bodies specifically devoted to the protection of

personal data, but of only one concerned with fundamental rights in general. This can have undesired effects in the framing of some discussions, unless a deliberate effort is made to permanently widen the scope of concerns and perspectives.

In the post-Lisbon environment, discussions on the review of the EU DPF – admittedly aimed primarily at the Data Protection Directive – invite a re-evaluation of the regulatory framework for personal data processing in the AFSJ. As revealed by this study, the relevant regulations of data protection currently in effect at best adopt an isolated, piecemeal approach and at worst grant generous exemptions, perhaps appearing overeager to please, in favour of the requirements of law enforcement processing. This regulatory patchwork ultimately forms a framework that is difficult to follow and apply, to the disadvantage of exactly those persons whose interests it supposedly protects, that is, individuals. On the other hand, data processing in the scope of police and judicial cooperation in criminal matters does present a number of unique characteristics that substantially differentiate it from other, routine, personal data processing.

It is necessary that the new legal framework on data protection extends the general data protection rules to policies falling under the former third pillar (now Chapter 4 on Judicial Cooperation in Criminal Matters, and Chapter 5 on Police Cooperation of Title V TFEU). Furthermore, what is required is an amended regulatory framework for data protection in data processing across the AFSJ that will both accommodate special law enforcement needs and grant effective protection to individual rights.

The drafting of such an amended regulatory framework needs to take into consideration the legal foundation upon which it will be based. Apart from the Lisbon Treaty, with its Article 16 TFEU as well as exemptions and acknowledgements in its Protocols and Declarations, the imminent accession of the EU to the ECHR means that the extensive case law of the ECtHR likewise needs to be taken into account. In this sense, the sustained scrutiny by the ECtHR of security-related practices in data processing and the Court's insistence on the application of the principles of necessity and legality warrant positive expectations, at least from the viewpoint of data protection.

A concrete example of the continuing importance of ensuring a high level of personal data protection in the EU data protection law applying to the area of police and judicial cooperation in criminal matters can be found in the discussions on reinforced cooperation among Member States in the area of evidence gathering and criminal investigation. More specifically, an initiative such as the European Investigation Order (EIO) in criminal matters, proposed by seven Member States in April 2010,[518] confirms the urgency of establishing clearly defined and strong provisions for data protection in the field. Indeed, the proposed EIO would allow Member States to carry out, following the decision of another Member State, such investigative measures as searches and seizures, and possibly the interceptions of communications and monitoring of bank accounts. The initiative originally lacked any measure on the applicable provisions for data protection, leading to a critical reaction from the EDPS, who underlined that this type of reinforced cooperation reiterates the need for a comprehensive EU framework for data protection.[519]

[518] Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters, OJ C 165, 24.6.2010, p. 22.

[519] EDPS, *Opinion of the European Data Protection Supervisor on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Hungary, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Finland and the Kingdom of Sweden for a Directive of the European Parliament and of the Council on the European Protection Order, and on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters*, OJ C 355, 29.12.2010, pp. 1-9.

The selection of the regulatory means for regulating personal data processing in the AFSJ is therefore important and far from straightforward. The law-making means could include anything from special AFSJ provisions within a single, EU-wide, data protection instrument, to the amendment or replacement of the Data Protection Framework Decision currently in effect. Yet over-elaboration of the regulatory means risks overlooking discussions as to the best ways to translate the data protection concerns into comprehensive, general and specific legal principles and standards. These presently include, among others, such issues as regulating the networking and profiling society, implementing the principle of accountability in AFSJ data processing and reinforcing the individual right of access to justice.

The increasing deployment of technologies for law enforcement purposes, the policies emerging from the networking and profiling society and the centrality of personal data in the work and cooperation between EU home affairs agencies need to be carefully scrutinised through specific, practical provisions for data protection, in order for individual rights to be effectively protected. The application of the principle of accountability to AFSJ processing actors, which until today has remained largely unknown, would be a significant step towards this end. Ultimately, individuals need to be provided with simple and accessible means in order to prove their case in front of courts – indeed, the same factors that make personal data processing special in law enforcement also make necessary the reversal of procedural burdens placed upon individuals while proving their case in courts.

The new EU DPF needs to be designed in a way that ensures it has a genuine impact on current and future EU security measures, systems and practices, and effectively addresses the dilemmas posed by technologies and data processing practices in the AFSJ. This result can only be attained if data protection becomes relevant at all stages of EU policy-making. For this to occur, certain common principles and basic elements need to be ensured.

When regulating data processing in the AFSJ, the lessons learned from the discussions on the amendment of the Data Protection Directive could provide useful insights. Data protection not only consists of a set of legal principles that should be respected. It also encompasses a wider number of standards, guidelines and institutional arrangements that make practical the actual provision of this fundamental right to the individual and make it applicable to EU policy-making processes as well. The means for data protection, including both those at hand (such as the fair information principles or the national DPAs or the WP29) and under consideration (such as implementation of privacy by design or impact assessments), if properly adjusted in the law enforcement (police and criminal justice) field, could form a useful starting point, once the regulatory means have also been decided, for the actual contents of the amended framework for personal data processing in the AFSJ.

5.2. Policy recommendations

In light of the above we put forward the following policy recommendations:

1) One of the key elements in the revision of the EU DPF should be the extension of the general data protection rules that apply to data processing in police and judicial cooperation in criminal matters (which have until now been kept aside), fully substantiating the fundamental right to the protection of personal data across EU law. This extension would make a key contribution to resolving the issues posed by the increasing reliance on technology for security purposes. More precisely,

   - it would address the concerns expressed by the European Commission and DPAs about the shortcomings and current deficits affecting the scope of the DPFD;
   - it would provide benchmarks and general standards against which initiatives aimed at establishing new data processing schemes could be evaluated. The extension would contribute significantly to the policy process pertaining to the deployment of new data processing schemes and systems at the EU level; and
   - it would further make certain that the processing of data taking place under the

remit of EU home affairs agencies and the processing of data by national authorities is conducted according to the same standards, thus ensuring the equal treatment of citizens and third-country nationals along with the absence of discrimination.

2) Specific emphasis should be placed on the foreseeable orientations in data processing for security purposes to ensure that the data protection framework is robust and long lasting. The new DPF should develop a set of legal principles governing profiling in the EU's AFSJ. A definition of profiling should be included in the revised framework. This definition should also include the types of profiling that should be definitely prohibited under all circumstances and solid legal safeguards for those considered legitimate. The first type of profiling to be expressly prohibited is that which uses sensitive personal data as part of its basis. The second prohibition for profiling in the AFSJ should be on the use of unlawfully acquired data. Lastly, the profiling logic needs to adhere expressly to the general principles of data protection, particularly that of fair and lawful processing.

3) The EP should consider carefully the design of data protection supervision, as well as the structure for the coordination of supervisory authorities in the future EU data protection landscape. Both the supervision by and coordination of supervisory authorities will ultimately depend on the possible extension of the EU's main instrument for data protection to the former third pillar, but should in any case be aimed at ensuring that clear guidelines are provided to policy-makers envisaging the development and deployment of new security-related schemes involving data processing. These guidelines would in turn lay down the basis for sound, evidence-based impact assessments, which have been lacking so far.

