ECLI:EU:C:2022:703

Provisional text

JUDGMENT OF THE COURT (Grand Chamber)

20 September 2022 (*)

(References for a preliminary ruling – Single Market for financial services – Market abuse – Insider dealing – Directive 2003/6/EC – Article 12(2)(a) and (d) – Regulation (EU) No 596/2014 – Article 23(2)(g) and (h) – Supervisory and investigatory powers of the Autorité des marchés financiers (AMF) – General interest objective seeking to protect the integrity of financial markets in the European Union and public confidence in financial instruments – Option open to the AMF to require the traffic data records held by an operator providing electronic communications services – Processing of personal data in the electronic communications sector – Directive 2002/58/EC – Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Confidentiality of communications – Restrictions – Legislation providing for the general and indiscriminate retention of traffic data by operators providing electronic communications services – Option for a national court to restrict the temporal effects of a declaration of invalidity in respect of provisions of national law that are incompatible with EU law – Precluded)

In Joined Cases C-339/20 and C-397/20,

REQUESTS for a preliminary ruling under Article 267 TFEU from the Cour de cassation (Court of Cassation, France), made by decisions of 1 April 2020, received at the Court on 24 July 2020 and 20 August 2020 respectively, in the criminal proceedings against

**VD** (C-339/20),

**SR** (C-397/20),

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis and I. Ziemele, Presidents of Chambers, T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (Rapporteur), N. Piçarra, L.S. Rossi and A. Kumin, Judges,

Advocate General: M. Campos Sánchez-Bordona,

Registrar: R. Șereș, Administrator,

having regard to the written procedure and further to the hearing on 14 September 2021,

after considering the observations submitted on behalf of:

– VD, by D. Foussard and F. Peltier, avocats,

– SR, by M. Chavannes and P. Spinosi, avocats,

– the French Government, by A. Daniel, E. de Moustier, D. Dubois, J. Illouz and T. Stéhelin, acting as Agents,

– the Danish Government, by N. Holst-Christensen, N. Lykkegaard and M. Søndahl Wolff, acting as Agents,

– the Estonian Government, by A. Kalbus and M. Kriisa, acting as Agents,

– Ireland, by M. Browne, A. Joyce and J. Quaney, acting as Agents, and by D. Fennelly, Barrister-at-Law,

– the Spanish Government, by L. Aguilera Ruiz, acting as Agent,

– the Polish Government, by B. Majczyna, acting as Agent,

– the Portuguese Government, by P. Barros da Costa, L. Inez Fernandes, L. Medeiros and I. Oliveira, acting as Agents,

– the European Commission, by S.L. Kalėda, H. Kranenborg, T. Scharf and F. Wilman, acting as Agents,

– the European Data Protection Supervisor, by A. Buchta, M. Guglielmetti, C.-A. Mamier and D. Nardi, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 18 November 2021,

gives the following

**Judgment**

1 These requests for a preliminary ruling concern, in essence, the interpretation of Article 12(2)(a) and (d) of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) (OJ 2003 L 96, p. 16) and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (OJ 2014 L 173, p. 1), read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council 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 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), and read in the light of Articles 7, 8 and 11 and of Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’).

2 The requests have been made in the context of criminal proceedings brought against VD and SR in respect of insider dealing, concealment of insider dealing, aiding and abetting, corruption and money laundering.

## Legal context

### *European Union law*

*Directive 2002/58*

3 Recitals 2, 6, 7 and 11 of Directive 2002/58 state:

‘(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the [Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

…

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

…

(11) Like Directive [95/46/EC of the European Parliament and of the 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 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.’

4 Article 1 of Directive 2002/58, headed ‘Scope and aim’, provides:

‘1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to

privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the [FEU Treaty], such as those covered by Titles V and VI [of the EU Treaty], and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

5 Article 2 of that directive, headed 'Definitions', provides in point (b) of the second paragraph:

'The following definitions shall … apply:

…

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.

6 Article 5 of the directive, headed 'Confidentiality of the communications', provides:

'1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'

7 Article 6 of Directive 2002/58, headed 'Traffic data', provides:

'1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or

made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

…

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

…'

8 Article 9 of that directive, headed 'Location data other than traffic data', provides, in paragraph 1 thereof:

'1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …'

9 Article 15 of Directive 2002/58, headed 'Application of certain provisions of Directive [95/46]', provides, in paragraph 1 thereof:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].'

*Directive 2003/6*

10 Recitals 1, 2, 12, 37, 41 and 44 of Directive 2003/6 are worded as follows:

‘(1) A genuine Single Market for financial services is crucial for economic growth and job creation in the Community.

(2) An integrated and efficient financial market requires market integrity. The smooth functioning of securities markets and public confidence in markets are prerequisites for economic growth and wealth. Market abuse harms the integrity of financial markets and public confidence in securities and derivatives.

…

(12) Market abuse consists of insider dealing and market manipulation. The objective of legislation against insider dealing is the same as that of legislation against market manipulation: to ensure the integrity of Community financial markets and to enhance investor confidence in those markets. …

…

(37) A common minimum set of effective tools and powers for the competent authority of each Member State will guarantee supervisory effectiveness. Market undertakings and all economic actors should also contribute at their level to market integrity. …

…

(41) Since the objective of the proposed action, namely to prevent market abuse in the form of insider dealing and market manipulation, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the measures, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 [TEU]. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(44) This Directive respects the fundamental rights and observes the principles recognised in particular by [the Charter] and in particular by Article 11 thereof and Article 10 of the European Convention [for the Protection of] Human Rights [and Fundamental Freedoms]. …’

11 Article 11 of that directive provides:

‘Without prejudice to the competences of the judicial authorities, each Member State shall designate a single administrative authority competent to ensure that the provisions adopted pursuant to this Directive are applied.

…’

12 Article 12 of that directive provides:

‘1. The competent authority shall be given all supervisory and investigatory powers that are necessary for the exercise of its functions. …

2. Without prejudice to Article 6(7), the powers referred to in paragraph 1 of this Article shall be exercised in conformity with national law and shall include at least the right to:

(a) have access to any document in any form whatsoever, and to receive a copy of it;

…

(d) require existing telephone and existing data traffic records;

…’

*Regulation No 596/2014*

13 Regulation No 596/2014 repealed and replaced Directive 2003/6 with effect from 3 July 2016.

14 Recitals 1, 2, 7, 24, 44, 62, 65, 66, 77 and 86 of that regulation are worded as follows:

‘(1) A genuine internal market for financial services is crucial for economic growth and job creation in the Union.