   The principles of transparency and openness should be at the heart of this exercise. The new legal framework should make explicit reference to these principles. They should apply to data processors and controllers and to the processing operations themselves. The principle of accountability should be also further developed in the context of AFSJ processing. The lack of transparency, openness and accountability directly affects the individual's right of access to justice. Impact assessments of data protection could be a useful 'soft law' tool to implement the principle of accountability (and to address the data protection risks before conducting profiling) and the analysis of the 'necessity of processing' test.

4) National DPAs should be reorganised to allow them to play the decisive role entrusted to them by data protection law for monitoring the effective implementation of these legal principles and standards on the ground. The further harmonisation of their competencies should be carefully considered, particularly to make sure that they can be more actively involved in litigation in relevant jurisdictions and assist individuals to adjudicate their rights and freedoms. They should also be competent in the event of disputes to recommend a remedy or to come up with a solution assisting individuals to protect their rights.

5) Comprehensive provisions on data protection should be integral to the legal mandates of all EU home affairs agencies, requiring full compliance with principles of purpose limitation, purpose specification and rights for the data subject to access and correct the personal data held by agencies. Legal provisions must be accompanied by a robust supervisory mechanism that would ensure the practical application of these common principles and standards.

6) The EP should recommend the modernisation of supervisory and coordination mechanisms for the authorities responsible for data protection supervision in the field of police and judicial cooperation in criminal matters. The various joint supervisory bodies currently tasked with supervising data processing at the EU level by agencies like EUROPOL and EUROJUST are already very often staffed by the same officials operating under different 'hats'. An enhanced and strengthened supervisory role for the WP29 should be duly established in the next phase of data protection in the AFSJ.

7) The individual should be placed at the heart of the debates and legislative goals. A reversal of the burden of proof should be guaranteed in favour of the individual. The law enforcement authorities should be those convincing the courts about the lawfulness of the processing. The role of individual consent in personal data processing for security purposes should be placed at the centre of attention when used to justify such data processing. This should also be accompanied by a 'closest to home' individual right of redress to make certain individuals have practical and reasonable opportunities to defend their rights.

8) An independent evaluation or review of existing and future EU data-processing systems in the EU's AFSJ should be carried out by the EP. The adoption of a comprehensive framework for data protection is not a panacea in the short run. Initiatives, proposals and programmes for the development and deployment of new data processing schemes in the EU have proliferated over the past few years, to the extent that keeping track of all of them is proving a considerable strain not only for civil society organisations and DPAs, but also for EU institutions.

The revision of the data protection framework therefore seems a good occasion to undertake a general, in-depth review of existing, upcoming and envisaged data processing schemes. Since the entry into force of the Treaty of Lisbon places the EP in the position of co-legislator in addition to its pre-existing powers as a budgetary authority, it is fully competent and entitled to conduct this exercise. The elements of such a review have already been suggested in another study on behalf of the EP on EU activities in the field of security research and development,[520] which consist of the following:

- an account and budgetary review conducted by the Court of Auditors acting on the basis of Article 287(4) TFEU, which foresees that it shall assist the EP in exercising its powers of control over the implementation of the budget; and
- a data protection and privacy review. This review could be initiated by the EP through its Science and Technology Options Assessment unit, in liaison with the EDPS, the WP29 and the Fundamental Rights Agency acting in their advisory capacities. It should include consultations with civil society organisations and academia.

The legislative review should focus on assessing the necessity and proportionality of the present, upcoming and envisaged schemes for data processing. No further initiative in security-related data processing – particularly the impending 'smart borders' initiatives of DG Home Affairs – should be allowed to proceed until this review is completed and the data protection framework is adopted.

[520] Jeandesboz and Ragazzi (2010), op. cit.

ANNEX 1

Table 1. Tabled, upcoming and envisaged proposals for EU-level data systems for law enforcement purposes (as of April 2011)

Designation	Scope	Data processed	Costs	Data subjects
Tabled proposals				
European Criminal Record Information System (ECRIS)	Exchange of criminal records among the criminal records databases of Member States, in a standardised format	Information relating to the contents of the conviction of a Member State national, including the sentence, supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence. This information should be accompanied by the parameters regarding the degree of completion, level of participation and the existence of partial or total exemption from criminal liability.[521]	• **€8.2 million** in operational and administrative expenditures (some of the set-up costs absorbed by basing the communications infrastructure of ECRIS on the Commission's S-TESTA network)	• EU citizens facing a criminal trial in a Member State court
European Passenger Name Record (EU PNR)[522]	Allow for the access of law enforcement agencies to PNR data held by carriers (air travel) for prevention and detection as well as investigation and prosecution purposes	Biographic and payment data submitted to carriers by passengers on buying their ticket and at check-in. The current proposal includes 19 categories, comprising PNR record locator, date of reservation/issue of ticket, date(s) of intended travel, name(s), address and contact information (telephone number and email address), all forms of payment information, including billing address, complete travel itinerary for specific PNR, frequent	• Estimate of overall set-up costs (Member States and EU carriers): **€241 million**, with annual overall recurring costs of **€102 million**, broken down as follows: • **€221 million** in set-up costs for Member State public authorities and recurring costs (annual) of **€11 million** (personnel) and **€61 million** (maintenance)	• All passengers travelling to the EU. Internal flights are not covered by the proposal, although the Commission considers an extension would be possible in a few years' time should the Member States deem it necessary.

[521] In his September 2008 opinion on ECRIS, the EDPS expresses concern that the system might be used for the exchange of biometric data, a possibility that is left unaddressed in the text of the Decision, and which would call for an enhanced set of data protection measures (OJ C 42, 20.2.2009).

[522] European Commission, *Proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, 02.02.2011.

		flyer information, travel agency/agent, travel status of passenger including confirmations, check-in status, no show or go show information, split/divided PNR information, general remarks (including all available information on unaccompanied minors), ticketing field information (ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields), seat number and other seat information, code share information, all baggage information, number and other names of travellers on PNR, any API data collected, all historical changes to the PNR listed in numbers 1 to 18.	• **€20 million** in set-up costs for EU carriers and recurring (annual) costs of **€24 million** (communications, PUSH system) and **€6 million** (personnel and maintenance)[523]	
FRONTEX Information System (modification of existing FIS)	Give FRONTEX a limited mandate to process personal data related to the fight against criminal networks organising illegal immigration.[524]	Not specified	Not specified	• Persons suspected on reasonable grounds of involvement in cross-border criminal activities, in illegal migration activities or in human trafficking activities • Persons who are victims of such illegal activities and whose data may lead to the perpetrators of such illegal activities • Persons who are subject to return operations in

[523] One should note that the estimation of costs conducted by the Commission in the Impact Assessment for its original 2007 PNR proposal was significantly different. Set-up costs for Member States were evaluated at €614 million and €73 million in recurring costs. For carriers the estimate was €14 million in set-up costs and €7 million in recurring costs. In its 2011 Impact Assessment, DG Home notes that "[t]he actual costs will be somewhere in between these two assessments" (SEC(2011) 132, p. 7), which is arguably somewhat imprecise as regards set-up costs for Member States or recurring costs for carriers.

[524] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union,* COM(2010) 61 final, Brussels, 24.02.2010 and modifications suggested in the European Parliament's draft report (PE 475.754, 12.11.2010).

				which FRONTEX is involved

Upcoming proposals				
European Terrorist Financing Tracking Programme (European TFTP)[525]	Allow for the provision of financial messaging data by the private company in charge to a European authority, which might then selectively forward it to the US authorities in the context of the EU–US TFTP agreement	Not specified at this stage but within the range of the data provided for by the EU–US TFTP: *inter alia* name, account number, address and ID number of originators and recipients of financial transactions	Not specified at this stage	• Persons making use of banking services in the EU and abroad
Registered Traveller Programme (RTP)[526]	Allow the use of automated border controls for frequent, pre-screened and pre-vetted third-country nationals	Possibly similar to the data for Schengen visa applications (including biometric data)	See below entry on EES	• Volunteer enrolees from third countries on the 'negative' Schengen visa list. • The possibility of extending the RTP to EU citizens is considered
Entry/Exit System (EES)[527]	Automatically record the dates of entry and exit of third-country nationals with a visa obligation, identify overstayers and trace the travels of persons suspected of criminal activities	Biographic information with the possible addition of biometric data (fingerprints)	Combined cost of RTP and EES: • **€20 million** for the main system (centralised option) from the EU budget • **€6 million** annually in functioning costs (recurring) • **€35 million** across all Member States	• All third-country nationals with visa obligations (countries on the 'negative' Schengen visa list)
European Border Surveillance System (EUROSUR)[528]	Allow for the monitoring of the EU's southern maritime waters within a	EUROSUR would eventually process information on vessels (size, type, purpose, registry, location, destination, track data, history,	• No full impact assessment. Estimate: about **€806.5 million**, based on the following elements:	• The extent to which EUROSUR will process personal data has not been specified clearly.

[525] European Commission, *Roadmap – European Terrorist Financing Tracking Programme (European TFTP)*, DG Home, 10.2010.

[526] European Commission, *Roadmap - Initiatives on Smart Borders: Legislative Proposal to set up Registered Traveller Programme (RTP)*, 2010/JLS/03.

[527] European Commission, *Roadmap - Legislative proposal to set up Entry/Exit System (EES)*, 2010/JLS/04.

[528] European Commission, *Roadmap - Legislative proposal on the establishment of a European Border Surveillance System (EUROSUR)*, DG Home, 10.2010.

	Common Information System (CIS)	ownership, technical characteristics) and their activities as well as on persons (operators, passengers, crews, dock workers, etc.).[529] As such, EUROSUR "may involve the processing of personal data"[530] although the extent of this (e.g. biometric data?) has not been specified so far.	• Conservative option envisages costs of about **€5 million** to the EU budget, with Member States using up to 45% (about **€695 million** over the period 2007-2013)[531] of the funds available under the EBF to develop the required infrastructure • Costs incurred to the Security theme of the Seventh Framework Research Programme: about **€106.5 million** for the projects funded under the first and second calls of FP7-ST.[532] • This assessment does not take into account the use of the Schengen Facility/Cash Flow and Facility by Member States acceding to Schengen.	• Indications from European Commission documents suggest that the system might be called to process the data of ship owners and ship crew members.
Envisaged proposals				
EU Electronic System of Travel Authorisation (ESTA)[533]	Enable the screening of third-country nationals who do not face visa requirements prior to their departure	Biographic information (similar to US ESTA).	• Not specified at this stage; likely to have an impact on the EU budget	• All third-country nationals travelling to the EU regardless of their visa obligations.
European Index of Convicted Third-	Enable the Member States to exchange	The index will build on national criminal record systems. Two	The cost of a full index based on the ECRIS blueprint was estimated	• Third-country nationals with a criminal record in

[529] European Commission, *Commission staff document – Examining the creation of a European Border Surveillance System*, SEC(2008) 151, Brussels, 2008, p. 57.

[530] Idem.

[531] The total amount of funds available under the EBF is €1,820 million over the 2007-2013 period. Funds distributed among Member States out of the EBF for this period amount to €1,543 million.

[532] On the basis of the information provided by the European Commission in its January 2011 working paper on the technical and operational framework of EUROSUR (see SEC(2011) 145, 28.1.2011).

[533] European Commission, *Communication on the possibility of introducing an EU ESTA*.

country nationals[534] (EICTCN)	information regarding the criminal records of those third-country nationals who are facing conviction in a Member State	options are envisaged, for a decentralised and centralised structure. Data processed in a decentralised structure would depend on the capacities of national criminal-record systems, of which most process alphanumeric data and few have links with fingerprint databases. In the centralised version, the processing of biometric data could be established as a baseline requirement.	in 2006 at about €4 million, with additional (non-specified) costs to be incurred by the EU budget should the biometric option be pursued.	an EU Member State
European Police Record Index System (EPRIS)	Originally proposed by the German delegation at a Police Chiefs meeting (2 April 2007). According to the note transmitted by the Swedish Presidency to the Ad Hoc Working Group on Information Exchange in December 2009, EPRIS would give "law enforcement authorities [of Member States] a quick overview of whether and possibly where relevant police information on a certain person can be found".[535]	Commission feasibility study and report to the Council is expected in 2012.	See previous column	See previous column
Review of the Data Retention Directive[536]	Possibilities under consideration include a reduction of the data retention period, a clarification and specification of data	See previous column	N/A	• Same as initial Directive.

[534] Initially proposed in a July 2006 Commission working paper (COM(2006) 359 final, 4.7.2006). A feasibility study was launched in 2009 by DG JLS/Justice (attributed to Unisys) and released in January 2010 (not available).

[535] Council document 15526/1/09, p. 1.

[536] European Commission, *Proposal for a review of the Directive 2006/24/EC (Data Retention)*, DG Home, 9.2010.

	categories listed in the directive, and the withdrawal of the directive.			

REFERENCES

Literature

Amicelle, A., D. Bigo, J. Jeandesboz and F. Ragazzi (2009), *Catalogue of Security and Border Technologies at Use in Europe Today*, D.1.2., Oslo.

Amicelle, A. (2011), *The Great (Data) Bank Robbery: Terrorist Finance Tracking Programme and the "SWIFT Affair"*, CERI Research Questions No. 36, Centre d'études et de recherches internationals, Sciences Po, Paris.

Baldaccini, A. et al. (2008), *Controlling Security*, C&C CHALLENGE, Paris: L'Harmattan.

Bigo, D. and J. Jeandesboz (2008), *Review of Security Measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*, PE 393.289, May.