(2) An integrated, efficient and transparent financial market requires market integrity. The smooth functioning of securities markets and public confidence in markets are prerequisites for economic growth and wealth. Market abuse harms the integrity of financial markets and public confidence in securities and derivatives.

…

(7) Market abuse is a concept that encompasses unlawful behaviour in the financial markets and, for the purposes of this Regulation, it should be understood to consist of insider dealing, unlawful disclosure of inside information and market manipulation. Such behaviour prevents full and proper market transparency, which is a prerequisite for trading for all economic actors in integrated financial markets.

…

(24) Where a legal or natural person in possession of inside information acquires or disposes of, or attempts to acquire or dispose of, for his own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates, it should be implied that that person has used that information. That presumption is without prejudice to the rights of the defence. The question whether a person has infringed the prohibition on insider dealing or has attempted to commit insider dealing should be analysed in the light of the purpose of this Regulation, which is to protect the integrity of the financial market and to enhance investor confidence, which is based, in turn, on the assurance that investors will be placed on an equal footing and protected from the misuse of inside information.

…

(44) Many financial instruments are priced by reference to benchmarks. The actual or attempted manipulation of benchmarks, including interbank offer rates, can have a serious impact on market confidence and may result in significant losses to investors or distort the real economy. …

…

(62) A set of effective tools and powers and resources for the competent authority of each Member State guarantees supervisory effectiveness. Accordingly, this Regulation, in particular, provides for a minimum set of supervisory and investigative powers competent authorities of Member States should be entrusted with under national law. Those powers should be exercised, where the national law so requires, by application to the competent judicial authorities. …

…

(65) Existing recordings of telephone conversations and data traffic records from investment firms, credit institutions and financial institutions executing and documenting the execution of transactions, as well as existing telephone and data traffic records from telecommunications operators, constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation. Telephone and data traffic records may establish the identity of a person responsible for the dissemination of false or misleading information or that persons have been in contact at a certain time, and that a relationship exists between two or more people. Therefore, competent authorities should be able to require existing recordings of telephone conversations, electronic communications and data traffic records held by an investment firm, a credit institution or a financial institution in accordance with Directive 2014/65/EU [of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ 2014 L 173, p. 349)]. Access to data and telephone records is necessary to provide evidence and investigate leads on possible insider dealing or market manipulation, and therefore for detecting and imposing sanctions for market abuse. In order to introduce a level playing field in the Union in relation to the access to telephone and existing data traffic records held by a telecommunications operator or the existing recordings of telephone conversations and data traffic held by an investment firm, a credit institution or a financial institution, competent authorities should, in accordance with national law, be able to require existing telephone and existing data traffic records held by a telecommunications operator, in so far as permitted under national law and existing recordings of telephone conversations as well as data traffic held by an investment firm, in cases where a reasonable suspicion exists that such records related to the subject matter of the inspection or investigation may be relevant to prove insider dealing or market manipulation infringing this Regulation. Access to telephone and data traffic records held by a telecommunications operator does not encompass access to the content of voice communications by telephone.

(66) While this Regulation specifies a minimum set of powers competent authorities should have, those powers are to be exercised within a complete system of national law which guarantees the respect for fundamental rights, including the right to privacy. For the exercise of those powers, which may amount to serious interferences with the right to respect for private and family life, home and communications, Member States should have in place adequate and effective safeguards against any abuse, for instance, where appropriate a requirement to obtain prior authorisation from the judicial authorities of a Member State concerned. Member States should allow the possibility for competent authorities to exercise such intrusive powers to the extent necessary for the proper investigation of serious cases where there are no equivalent means for effectively achieving the same result.

…

(77) This Regulation respects the fundamental rights and observes the principles recognised in the [Charter]. Accordingly, this Regulation should be interpreted and applied in accordance with those rights and principles. …

…

(86) Since the objective of this Regulation, namely to prevent market abuse in the form of insider dealing, the unlawful disclosure of inside information and market manipulation, cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 [TEU]. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.'

15 Under Article 1 of that regulation:

'This Regulation establishes a common regulatory framework on insider dealing, the unlawful disclosure of inside information and market manipulation (market abuse) as well as measures to prevent market abuse to ensure the integrity of financial markets in the Union and to enhance investor protection and confidence in those markets.'

16 Under the heading 'Definitions', Article 3 of that regulation provides, in subparagraph (1) (27):

'For the purposes of this Regulation, the following definitions apply:

…

(27) "data traffic records" means records of traffic data as defined in point (b) of the second paragraph of Article 2 of Directive [2002/58];'

17 Under Article 14 of Regulation No 596/2014, headed 'Prohibition of insider dealing and of unlawful disclosure of inside information':

'A person shall not:

(a) engage or attempt to engage in insider dealing;

(b) recommend that another person engage in insider dealing or induce another person to engage in insider dealing; or

(c) unlawfully disclose inside information.'

18 Article 22 of that regulation provides:

'Without prejudice to the competences of the judicial authorities, each Member State shall designate a single administrative competent authority for the purpose of this Regulation. …'

19 Article 23 of that regulation, headed 'Powers of competent authorities', provides in paragraphs 2 and 3 thereof:

'2. In order to fulfil their duties under this Regulation, competent authorities shall have, in accordance with national law, at least the following supervisory and investigatory powers:

(a) to access any document and data in any form, and to receive or take a copy thereof;

…

(g) to require existing recordings of telephone conversations, electronic communications or data traffic records held by investment firms, credit institutions or financial institutions;

(h) to require, in so far as permitted by national law, existing data traffic records held by a telecommunications operator, where there is a reasonable suspicion of an infringement and where such records may be relevant to the investigation of an infringement of point (a) or (b) of Article 14 or Article 15;

…

3. Member States shall ensure that appropriate measures are in place so that competent authorities have all the supervisory and investigatory powers that are necessary to fulfil their duties.