———— (2009), *The EU and the European Security Industry: Questioning the 'Private-Public Dialogue'*, CEPS INEX Policy Briefs No. 5, CEPS, Brussels, February.

Bigo, D. (2006), *The principle of availability of information*, PE 378.272, January.

Boehm, F. (forthcoming), *Information Sharing in the Area of Freedom, Security and Justice – Towards a common standard for data exchange between agencies and EU information systems.*

Breitbarth, P. (2011), Letter to the Head of Delegation of the EU Joint Review Team TFTP, Den Haag, 18 April.

Brouwer, E. (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden: Martijnus Nijhoff.

———— (2008), *The Other Side of Moon: The Schengen Information System and Human Rights: A Task for National Courts*, CEPS Working Document No. 288, CEPS, Brussels, April.

———— (2011), *Ignoring Dissent and Legality: The EU's proposal to share the personal information of all passengers*, CEPS Liberty and Security in Europe, CEPS, Brussels, June.

Campbell, D. (1999), *The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5*, in STOA (ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, PE 168.184, October.

De Hert, P. and R. Bellanova (2009), *Data Protection in the Area of Freedom, Security and Justice: A System Still to Be Developed?*, PE 410.692, Brussels, March.

De Hert, P. and F. Boehm (2011), *The rights of notification after surveillance is over: ready for recognition?*, Human Rights in the Digital Era Conference, University of Leeds, 16 September.

De Hert, P. and S. Gutwirth (2009), "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", in S. Gutwirth et al. (eds), *Reinventing Data Protection?*, Springer Science.

De Schutter, Olivier (2001), *Vie Privée Et Protection De L'individu Vis-À-Vis Des Traitements De Données À Caractère Personnel*, Revue Trimestrielle des Droits de l'Homme (R.T.D.H.), No. 2001/45, pp. 148-183.

De Vries, K. et al. (2010), *Proportionality overrides Unlimited surveillance: The German Constitutional Court Judgement on Data Retention*, CEPS Liberty and Security in Europe, CEPS, Brussels, May.

Erdos, D. (2011), "Systematically handicapped? Social research in the data protection framework", *Information & Communications Technology Law*, Vol. 20, No. 2, June.

European Parliament's Committee on Civil Liberties (2011), *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies FRONTEX, EUROPOL and the European Asylum Support Office*, EP Studies.

Flaherty, David H. (1986), "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies", *Science, Technology & Human Values,* Vol. 11, No. 1, pp. 7-18.

Future Group (2008), *Freedom, Security, Privacy - European Home Affairs in an open world*, Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, Brussels, June.

Geyer, F. (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS CHALLENGE Research Paper No. 9, CEPS, Brussels, May.

Gonzalez Fuster G., Gutwirth S., Ellyne E. (2009), *Profiling in the European Union: A high-risk practice*, CEPS INEX Policy Brief No. 10, CEPS, Brussels, June.

González Fuster, G., P. De Hert, E. Ellyne and S. Gutwirth (2010), *Huber, Marper and Others: Throwing new light on the shadows of suspicion*, INEX Policy Brief No. 11, CEPS, Brussels, June.

Guild, E. and E. Brouwer (2006), *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, CEPS, Brussels, July.

Guild, E. (2007), *Enquiry into the EU–US Passenger Name Record Agreement*, CEPS Policy Brief No. 125, CEPS, Brussels, March.

———— (2009), *Global Data Transfers: the Human Rights Implications*, CEPS INEX Policy Brief No. 9, CEPS, Brussels, May.

———— (2010), "The European Union after the Treaty of Lisbon, Fundamental Rights and EU Citizenship", presentation held at the Global Jean Monnet/European Community Studies Association, World Conference, 25-26 May.

Hempel, L., M. Carius and C. Ilten (2009), *Exchange of information and data between law-enforcement authorities within the European Union*, PE 419.590, Brussels, April.

Hijmans, H. and A. Scirocco (2009), "Shortcomings in EU data protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?", *Common Market Law Review,* Vol. 46, pp. 1485-1525.

Hijmans, H. (2011), "Principles of Data Protection: Renovation Needed?", presentation held at the International Data Protection Conference, Budapest, 16-17 June.

Hildebrandt, M. and S. Gutwirth (eds) (2008), *Profiling the European Citizen: Cross Disciplinary Perspectives*, Dordrecht: Springer.

Hobbing, P. (2008), *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, CEPS Special Report, CEPS, Brussels, September.

Hustinx, P. (2009), *Data Protection and the need for an EU Information Management Strategy*, Council Ad Hoc Working Group on Information Exchange Reception by Swedish Presidency, Brussels, 6 July.

Jay, R. (2007), *Data Protection Law and Practice*, London: Sweet & Maxwell.

Jeandesboz, J. and F. Ragazzi (2010), *Review of Security Measures in the Research Framework Programme*, PE 432.740, October.

Jeandesboz, J. (2008), *An analysis of the Commission communications on future development of FRONTEX and the creation of a European Border Surveillance System*, PE 408.295, Brussels.

Kierkegaard, S., W. Nigel, G. Graham, L. Bygrave, I. Lloyd and S. Saxby (2011), "30 years on - The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Report*, Vol. 27, No. 3, pp. 223-231.

Moerel, L. (2011), "The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *International Data Privacy Law*, Vol. 1, No. 1, pp. 28-46.

Papakonstantinou, V. and P. de Hert (2009), "The PNR Agreement and Transatlantic anti-Terrorism and Co-operation: No Firm Human Rights Framework on either side of the Atlantic", *Common Market Law Review*, Vol. 46, No. 3, pp. 885-919.

Parkin, J. (2011), *The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law*, CEPS Liberty and Security in Europe, CEPS, Brussels, April.

Reding, V. (2010), "Towards a true Single Market of data protection", SPEECH/10/386, Meeting of the Article 29 Data Protection Working Party on the "Review of the Data protection legal framework", Brussels, 14 July (http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386).

———— (2011), "Your data, your rights: Safeguarding your privacy in a connected world", SPEECH/11/183, Privacy Platform "The Review of the EU Data Protection Framework", Brussels, 16 March.

Science and Technology Options Assessment unit (STOA) (ed.) (1999), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, PE 168.184, October.

Surveillance Studies Network (2006), *A Report on the Surveillance Society – For the Information Commissioner by the Surveillance Studies Network*, London, September.

Van Brakel, R. and P. De Hert (2011), "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies", *Journal of Police Studies*, Vol. 20, No. 3.

Voss, A. (2011), *Working Document 1 on a comprehensive approach on personal data protection in the European Union*, PE 460.637, 15.03.2011.

———— (2011), *Working Document 2 on a comprehensive approach on personal data in the European Union*, PE 460.638, 15.03.2011.

Wright, D. (2011), "Should privacy impact assessments be mandatory?", *Communications of ACM*, August.

Official documents

Article 29 Data Protection Working Party (2002), *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, WP 56, Brussels, 30.05.2002.

———— (2010), *Opinion 3/2010 on the principle of accountability*, WP 173, Brussels, 13.07.2010.

———— (2011), *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, WP 180, Brussels, 11.02.2011.

———— (2011), *Opinion 15/2011 on the definition of consent*, WP187, Brussels, 13.07.2011.

Article 29 Data Protection Working Party and Working Party on Police and Justice (2009), *The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168, Brussels, 01.12.2009.

Committee of Experts on New Media (MC-NM) (2010), *Draft Recommendation on the protection of human rights with regard to search engines*, Strasbourg, 11.03.2010.

Committee of Ministers (2010), *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, adopted by the Committee of Ministers on 23 November 2010.

Conference of the Speakers of the Parliaments of the EU (2011), *Presidency Conclusions,* 4-5 April, Brussels.

Council of the European Union (1998), Act of 18 December 1997 drawing up, on the basis of Article K.3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations (98/C 24/01), OJ C24, 23.1.1998.

———— (1999), *Decision of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (1999/468/EC)*, OJ L 184, 17.7.1999.

———— (2000), *Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA),* OJ L 271, 24.10.2000.

———— (2000), *Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention*, OJ L 361, 15.12.2000.

———— (2001), *Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II)*, OJ L 328, 13.12.2001.

———— (2001), *Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II)*, OJ L 328, 13.12.2001, p. 4.

———— (2001), *Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II)*, OJ L 328, 13.12.2001.

———— (2002), *Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)*, OJ L 164, 22.6.2002.

———— (2002), *Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States*, OJ L 190, 18.7.2002.

———— (2004), *Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection*, OJ 2004 L 183, 25.5.2004.

———— (2004), *Decision 2004/512/EC establishing the Visa Information System (VIS) (CNS/2004/0029)*, OJ L 213, 15.6.2004.

———— (2004), *Directive 2004/82/EC of 29 April 2004 on the obligations of carriers to communicate passenger data*, OJ L 261, 6.8.2004.

———— (2004), *Regulation (EC) No 2007/2008 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union*, OJ L 349, 25.11.2004.

———— (2004), *The Hague Programme: Strengthening freedom, security and justice in the European Union*, 16054/04, Brussels, 13.12.2004.

———— (2006), *Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union*, OJ L 386, 29.12.2006.

———— (2007), *Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS)*, OJ L 204, 04.08.2007.

———— (2007), *Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to crime*, OJ L 332, 18.12.2007.

———— (2008), *Decision 2008/615/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*, OJ L 210, 6.8.2008.

———— (2008), *Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, OJ L 218, 13.8.2008.

———— (2008), *Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by EUROPOL for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, OJ L 350, 30.12.2008.

———— (2008), *Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service*, OJ L 213, 8.8.2008.

———— (2008), *Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, OJ L 350, 30.12.2008.

———— (2008), *Note from the Presidency to COREPER on the EU–US Summit, 12 June 2008: Final Report by EU–US High Level Contact Group on information sharing and privacy and personal data protection,* 9831/08, Brussels, 28.5.2008.

———— (2008), *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 12251/08, Brussels, 24.09.2008.

———— (2009), *Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA*, OJ L 93, 7.4.2009.

———— (2009), *Decision of 6 April 2009 establishing the European Police Office (2009/371/JHA)*, OJ L 121, 15.5.2009.

———— (2009), Draft Council Conclusions on an Information Management Strategy for EU internal Security, 16637/09, Brussels, 25.11.2009.

———— (2009), *Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States*, OJ L 93, 7.4.2009.

———— (2009), *Note on the Draft Agreement on SWIFT*, 15671/09, 10.11.2009.

———— (2009), *Proposal for an EU Information Management Strategy for Justice and Home Affairs*, 11312/09, Brussels, 26.6.2009.

———— (2009), *Results of the data collection exercise*, 13267/09, Brussels, 22.9.2009.

———— (2010), *Draft Internal Security Strategy for the European Union: "Towards a European Security Model"*, 5842/2/10, 23.02.2010.

———— (2010), *Final report on cooperation between JHA Agencies*, 8387/10, Brussels, 9.4.2010.

———— (2010), *Interim Report on Cooperation between JHA agencies,* 5816/10, Brussels, 2.2.2010.

———— (2010), *New JHA working structures: Abolition of CIREFI and transfer of its activities to FRONTEX and the Working Party on Frontiers*, Brussels, 6504/10, 22.2.2010.

———— (2010), *Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 8466/10, Brussels, 3.5.2010.

———— (2010), *The Stockholm Programme – An open and secure Europe serving and protecting citizens*, 5731/10, 03.03.2010.

———— (2011), Conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union, 24-25.02.2011.

———— (2011), *EU agency for large-scale IT systems*, 11337/11, 9.6.2011.

———— (2011), *Note from German delegation to delegations on EUROPOL's role in the framework of the EU–US TFTP Agreement and state of play of operational and strategic agreements of EUROPOL – EU information policy on the TFTP Agreement,* 6266/11, Brussels, 8.2.2011.

———— (2011), *Note from the Presidency to the Mixed Committee at the level of Senior Officials on Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice: Possible agreement with the EP*, Brussels, 30.5.2011.

———— (2011), *Note on the Draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record data to the United States Department of Homeland Security*, 10453/11, Brussels, 20.5.2011.

———— (2011), *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Possible agreement with the EP*, 10827/1/11, Brussels, 6.6.2011.

———— (2011), *Strengthening the European external borders agency Frontex – Political agreement between Council and Parliament*, 11916/11, Brussels, 23.6.2011.

European Commission (1972), "The European Community and Data Processing – Government Development Aids Permitted", Information [Competition] 21/72.

———— (1973), *Communication by the Commission of the European Communities concerning a Community policy for data processing: Information Memo P-63/73*, November 1973.

———— (1973), *Communication on Community Policy on Data Processing*, SEC(73) 4300 final, Brussels, 21.11.1973.

———— (1975), *Community Policy for Data-processing*, COM(75) 467 final, Brussels.

———— (1981), *Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data*, OJ L 246, 29.8.1981.

———— (2000), *Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441*, OJ L 215, 25.8.2000.

———— (2004), *Annex to the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas – Extended Impact Assessment*, SEC(2004) 1628 final, Brussels, 28.12.2004.

———— (2004), *Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under document number C(2004) 1914)*, OJ L 235 , 06.07.2004.

———— (2005), *Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597, Brussels, 24.11.2005.

———— (2005), *Compliance with the Charter of Fundamental Rights in Commission legislative proposals*, COM(2005) 172 final, Brussels, 27.4.2005.

———— (2005), *Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*, COM(2005) 230 final, Brussels, 31.05.2005.

———— (2005), *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, COM(2005) 475 final, Brussels, 04.10.2005.

———— (2005), *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II)*, COM(2005) 236 final/2, Brussels, 23.08.2005.

———— (2007), *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, Brussels, 6.11.2007.

———— (2008), *Examining the creation of a European Border Surveillance System*, COM(2008) 68 final, 13.12.2008.

———— (2008), *Examining the creation of a European Border Surveillance System*, SEC(2008) 151, Commission Staff Document, Brussels.