…'

***French law***

*The CPCE*

20 Article L. 34-1 of the Code des postes et des communications électroniques (Post and Electronic Communications Code), in the version applicable to the disputes in the main proceedings ('the CPCE'), provided:

'I. – This Article shall apply to the processing of personal data in the course of the provision to the public of electronic communications services; it shall apply in particular to networks that support data collection and identification devices.

II. – Electronic communications operators, in particular persons whose business is to provide access to online public communication services, shall erase or render anonymous any data relating to traffic, subject to the provisions contained in points III, IV, V and VI.

Persons who provide electronic communications services to the public shall, with due regard for the provisions contained in the preceding paragraph, establish internal procedures for responding to requests from the competent authorities.

Persons who, as a principal or ancillary business activity, provide to the public a connection allowing online communication via access to the network shall, including where this is offered free of charge, be subject to compliance with the provisions applicable to electronic communications operators under this Article.

III. – For the purposes of investigating, detecting and prosecuting criminal offences or a failure to fulfil an obligation laid down in Article L. 336-3 of the code de la propriété intellectuelle (Intellectual Property Code) or for the purposes of preventing breaches of automated data processing systems as provided for and punishable under Articles 323-1 to 323-3-1 of the Code pénal (Criminal Code), and for the sole purpose of making information available, as necessary, to the judicial authority or high authority mentioned in Article L. 331-12 of the Intellectual Property Code or to the national authority for the security of information systems mentioned in Article L. 2321-1 of the code de la défense (Defence Code), operations designed to erase or render anonymous certain categories of technical data may be deferred for a maximum period of one year.

A decree to be adopted following consultation of the Conseil d'État (Council of State, France) and the Data Protection Authority shall, within the limits laid down in point VI, determine the categories of data involved and the period for which they are to be retained, depending on the business of the operators, the nature of the communications and the methods of offsetting any identifiable and specific additional costs associated with the services provided for these purposes by operators at the request of the State.

…

VI. – Data retained and processed under the conditions set out in points III, IV and V shall relate exclusively to the identification of persons using the services provided by operators, the technical characteristics of the communications provided by the latter and the location of terminal equipment.

Under no circumstance may such data relate to the content of the correspondence or the information consulted, in any form whatsoever, as part of those communications.

The retention and processing of such data shall be effected with due regard for the provisions of loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Law No 78-17 of 6 January 1978 on information technology, files and freedoms).

Operators shall take any measures necessary to prevent such data from being used for purposes other than those provided for in this Article.'

21 Article L. 34-1 of the Post and Electronic Communications Code, in the version resulting from loi nº 2021-998, du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement (Law No 2021-998 of 30 July 2021 on the prevention of terrorist acts and information) (JORF of 31 July 2021, text No 1), provides in points II bis to III bis:

'II bis – Electronic communications operators shall retain:

1. For the purposes of criminal proceedings, the prevention of threats to public security and the safeguarding of national security, information on the user's civil identity for a period of five years from the end of the term of his or her contract;

2. For the same purposes as those set out in point II bis(1), the other information provided by the user when entering into a contract or setting up an account and the payment information, for a period of one year from the end of the term of his or her contract or of the closure of his or her account;

3. For the purposes of combating crime and serious crime, the prevention of serious threats to public security and the safeguarding of national security, technical data that make it possible to identify the source of the connection or data relating to the terminal equipment used, for a period of one year from the connection or use of terminal equipment.

III. – For reasons relating to the safeguarding of national security, where there is a serious, present or foreseeable threat to national security, the Prime Minister may, by decree, order electronic communication operators to retain for a period of one year certain categories of traffic data, in addition to the data referred to in point II bis(3), and location data specified by a decree to be adopted after consultation of the Conseil d'État (Council of State).

The Prime Minister's order, which may be applicable for up to one year, may be renewed if the conditions laid down for its enactment continue to be met. Its expiry shall have no effect on the data retention period referred to in the first paragraph of this point III.

III bis – Data retained by operators under this Article may be subject to an expedited retention order issued by the authorities having access, under the law, to electronic communications data for the purposes of preventing and punishing crime, serious crime and other serious breaches of rules the observance of which they are responsible for ensuring, in order that those authorities may access those data.'

22 Article R. 10-13 of the CPCE is worded as follows:

'I. – Pursuant to point III of Article L. 34-1, electronic communications operators shall retain the following data for the purposes of investigating, detecting and prosecuting criminal offences:

(a) information identifying the user;

(b) data relating to the communications terminal equipment used;

(c) the technical characteristics and date, time and duration of each communication;

(d) data relating to the additional services requested or used and the providers of those services;

(e) data identifying the addressee or addressees of the communication.

II. – In the case of telephony activities, the operator shall retain the data referred to in point II and, additionally, data enabling the origin and location of the communication to be identified.

III. – The data referred to in this Article shall be retained for one year from the date of registration.

…'

*The LCEN*

23 Article 6 of Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy) (JORF of 22 June 2004, p. 11168), in the version applicable to the disputes in the main proceedings ('the LCEN') provided:

'I – 1. Persons whose business is to provide access to online public communication services shall inform their subscribers of the existence of technical tools enabling access to some services to be restricted or for a selection of those services to be made and shall offer them at least one of those tools.

…

2. Natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services, may not incur any civil liability for the activities or information stored at the request of a recipient of those services if they had no actual knowledge of either the unlawful nature of the activities or information in question or of the facts and

circumstances pointing to their unlawful nature, or if, as soon as they became aware of that unlawful nature, they acted expeditiously to remove the data at issue or block access to them.

…

II. – The persons referred to in point I(1) and (2) shall keep and retain the data in such a way as to make it possible to identify anyone who has assisted in the creation of all or part of the content of the services of which they are the providers.

They shall provide persons who publish an online public communication service with technical tools enabling them to satisfy the identification conditions laid down in point III.

A judicial authority may require the service providers mentioned in point I(1) and (2) to communicate the data referred to in the first paragraph.

The provisions of Articles 226-17, 226-21 and 226-22 of the Criminal Code shall apply to the processing of those data.