———— (2008), *Preparing the next steps in border management in the European Union*, COM(2008) 69 final, Brussels, 13.2.2008.

———— (2008), *Preparing the next steps in border management in the European Union – Summary of the impact assessment*, SEC(2008) 153 final, Brussels, 13.2.2008.

———— (2008), *Report on the evaluation and future development of the FRONTEX agency*, COM(2008) 67 final, Brussels, 13.2.2008.

———— (2009), *Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen*, COM(2009) 262 final, Brussels, 10.06.2009.

———— (2009), *Impact Assessment Guidelines*, SEC(2009) 92 final, Brussels, 15.1.2009.

———— (2009), *Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty*, COM(2009) 294 final, Brussels, 24.6.2009.

———— (2009), *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, COM(2009) 293 final, Brussels, 24.6.2009.

———— (2009), *Report on progress made in developing the European Border Surveillance System*, SEC(2009) 1265 final, Brussels, 24.9.2009.

———— (2010), Communication from the Commission on the global approach to transfers of Passengers Name Record (PNR) data to third countries, COM(2010) 492 final, Brussels, 21.9.2010.

———— (2010), *Communication on the overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, Brussels, 20.7.2010.

———— (2010), *Communication on the procedures for the scrutiny of EUROPOL's activities by the European Parliament, together with national Parliaments*, COM(2010) 776, Brussels, 17.12.2010.

———— (2010), *Communication on the Use of Security Scanners at EU airports*, Brussels, 15.6.2010.

———— (2010), *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Delivering an area of freedom, security and justice for Europe's citizens: Action Plan Implementing the Stockholm Programme*, COM(2010) 171 final, Brussels, 20.4.2010.

———— (2010), *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 4.11.2010.

———— (2010), *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, Final Report, Brussels, 20.1.2010.

———— (2010), *Delivering an Area of Freedom, Security and Justice for Europe's citizens: Action Plan Implementing the Stockholm Programme*, COM(2010) 171 final, Brussels, 20.4.2010.

———— (2010), *Impact Assessment accompanying the Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, SEC(2010) 149 final, Brussels, 24.2.2010.

———— (2010), *Proposal for a Council Decision on the signature of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, COM(2010) 317 final, Brussels, 15.06.2010.

———— (2010), *Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency*

for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, COM(2010) 61 final, Brussels, 24.2.2010.

——— (2010), *Proposal for a review of the Directive 2006/24/EC (Data Retention)*, DG Home, Brussels, September.

——— (2010), *Roadmap - Initiatives on Smart Borders: Legislative Proposal to set up Registered Traveller Programme (RTP)*, 2010/JLS/03, Brussels.

——— (2010), *Roadmap – European Terrorist Financing Tracking Programme (European TFTP)*, DG Home, Brussels, October.

——— (2010), *Roadmap – Legislative proposal on the establishment of a European Border Surveillance System (EUROSUR)*, DG Home, Brussels, October.

——— (2010), *Roadmap – Legislative proposal to set up Entry/Exit System (EES)*, 2010/JLS/04, Brussels.

——— (2010), *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*, COM(2010) 573 final, Brussels, 19.10.2010.

——— (2010), *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM(2010) 673 final, Brussels, 22.11.2010.

——— (2010), *The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens*, OJ C 115, 4.5.2010.

——— (2011), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European terrorist finance tracking system: available options*, COM(2011) 429 final, Brussels, 13.07.2011.

——— (2011), *Communication on a comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, 4.11.2011.

——— (2011), *Determining the technical and operational framework of the European Border Surveillance System (EUROSUR) and the actions to be taken for its establishment*, SEC(2011) 145, Brussels, 28.1.2011.

——— (2011), *Evaluation Report on the Data Retention Directive*, COM(2011) 225 final, Brussels, 18.4.2011.

——— (2011), *Note for the attention of Stefano Manservisi, Director General, DG Home*, Document SJ.1(2011) 603245, Legal Service, Brussels, 18 May (Statewatch: http://www.statewatch.org/news/2011/jun/03eu-us-pnr-com-ls.htm).

——— (2011), *Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments*, Commission Staff Working Paper, SEC(2011) 567 final, Brussels, 6.5.2011.

——— (2011), *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, Brussels, 2.2.2011.

——— (2011), *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM(2011) 225, Brussels, 18.4.2011.

——— (2011), *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, Brussels, 16.03.2011.

European Council (2010), *Internal Security Strategy for the European Union: Towards a European security model*, adopted by the Justice and Home Affairs Council on 25 and 26 February 2010, and approved by the European Council on 25 and 26 March 2010.

European Data Protection Supervisor (2006), *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final)*, OJ C 91, 19.4.2006.

——— (2008), Preliminary Comments on COM(2008) 69 final, COM(2008) 68 final, COM(2008) 67 final, March.

——— (2010), *EDPS' comments on Amendment 59 in the Draft report on the Proposal for a Regulation of The European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)(COM(2010)0061 – C7-0045/2010-2010/0039(COD))*, Brussels, 3 December.

——— (2010), *Letter from the European Data Protection Supervisor, Peter Hustinx, to the Chairman of the Committee on Civil Liberties, Justice and Home Affairs, Juan Fernando López Aguilar*, Brussels, 25 January.

———(2010), *Monitoring and Ensuring Compliance with Regulation (EC) 45/2001* Policy Paper, 13 December.

——— (2010), *Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Personal Name Record (PNR) data to third countries*, Brussels, 16 October, pp. 3-4.

——— (2010), *Opinion on a Notification for Prior Checking received from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) concerning the "Collection of names and certain other relevant data of returnees for joint operations (JRO)"*, Brussels, 26 April.

———(2010), *Opinion on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union*, Brussels, 17 May.

——— (2010), *Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II)*, Brussels, 22 June.

——— (2011), *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, Brussels, 31 May.

——— (2011), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union*, Brussels, 14 January.

——————— (2011), *Opinion on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union"*, 14 January.

European Ombudsman (2001), *Note on Openness and Data Protection*, Strasbourg, 14 November.

European Parliament and Council of the European Union (1998), *Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*, OJ L 24, 30.1.1998.

——————— (2001), *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, OJ L 8, 12.1.2001.

——————— (2002), *Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, OJ L 201, 31.7.2002.

——————— (2005), *Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*, OJ L 309, 25.11.2005.

——————— (2006), *Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, OJ L 105, 13.4.2006.

——————— (2006), *Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, OJ L 381, 28.12.2006.

European Parliament (1975), *Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, OJ C 60, 13.3.1975.

——————— (1976), *Resolution of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing,* OJ C 100, 3.5.76.

——————— (1979), *Resolution on the protection of the rights of the individual in the face of technical developments in data processing*, OJ C 140, 5.6.1979.

——————— (1982), *Resolution of 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing*, OJ C 87, 5.4.82.

——————— (1994), *Resolution of 15 December 1993 on relations between the Union and the Council of Europe*, OJ No C 20, 24.01.94.

——————— (1994), *Resolution of 18 January 1994 on Community accession to the European Convention on Human Rights*, OJ C 44, 14.02.94.