A decree to be adopted following consultation of the Conseil d'État (Council of State) and after consultation of the Data Protection Authority shall define the data referred to in the first paragraph and determine the period for which, and the methods by which, those data is to be retained.

…'

*The CMF*

24 The first paragraph of Article L. 621-10 of the Code monétaire et financier (Monetary and Financial Code), in the version applicable to the disputes in the main proceedings ('the CMF'), provided:

'Investigators and reviewers may, for the purposes of their investigation or review, be provided with all documents, whatever their format. Investigators may also be provided with the data retained and processed by telecommunications operators in the context of Article L. 34-1 of [the CPCE] and the service providers referred to in point I(1) and (2) of Article 6 of the [LCEN] and obtain copies of those data.

…'

25 After drawing conclusions from the decision of 21 July 2017 of the Conseil constitutionnel (Constitutional Council, France) declaring unconstitutional the second sentence of the first paragraph of Article L. 621-10 of the CMF, the legislature, by loi nº 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude (Law No 2018-898 of 23 October 2018 on combating fraud) (JORF of 24 October 2018, text No 1), inserted Article L. 621-10-2 into the Code monétaire et financier (Monetary and Financial Code), which provides:

'For the purpose of investigating market abuse as defined by Regulation [No 596/2014], the investigators may be provided with the data retained and processed by telecommunications operators, subject to the conditions and within the limits laid down in Article L. 34-1 of the [CPCE], and by the service providers referred to in point I(1) and (2) of Article 6 of the [LCEN].

Communication of the data mentioned in the first paragraph of this Article shall be the subject of prior authorisation by a reviewer of connection data requests.

The reviewer of connection data requests shall be, alternately, either an active or honorary member of the Conseil d'État (Council of State) elected by the General Assembly of the Conseil d'État (Council of State), then either an active or honorary judge of the Cour de cassation (Court of Cassation, France) elected by the General Assembly of that court. His or her alternate, from the other court, shall be appointed in accordance with the same rules. The reviewer of connection data requests and his or her alternate shall be elected for a non-renewable four-year term.

…

The reviewer of connection data requests may not receive or request any instruction from the Autorité des marchés financiers (Financial Markets Authority, France) or from any other authority in the performance of his or her duties. He or she shall be bound by the obligation of professional secrecy subject to the conditions laid down in Article L. 621-4 of this Code.

The matter shall be referred to him or her by reasoned request from the Secretary General or Deputy Secretary General of the Autorité des marchés financiers (Financial Markets Authority). The request shall contain information justifying its substance.

The authorisation shall be included in the investigation file.

The investigators shall use the data submitted by the telecommunications operators and service providers referred to in the first paragraph of this Article exclusively for the purposes of the investigation in the context of which they received the authorisation.

Connection data relating to acts which are the subject of notifications of objections by the Board of the Autorité des marchés financiers (Financial Markets Authority) shall be destroyed after a period of six months from the final decision of the Enforcement Committee or the appeal courts. In the case of an administrative settlement, the six-month period shall run from the date of execution of the agreement.

Connection data relating to acts which have not been the subject of a notification of objections by the Board of the Autorité des marchés financiers (Financial Markets Authority) shall be destroyed after a period of one month from the date of the decision of the Board.

In the event that the investigation report is sent to the procureur de la République financier (Financial Public Prosecutor, France) or the procureur de la République financier (Financial Public Prosecutor) brings a public prosecution ..., the connection data shall be delivered to the procureur de la République financier (Financial Public Prosecutor) and shall not be retained by the Autorité des marchés financiers (Financial Markets Authority).

The detailed rules for the implementation of this Article shall be set out in a decree to be adopted following consultation of the Conseil d'État (Council of State).'

**The disputes in the main proceedings, the questions referred for a preliminary ruling and the procedure before the Court**

26 Further to an application made by the public prosecutor on 22 May 2014, a judicial investigation was launched into VD and SR in respect of acts constituting the offences of insider

dealing and concealment of insider dealing. That investigation was subsequently extended, by a first supplementary application of 14 November 2014, to cover the offence of aiding and abetting.

27 On 23 and 25 September 2015, the Autorité des marchés financiers (Financial Markets Authority; 'AMF') sent to the investigating judge certain information available to it in the context of an investigation which it had carried out under Article L. 621-10 of the CMF, which included personal data from telephone calls made by VD and SR which the AMF investigators had collected, on the basis of Article L. 34-1 of the CPCE, from operators providing electronic communications services.

28 Further to that report issued by the AMF, the investigation was extended, by three supplementary applications of 29 September 2015, 22 December 2015 and 23 November 2016, to cover the offences of corruption and money laundering.

29 On 10 March and 29 May 2017 respectively, VD and SR were placed under investigation; the investigation in respect of VR related to the offences of insider dealing and money laundering, while the investigation in respect of SR related to the offence of insider dealing.

30 In so far as the investigation into them was based on the traffic data provided by the AMF, VD and SR each brought an action before the cour d'appel de Paris (Court of Appeal, Paris, France), relying, inter alia, on a plea alleging, in essence, infringement of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter. Specifically, VD and SR, relying on the case-law arising from the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), challenged the fact that that authority took Article L. 621-10 of the CMF and Article L. 34-1 of the CPCE as its legal basis for the collection of those data, while those provisions, first, did not comply with EU law in so far as they provided for general and indiscriminate retention of connection data and, second, laid down no restrictions on the powers of the AMF's investigators to require the retained data to be provided to them.

31 By two judgments of the cour d'appel de Paris (Court of Appeal, Paris) of 20 December 2018 and 7 March 2019, that court rejected the action brought by VD and SR. It is apparent from the information in the requests for a preliminary ruling that, when it rejected the plea alleging, in essence, infringement of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, the court adjudicating on the substance of the case relied, inter alia, on the fact that Article 23(2)(h) of Regulation No 596/2014, relating to market abuse, allows the competent authorities to require, in so far as permitted by national law, existing data traffic records held by operators providing electronic communications services, where there is a reasonable suspicion of an infringement of the prohibition on insider dealing under Article 14(a) and (b) of that regulation and where such records may be relevant to the investigation of that infringement.

32 VD and SR brought an appeal against those judgments before the referring court, raising a plea alleging infringement, inter alia, of the provisions of the Charter and Directive 2002/58 referred to in the preceding paragraph.

33 As regards access to the connection data, the referring court refers to a decision of the Conseil constitutionnel (Constitutional Council, France) of 21 July 2017, from which it is apparent that the procedure for accessing personal data retained by the AMF investigators, as provided for by French law, is not consistent with the right to respect for privacy, as protected by Article 2 of the Declaration of the Rights of Man and of the Citizen of 1789, stating that, although the national legislature had given authorised agents who are obliged to observe professional secrecy the power

to obtain such data in the context of an investigation and had not given them enforcement powers, it had not, however, built into that procedure any other guarantee such as to ensure an equal balance between, first, the right of respect for privacy and, second, the prevention of breaches of public order and the investigation of offenders, with the result that the second sentence of the first paragraph of Article L. 621-10 of the CMF had to be declared to be contrary to the French Constitution.

34 The referring court also notes, first, that the Conseil constitutionnel (Constitutional Council) took the view that, in view of the 'manifestly excessive' consequences that immediate repeal of that provision might have for pending proceedings, it was necessary to defer the date of that repeal to 31 December 2018 and, second, that the national legislature, drawing the appropriate conclusions from the declaration that the first paragraph of Article L. 621-10 of the CMF was unconstitutional, inserted Article L. 621-10-2 into that code.

35 The referring court, while recalling the findings set out in paragraph 125 of the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), is of the opinion that, in view of the fact that the effects of the repeal of the second sentence of the first paragraph of Article L. 621-10 of the CMF, applicable at the material time, were postponed, it cannot result from the declaration that that provision is unconstitutional that it is invalid. It takes the view, however, that the power of AMF investigators under that provision to obtain connection data without prior review by a court or an independent administrative authority is inconsistent with the requirements of Articles 7, 8 and 11 of the Charter, as interpreted by the Court.

36 In those circumstances, the only question that arises in that regard is whether it is possible to postpone the temporal effects of the repeal of Article L. 621-10 of the CMF, even though it does not comply with the Charter.

37 As regards the retention of connection data, the referring court states first of all that, although point II of Article L. 34-1 of the CPCE lays down an obligation in principle, according to which operators providing electronic communications services must erase or make anonymous any traffic data, that obligation is nevertheless accompanied by a number of exceptions, including the exception laid down in point III of that provision, relating to 'the purposes of investigating, detecting and prosecuting criminal offences'. For those specific purposes, the operations to erase or make anonymous certain pieces of data would be deferred for one year.

38 It states, in that regard, that the five categories of data concerned in particular by the conditions laid down in point III of Article L. 34-1 of the CPCE are those set out in Article R. 10-13 of the CPCE. Those connection data are generated or processed following a communication and relate to the circumstances of that communication and service users, but give no indication of the content of the communications concerned.

39 Next, the referring court makes reference to paragraph 112 of the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), according to which Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and observes that, in the context of the cases in the main proceedings, the AMF had access to the data retained by operators providing electronic communications services as there were suspicions concerning insider dealing and market abuse that may fall within the scope of a

number of serious offences. That access was justified by the need for that authority, in order to ensure the effectiveness of its investigation, to cross-reference various pieces of retained data over a certain period of time, with a view to updating the inside information being exchanged by a number of interlocutors, which revealed the existence of unlawful practices in that regard.

40 According to the referring court, the investigations carried out by the AMF satisfy the obligations imposed on the Member States by Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, read in the light of Article 1 of that regulation, including, in particular, the obligation to require existing data traffic records held by operators providing electronic communications services to be submitted.

41 In addition, that court, first, refers to recital 65 of that regulation and observes that those connection data constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing since they make it possible to establish the identity of a person responsible for the dissemination of false or misleading information or that persons have been in contact at a certain time.

42 Second, the referring court cites recital 66 of that regulation, from which it is apparent that the exercise of powers conferred on competent authorities in the field of finance may interfere with the right to respect for private and family life, home and communications and that, consequently, Member States should have in place adequate and effective safeguards against any abuse by restricting the scope of those powers solely to where they are necessary for the proper investigation of serious cases where there are no equivalent means for effectively achieving the same result. According to that court, it follows from that recital that certain cases of market abuse must be regarded as serious infringements.

43 The referring court also observes that, in the cases in the main proceedings, the inside information that may have constituted the substantive element of the unlawful market practices was essentially oral information that was secret.

44 In the light of the findings above, the referring court is uncertain how to reconcile Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter with the requirements under Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014.

45 Lastly, should the Court find that the legislation on the retention of the connection data at issue in the main proceedings does not comply with EU law, the question arises as to whether that legislation retains its effects provisionally, in order to avoid legal uncertainty and to allow the data previously collected and retained to be used for the purpose of detecting insider dealing and bringing criminal proceedings in respect of it.

46 In those circumstances, the Cour de cassation (Court of Cassation) decided to stay the proceedings and to refer the following questions, which are worded identically in Cases C-399/20 and C-397/20, to the Court of Justice for a preliminary ruling:

‘(1) Do Article 12(2)(a) and (d) of Directive [2003/6] and Article 23(2)(g) and (h) of Regulation [No 596/2014], which replaced that directive from 3 July 2016, read in the light of recital 65 of that regulation, not imply that, account being taken of the covert nature of the information exchanged and the fact that the potential subjects of investigation are members of the general public, the national legislature must be able to require electronic communications operators to retain connection data on a temporary but general basis in order to enable the administrative authority

referred to in Article 11 of [Directive 2003/6] and Article 22 of [Regulation No 596/2014], in the event of the emergence of grounds for suspecting certain persons of being involved in insider dealing or market manipulation, to require the operator to surrender existing records of traffic data in cases where there are reasons to suspect that the records so linked to the subject matter of the investigation may prove relevant to the production of evidence of the actual commission of the breach, to the extent, in particular, that they offer a means of tracing the contacts established by the persons concerned before the suspicions emerged?

(2) If the answer … [to the first question] is such as to prompt the Cour de cassation (Court of Cassation) to form the view that the French legislation on the retention of connection data is not consistent with EU law, could the effects of that legislation be temporarily maintained in order to avoid legal uncertainty and to enable data previously collected and retained to be used for one of the objectives of that legislation?