——————— (1998), *Annual Report of 2 December 1998 on respect for human rights in the European Union*, PE 228.192/fin.

——————— (2000), *Report of 8 October 2000 of the Committee on Constitutional Affairs on the impact of the Charter of Fundamental Rights of the European Union and its future status* (2002/2139(INI)), PE 313.401.

——————— (2000), *Resolution of 16 March 2000 on respect for human rights in the European Union (1998-1999) (11350/1999 – C5-0265/1999 – 1999/2001(INI))*, A5-0050/2000, § 7(a).

——————— (2000), *Resolution of 16 September 1999 on the establishment of the Charter of Fundamental Rights*, OJ C 54, 25.2.2000.

———— (2000), *Resolution of 5 July 2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related frequently asked questions issued by the US Department of Commerce (C5-0280/2000 – 2000/2144(COS))*, A5-0177/2000, OJ C 121/152, 25.8.2000.

———— (2001), *Legislative Resolution of 14 November 2000 on the proposal for a European Parliament and Council regulation on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (COM(1999) 337 - C5-0149/1999 - 1999/0153(COD))*, OJ C 223, 8.8.2001.

———— (2001), *Opinion of the LIBE Committee for the Committee on Transport and Tourism on aviation security with a special focus on security scanners (2010/2154(INI))*, Rapporteur: Judith Sargentini, 27.04.2001.

———— (2001), *Resolution of 5 September 2001 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)).*

———— (2003), *Recommendation to the Council of 20 November 2003 on the second-generation Schengen information system (SIS II)*, P5_TA(2003)0509.

———— (2003), *Resolution of 23 October 2002 on the impact of the Charter of Fundamental Rights of the European Union and its future status (2002/2139(INI))*, C 300 E/432, 11.12.2003.

———— (2003), *Resolution of 27 March 2003 on progress in 2002 in implementing an area of Freedom, Security and Justice (Articles 2 and 39 of the EU Treaty)*, P5_TA(2003)0126.

———— (2004), *Resolution of 31 March 2004 on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection, (2004/2011(INI))*, P5_TA(2004)0245.

———— (2004), *Resolution of 9 March 2004 on the First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI))*, P5_TA(2004)0141.

———— (2005), *Legislative Resolution of 14 December 2005 on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))*, P6_TA(2005)0512.

———— (2005), *Legislative Resolution of 27 September 2005 on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 – C6-0198/2004 – 2004/0813(CNS))*, P6_TA(2005)0348.

———— (2005), *Minority Opinion pursuant to Rule 48(3) of the Rules of Procedure*, by Giusto Catania, Ole Krarup, Sylvia-Yvonne Kaufmann and Kathalijne Maria Buitenweg, 28.11.2005.

———— (2005), *Report of 28 November 2005 on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)), Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Alexander Nuno Alvaro).

———— (2005), *Report of 31 May 2005 on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism* (8958/2004 – C6-0198/2004 – 2004/0813(CNS)), Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Alexander Nuno Alvaro), PE 357.618v03-00.

———— (2005), *Resolution of 26 May 2005 on promotion and protection of fundamental rights: the role of national and European institutions, including the Fundamental Rights Agency (2005/2007(INI))*, P6_TA(2005)0208.

———— (2006), *Legislative Resolution of 25 October 2006 on the proposal for a Council decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*, P6_TA(2006)0447.

———— (2006), *Legislative Resolution of 27 September 2006 on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM(2005)0475 – C6-0436/2005 – 2005/0202(CNS))*, P6_TA(2006)0370.

———— (2006), *Proposal for a Recommendation to the Council of 8 June 2006, by Alexander Alvaro, on behalf of the ALDE Group on interoperability and synergies among European databases in the area of justice and home affairs*, PE 374.607v01-00.

———— (2006), *Recommendation to the Council of 14 December 2006 on the progress of the negotiations on the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2006/2286(INI))*, P6_TA(2006)0602.

———— (2006), *Resolution of 6 July 2006 on the interception of bank transfer data from the SWIFT system by the US secret services*, P6_TA(2006)0317.

———— (2006), *Resolution on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS*), OJ 157, 6.7.2006.

———— (2007), *Legislative Resolution of 7 June 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (renewed consultation) (7315/2007 – C6-0115/2007 – 2005/0202(CNS))*, P6_TA(2007)0230.

———— (2007), *Legislative Resolution of 7 June 2007 on the proposal for a Council decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by EUROPOL for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*.

———— (2007), *Recommendation to the Council of 7 September 2007 on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime (2006/2193(INI))*, P6_TA(2006)0354.

———— (2007), *Resolution of 12 July 2007 on the PNR agreement with the United States of America*, P6_TA(2007)0347.

———— (2007), *Resolution of 14 February 2007 on SWIFT, the PNR agreement and the transatlantic dialogue on these issues*, P6_TA(2007)0039.

———— (2007), *Resolution of 25 April 2007 on transatlantic relations,* P6_TA(2007)0155.

———— (2008), *Legislative Resolution of 2 September 2008 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code (COM(2008)0101 – C6-0086/2008 – 2008/0041(COD))*, P6_TA(2008)0383.

———— (2008), *Legislative Resolution of 23 September 2008 on the Draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (16069/2007 – C6-0010/2008 – 2005/0202(CNS))*, P6_TA(2008)0436.

———— (2008), *Legislative Resolution of 24 September 2008 on the draft Council decision on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (12059/1/2008 – C6-0188/2008 – 2008/0077(CNS))*, P6_TA(2008)0441.

———— (2008), *Recommendation of 22 October 2008 to the Council on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service*, P6_TA(2008)0512.

———— (2008), *Resolution of 18 December 2008 on the evaluation and future development of the FRONTEX Agency and of the European Border Surveillance System (EUROSUR) (2008/2157(INI))*, P6_TA(2008)0633.

———— (2008), *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, P6_TA(2008)0561.

———— (2008), *Resolution of Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection*, P6_TA(2008)0521.

———— (2009), *Resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing*, P7_TA(2009)0016.

———— (2009), *Resolution of 22 October 2009 on progress of Schengen Information System II and Visa Information System*, P7_TA(2009)0055.

———— (2009), *Resolution of 22 October 2009 on the upcoming EU–US Summit and the Transatlantic Economic Council Meeting*, P7_TA(2009)0058.

———— (2009), *Resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme*, P7_TA(2009)0090.

———— (2010), *Legislative Resolution of 11 February 2010 on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, P7_TA(2010)0029.

———— (2010), *Legislative Resolution of 8 July 2010 on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE))*, P7_TA(2010)0279.

———— (2010), *Recommendation of 5 July on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the*

European Union to the United States for the purposes of the Terrorist Finance Tracking Program (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE)), Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Alexander Alvaro), A7-0224/2010, 5.7.2010.

———— (2010), *Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI))*, OJ C 184 E, 8.7.2010.

———— (2010), *Resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council to authorise the opening of negotiations between the European Union and Australia, Canada and the United States*, P7_TA(2010)0397.