(3) May a national court temporarily maintain the effects of legislation enabling the officials of an independent administrative authority responsible for investigating market abuse to obtain access to obtain connection data without prior review by a court or another independent administrative authority?'

47 By decision of the President of the Court of 17 September 2020, Cases C-339/20 and C-397/20 were joined for the purposes of the written and oral parts of the procedure and of the judgment.

48 On 21 April 2021, the Conseil d'État (Council of State, France) delivered the judgment in *French Data Network and Others* (No 393099, 394922, 397844, 397851, 424717, 424718), by which it ruled, inter alia, on the compatibility with EU law of certain national legislative provisions which are relevant to the disputes in the main proceedings, namely Article L. 34-1 of the CPCE and Article R. 10-13 of the CPCE.

49 At the Court's invitation, the participants in the hearings in the present cases were given the opportunity to express their views on the effect, if any, of that judgment of the Conseil d'État (Council of State) on the present references for a preliminary ruling.

50 The representative of the French Government stated at that hearing that, by that judgment, the Conseil d'État (Council of State), in essence, declared unlawful the provisions implementing the general and indiscriminate retention of connection data for the purposes of fighting crime with the exception of the retention of IP addresses and data relating to the civil identity of users of electronic communications networks, thereby giving due effect to the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791). He stated, however, that, in the context of the proceedings, the Conseil d'État (Council of State) also had to respond to the French Government's objection that that interpretation of EU law was inconsistent with rules of constitutional status, namely those relating to the prevention of breaches of public order, in particular the safety of persons and property, and the investigation of offenders.

51 In that regard, the representative of the French Government explained that the Conseil d'État (Council of State) had rejected that objection in two stages. First, it is true that it acknowledged that the general and indiscriminate retention of the connection data was a decisive factor for the success of criminal investigations and that no other method could effectively take the place of those investigations. Second, however, the Conseil d'État (Council of State) relied, in particular, on paragraph 164 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and took the view that the expedited retention of data

was authorised by EU law including where that expedited retention related to data initially retained for the purpose of safeguarding national security.

52 Furthermore, the representative of the French Government noted that, following the judgment of the Conseil d'État (Council of State) of 21 April 2021, *French Data Network and Others* (No 393099, 394922, 397844, 397851, 424717 and 424718), the national legislature had inserted point III bis into Article L. 34-1 of the Post and Electronic Communications Code, as mentioned in paragraph 21 of the present judgment.

## Consideration of the questions referred

### *Preliminary observations*

53 In the first place, it should be noted that, after the present requests for a preliminary ruling had been lodged, the Conseil d'État (Council of State) delivered the judgment of 21 April 2021, *French Data Network and Others* (No 393099, 394922, 397844, 397851, 424717, 424718), concerning, inter alia, the compatibility with EU law of Article L. 34-1 of the CPCE and Article R. 10-13 of the CPCE.

54 As the Advocate General observed in point 42 of his Opinion, and as is also apparent from the explanations provided by the referring court, as set out in paragraphs 27, 37 and 38 above, those articles are 'key provisions' in the context of the application of Article L. 621-10 of the CMF, which is at issue in the main proceedings.

55 At the hearing before the Court, after highlighting the legislative development of Article L. 34-1 of the CPCE in response to the clarifications provided by the Court in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), as referred to in paragraph 21 of the present judgment, the representative of the French Government indicated, in essence, that, in order to resolve the disputes in the main proceedings, the referring court was required, in accordance with the principle of the application of the law *ratione temporis* enshrined in Article 7 and 8 of the Declaration of the Rights of Man and of the Citizen of 1789, to take account of provisions of national law in the version applicable to the facts at issue in the main proceedings, which date from 2014 and 2015, with the result that the judgment of the Conseil d'État (Council of State) of 21 April 2021, *French Data Network and Others* (No 393099, 394922, 397844, 397851, 424717, 424718) could not be taken into consideration in any event when analysing the present requests for a preliminary ruling.

56 According to settled case-law, in proceedings under Article 267 TFEU, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine in the light of the particular circumstances of the case both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions submitted by the national court concern the interpretation of Union law, the Court of Justice is, in principle, bound to give a ruling (see, to that effect, judgment of 8 September 2010, *Winner Wetten*, C-409/06, EU:C:2010:503, paragraph 36 and the case-law cited).

57 The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the

questions submitted to it (see, to that effect, judgment of 19 November 2009, *Filipiak*, C-314/08, EU:C:2009:719, paragraph 42 and the case-law cited).

58 In the present case, it is apparent from the orders for reference that the first and third questions directly concern, not Article L. 34-1 of the CPCE and Article R. 10-13 of the CPCE, but Article L. 621-10 of the CMF, pursuant to which the AMF asked operators providing electronic communications services to submit to it traffic data relating to telephone calls made by VD and SR, on the basis of which an investigation was opened into them and the admissibility of which as evidence is disputed in the main proceedings.

59 In addition, it should be noted that, by the second and third questions referred in the present cases, which are an extension of the first questions, the referring court asks, in essence, whether, in the event that the national legislation at issue relating to the retention of and access to connection data proves to be incompatible with EU law, its effects could not, nevertheless, be provisionally maintained, so as to avoid legal uncertainty and to allow the data retained on the basis of that legislation to be used for the purposes of detecting insider dealing and bringing prosecutions accordingly.

60 In the light of the considerations above, as well as those referred to by the Advocate General in points 44 to 47 of his Opinion, it must be held that, irrespective of the judgment of the Conseil d'État (Council of State) of 21 April 2021, *French Data Network and Others* (No 393099, 394922, 397844, 397851, 424717, 424718), and of the decision of the Conseil constitutionnel (Constitutional Council) of 25 February 2022 (No 2021-976/977), which declared Article L. 34-1 of the CPCE, in the version referred to in paragraph 20 of the present judgment, to be unconstitutional in part, an answer from the Court to the questions referred remains necessary in order to resolve the disputes in the main proceedings.

61 In the second place, it should be noted that, at the hearing before the Court, VD's representative disputed the applicability *ratione temporis* of Regulation No 596/2014, claiming, in essence, that the facts at issue in the main proceedings had occurred before the entry into force of that regulation. Therefore, only the provisions of Directive 2003/6 are relevant for the purposes of examining the questions referred by the national court.