———— (2010), *Resolution of 15 December 2010 on the impact of advertising on consumer behaviour (2010/2052(INI))*, P7_TA(2010)0484.

———— (2010), *Resolution of 15 December 2010 on the situation of fundamental rights in the European Union – effective implementation after the entry into force of the Treaty of Lisbon*, 15 December, Strasbourg, P7_TA(2010)0483.

———— (2010), *Resolution of 15 June 2010 on the Internet of Things (IoT)*, P7_TA(2010)0207.

———— (2010), *Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada*, P7_TA(2010)0144.

———— (2010), *Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing*, P7_TA(2010)0143.

———— (2011), *Committee on Transport and Tourism, Report of 1 June 2011 on aviation security, with a special focus on security scanners* (2010/2154(INI)), Rapporteur: Luis de Grandes Pascual, A7-0216/2011.

———— (2011), *Draft report of Simon Busuttil (PE450.754v01-00) on the proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 2010/0039(COD), Amendment 59, 6.7.2011.

———— (2011), *Legislative Resolution of 5 July 2011 on the amended proposal for a regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (COM(2010)0093 – C7-0046/2009 – 2009/0089(COD))*, P7_TA(2011)0304.

———— (2011), *Legislative Resolution of 6 July 2011 on the Council position at first reading with a view to the adoption of a directive of the European Parliament and of the Council facilitating the cross-border exchange of information on road safety related traffic offences (17506/1/2010 – C7-0074/2011 – 2008/0062(COD)*, P7_TA(2011)0325).

———— (2011), *Report on a comprehensive approach on personal data protection in the European Union* (2011/2025(INI), A7-0244/2011, 22.6.2011.

———— (2011), *Resolution of 6 July 2011 on aviation security, with a special focus on security scanners (2010/2154(INI))*, P7_TA(2011)0329.

———— (2011), *Resolution of 8 June 2011 on the mid-term review of the Seventh Framework Programme of the European Union for research, technological development and demonstration activities (2011/2043(INI))*, P7_TA(2011)0256,

———— (2011), *Resolution of Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI))*, P7_TA(2011)0323.

———— (2011), *Resolution of Resolution of 6 July 2011 on the Commission Work Programme 2012*, P7_TA(2011)0327.

European Union Agency for Fundamental Rights (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, Vienna, 28 October.

———— (2011), *Opinion on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)*, Vienna, 14 June.

EUROPOL Joint Supervisory Body (2011), *Report on the inspection of EUROPOL's implementation of the TFTP agreement*, conducted in November 2010, JSB EUROPOL inspection report 11-07, Brussels, 1 March.

FRONTEX (2007), *General Report for 2007*, FRONTEX, Warsaw (http://www.frontex.europa.eu/gfx/frontex/files/justyna/frontex_general_report_2007_final.pdf).

House of Lords European Union Committee (2008), *FRONTEX: The EU external borders agency – Report with evidence*, 9th Report of Session 2007-2008, HL Paper 60, London, 5 March.

Legal Service of the European Parliament (2010), *Legal opinion on SWIFT (Conclusion of EU/US TFTP Agreement)*, 02.02.2010.

Temporary Committee on the ECHELON Interception System (2011), *Report of 11 July 2011 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)*, Explanatory Statement, § 8(2).

Working Party on General Matters including Evaluation (GENVAL) (2011), *Summary of discussion on 11 May 2011*, Brussels, 14 June.

Agreements, conventions and declarations

Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82, 21.03.2006.

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010.

Conference of European Data Protection Authorities, Declaration on three communications from the Commission on border management, Rome, 18 April 2008.

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000.

Declaration of Brussels, adopted on 1 October 2010 by the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the Member States of the European Union.

Joint Declaration by the European Parliament, Council and the Commission concerning the protection of fundamental rights and the ECHR, Luxembourg, 5 April 1977, OJ C 103, 27.04.1977.

Joint Review Team (2011), EU/USA Agreement: Processing and transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Program: the report relating to the joint review of the implementation of the agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

Case law

Court of Justice of the European Union, Case C-301/06, *Ireland v. European Parliament and Council of the European Union,* 10 February 2009

Court of Justice of the European Union, Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union and Commission of the European Communities*, 30 May 2006

Court of Justice of the European Union, C-92/09 and C-93/09, *Volker und Markus Schecke* and *Eifert*, 9 November 2010

Court of Justice of the European Union, Case C-28/08 P, *Commission v. Bavarian Lager*, 29 June 2010

Court of Justice of the European Union, Case T-529/09, *In't Veld v. Council,* 31 December 2009

European Court of Human Rights, *Antony & Margaret McMichael v. UK*, 24 February 1995, application no. 16424/90;

European Court of Human Rights, *Gaskin .v UK*, 10454/83, 7 July 1989, application No. 10454/83

European Court of Human Rights, *Guerra et al. v. Italy*, 19 February 1998, application no. 14967/89;

European Court of Human Rights, *K.U. v. Finland*, 2 December 2008, application no. 2872/02

European Court of Human Rights, *Klass v. Germany*, 06 September 1978, application no. 5029/71

European Court of Human Rights, *Leander v. Sweden*, 26 March 1987, application no. 9248/81

European Court of Human Rights, *Liberty and others v. the United Kingdom*, 1 July 2008, Application no. 58243/00

European Court of Human Rights, *McGinley & Egan v. UK*, 09 June 1998, application no. 21825/93 and 23414/94

European Court of Human Rights, *P.G. & J.H. v UK*, 25 September 2001, application no. 44787/98

European Court of Human Rights, *Peck v. UK*, 28 January 2003, application no. 44647/98

European Court of Human Rights, *Perry v. UK*, 17 July 2003, application no. 63737/00

European Court of Human Rights, *Rotaru v. Romania*, 04, May 2000, application no. 28341/95

European Court of Human Rights, *S & Marper v. UK*, 4 December 2008, application n. 30562/04 and 30566/04

European Court of Human Rights, *Shimovolos v. Russia*, 21 June 2011, application no. 30194/09

European Court of Human Rights, *Z. v. Finland*, 25 February 1997, application no. 22009/93

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

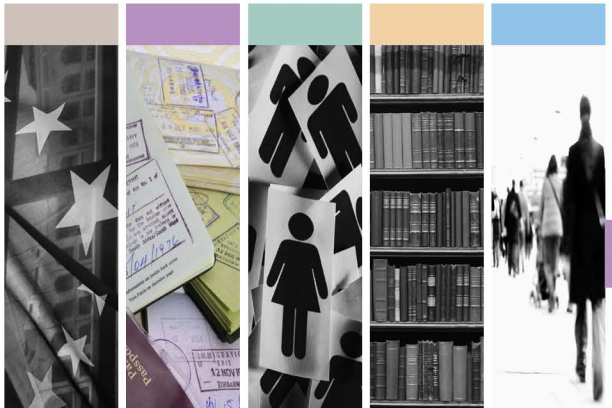
Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**



ISBN