62 In that regard, it must be borne in mind that, according to settled case-law, a new rule of law applies from the entry into force of the act introducing it, and, while it does not apply to legal situations that have arisen and become final under the old law, it does apply to their future effects, and to new legal situations. The position is otherwise, subject to the principle of the non-retroactivity of legal acts, only if the new rule is accompanied by special provisions which specifically lay down its conditions of temporal application (see, to that effect, judgments of 15 January 2019, *E.B.*, C-258/17, EU:C:2019:17, paragraph 50 and the case-law cited, and of 14 May 2020, *Azienda Municipale Ambiente*, C-15/19, EU:C:2020:371, paragraph 57).

63 As has been pointed out in paragraphs 26 to 29 above, although the legal situations concerned by the cases in the main proceedings arose before the entry into force of Regulation No 596/2014, which repealed and replaced Directive 2003/6 with effect from 3 July 2016, the proceedings in the main proceedings continued after that date, with the result that, as from that date, the future effects of those situations are, in accordance with the principle recalled in the preceding paragraph, governed by Regulation No 596/2014.

64 It follows that the provisions of Regulation No 596/2014 are applicable in the present case. Moreover, there is no need to draw a distinction between the provisions referred to by the referring

court resulting from Directive 2003/6 and Regulation No 596/2014, since their scope is essentially similar for the purposes of the interpretation which the Court will be required to give in the present cases.

***The first question***

65 By its first question, the referring court asks, in essence, whether Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, read in conjunction with Article 15(1) of Directive 2002/58, and in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures such as the one at issue in the main proceedings which, as a preventive measure, in order to combat market abuse offences including insider dealing, provide for the general and indiscriminate retention of traffic data for a year from the date on which they were recorded.

66 The parties to the main proceedings and the interested parties that submitted written observations to the Court have expressed differing views in that regard. For the Estonian Government, for Ireland and for the Spanish and French Governments, Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014 implicitly but necessarily empower the national legislature to impose a general and indiscriminate obligation on operators providing electronic communications services to retain data in order to allow the competent financial authority to detect and impose sanctions for insider dealing. Since, as is apparent from recital 65 of Regulation No 596/2014, those records constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing, such an obligation to retain is necessary both for ensuring the efficacy of instigations led by and prosecutions brought by that authority and, at the same time, the effectiveness of Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(h) of Regulation No 596/2014, and in order to meet the general interest objectives pursued by those instruments, which seek to guarantee the integrity of the EU financial markets and to enhance investor confidence in those markets.

67 VD, SR, the Polish Government and the European Commission submit, on the other hand, that those provisions, in so far as they merely provide a framework for the power to require operators providing electronic communications services to send ‘existing’ traffic data records held by those operators, govern only the issue of access to those data.

68 In that regard, it should be noted, in the first place, that it is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (see, to that effect, judgment of 17 April 2018, *Egenberger*, C-414/16, EU:C:2018:257, paragraph 44).

69 As regards the wording of the provisions referred to in the first question, it should be noted that, while Article 12(2)(d) of Directive 2003/6 refers to the power of the competent financial authority to ‘require existing telephone and existing data traffic records’, Article 23(2)(g) and (h) of Regulation No 596/2014 refers to the power of that authority to require, first, ‘existing … data traffic records held by investment firms, credit institutions or financial institutions’ and, second, to require, ‘in so far as permitted by national law, existing data traffic records held by a telecommunications operator’.

70 It is clear from the wording of those provisions that they merely provide a framework for that authority’s power to ‘require’ the data available to those operators, which corresponds to access to those data. Furthermore, the reference made to ‘existing’ records, such as those ‘held’ by those

operators, suggests that the EU legislature did not intend to lay down rules governing the option open to the national legislature to impose an obligation to retain such records.

71 In that regard, in accordance with settled case-law, an interpretation of a provision of EU law cannot have the result of depriving the clear and precise wording of that provision of all effectiveness. Thus, where the meaning of a provision of EU law is absolutely plain from its very wording, the Court cannot depart from that interpretation (judgment of 25 January 2022, *VYSOČINA WIND*, C-181/20, EU:C:2022:51, paragraph 39 and the case-law cited).

72 The interpretation outlined in paragraph 70 above is supported both by the context of Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, and by the objectives pursued by the rules of which those provisions form part.

73 As regards the context of those provisions, it should be noted that, although, under Article 12(1) of Directive 2003/6 and Article 23(3) of Regulation No 596/2014, read in the light of recital 62 of that regulation, the EU legislature intended to require the Member States to take the necessary measures to ensure that the competent financial authorities have a set of effective tools, powers and resources as well as the necessary supervisory and investigatory powers to ensure the effectiveness of their duties, those provisions make no mention of any option open to Member States of imposing, for that purpose, an obligation on operators providing electronic communications services to retain generally and indiscriminately traffic data, nor do they set out the conditions in which those data must be retained by those operators so that they can be submitted to the competent authorities where appropriate.

74 By Article 12(2) of Directive 2003/6 and Article 23(2) of Regulation No 596/2014, the EU legislature merely intended to grant to the competent financial authority, in order to ensure the effectiveness of its investigative and supervisory duties, ordinary powers of investigation, such as those enabling that authority to have access to documents, to carry out inspections and searches, or to issue orders or prohibitions against persons suspected of having committed market abuse offences including, inter alia, insider dealing.

75 Furthermore, it is clear that the provisions of Regulation No 596/2014 which specifically govern the question of data retention, namely the final subparagraph of Article 11(5), the second subparagraph of Article 11(6), Article 11(8), Article 11(11)(c), the first subparagraph of Article 17(1), Article 18(5) and Article 28 of that regulation, impose such an obligation to retain only on financial operators, as listed in Article 23(2)(g) of that regulation, and therefore concern only data relating to financial transactions and services provided by those specific operators.

76 As regards the objectives pursued by the legislation at issue, it must be observed that it is apparent, first, from recitals 2 and 12 of Directive 2003/6 and, second, from Article 1 of Regulation No 596/2014, read in the light of recitals 2 and 24 thereof, that the purpose of those instruments is to protect the integrity of EU financial markets and to enhance investor confidence in those markets, a confidence which depends, inter alia, on investors being placed on an equal footing and being protected against the improper use of inside information. The purpose of the prohibition on insider dealing laid down in Article 2(1) of Directive 2003/6 and Article 8(1) of Regulation No 596/2014 is to ensure equality between the contracting parties in stock-market transactions by preventing one of them who possesses inside information and who is, therefore, in an advantageous position vis-à-vis other investors, from profiting from that information, to the detriment of those who are unaware of it (see, to that effect, judgment of 15 March 2022, *Autorité des marchés financiers*, C-302/20, EU:C:2022:190, paragraphs 43, 65 and 77 and the case-law cited).

77 Although, according to recital 65 of Regulation No 596/2014, connection data records constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation, the fact remains that that recital makes reference only to records 'held' by operators providing electronic communications services and to the power of that competent financial authority to 'require' those operators to send 'existing' data. Thus, it is in no way apparent from that recital that the EU legislature intended, by that regulation, to give Member States the power to impose on operators providing electronic communications services a general obligation to retain data.

78 In the light of the foregoing, it must be held that neither Directive 2003/6 nor Regulation No 596/2014 can be interpreted as capable of constituting the legal basis for a general obligation to retain the data traffic records held by operators providing electronic communications services for the purposes of exercising the powers conferred on the competent financial authority under Directive 2003/6 and Regulation No 596/2014.

79 In the second place, it should be borne in mind that, as the Advocate General noted, in essence, in points 53 and 61 of his Opinion, Directive 2002/58 is the measure of reference on the retention and, more generally, the processing of personal data in the electronic communications sector, which means that the Court's interpretation in the light of that directive also governs the traffic data records held by operators providing electronic communications services, which the competent financial authorities, within the meaning of Article 11 of Directive 2003/6 and Article 22 of Regulation No 596/2014, may require from those operators.

80 According to Article 1(1) of Directive 2002/58, that directive provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector, the latter of which also covers the telecommunications sector.

81 Moreover, it is apparent from Article 3 of that directive that it is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices. Consequently, that directive must be regarded as regulating the activities of the providers of such services, including, in particular, telecommunications operators (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 93 and the case-law cited).

82 In the light of the foregoing, it must be held that, as the Advocate General submits, in essence, in points 62 and 63 of his Opinion, the assessment of the lawfulness of the processing of records held by operators providing electronic communications services, as provided for in Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, must be carried out in the light of the conditions laid down by Directive 2002/58 and of the interpretation of that directive in the Court's case-law.

83 That interpretation is borne out by Article 3(1)(27) of Regulation No 596/2014, in that it provides that, for the purposes of that regulation, traffic data records are those defined in point (b) of the second paragraph of Article 2 of Directive 2002/58.

84 In addition, according to recital 44 of Directive 2003/6 and recitals 66 and 77 of Regulation No 596/2014, the purposes of those instruments are to pursue the fundamental rights and principles

enshrined in the Charter, including the right to privacy. In that regard, the EU legislature expressly stated in recital 66 of Regulation No 596/2014 that, for the purposes of exercising the powers conferred on the competent financial authority under that regulation, which may amount to serious interferences with the right to respect for private and family life, home and communications, Member States should have in place adequate and effective safeguards against any abuse, for instance, where appropriate a requirement to obtain prior authorisation from the judicial authorities of a Member State concerned. Member States should make provision for the competent authorities to exercise such intrusive powers only to the extent that they are necessary for the proper conduct of an investigation into serious cases where there are no equivalent means for effectively arriving at the same result. It follows that the application of the measures governed by Directive 2003/6 and by Regulation No 596/2014 cannot, in any event, undermine the protection of personal data conferred under Directive 2002/58 (see, by analogy, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 57, and of 17 June 2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, paragraph 124 and the case-law cited).

85 Consequently, Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014 must be interpreted as not authorising the general and indiscriminate retention of traffic and location data for the purpose of combating market abuse offences and, in particular, insider dealing, since the compatibility with EU law of provisions of national law providing for such retention must be assessed in the light of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted in the Court's case-law.

86 As regards the examination of whether such national legislation is compatible with those provisions, it must be borne in mind that, as is apparent, in essence, from a combined reading of paragraphs 53, 54 and 58 of the present judgment, although the provision at the heart of the present references for a preliminary ruling is Article L. 621-10 of the CMF, under which the AMF requested operators providing electronic communications services to transmit traffic data relating to telephone calls made by VD and SR, on the basis of which an investigation was opened into the latter, the fact remains that, as the Advocate General noted in point 42 of his Opinion, Article 34-1 of the CPCE and Article R. 10-13 of the CPCE are 'key provisions' for the application of Article L. 621-10 of the CMF.

87 It is apparent from the explanations provided by the referring court, as summarised in paragraphs 27, 37 and 38 of the present judgment, that, first, the AMF investigators had collected the traffic data at issue on the basis of Article L. 34-1 of the CPCE, in the version applicable to the disputes in the main proceedings, point III of which established a certain number of exceptions to the obligation in principle laid down in point II of that article, according to which operators providing electronic communications services had to erase or make anonymous any traffic data, one exception of which related to 'the purposes of investigating, detecting and prosecuting criminal offences'. For those specific purposes, operations for the erasing or making anonymous of certain types of data were deferred for one year.

88 Second, that court states that the five categories of data concerned by point III of Article L. 34-1 of the CPCE, in the version applicable to the disputes in the main proceedings, were those listed in Article R. 10-13 of the CPCE, namely (i) information identifying the user, (ii) data relating to the communications terminal equipment used, (iii) the technical characteristics and date, time and duration of each communication, (iv) data relating to the additional services requested or used and the providers of those services and (v) data identifying the addressee or addressees of the communication. It is also clear from point II of Article R. 10-13 of the CPCE, in the version

applicable to the main proceedings, that, in the case of telephony activities, the operators concerned could also retain data enabling the origin and location of the communication to be identified.

89 It follows that the legislation at issue in the main proceedings covers all means of telephone communications and applies to all users of such means, without distinction or exception. Furthermore, the data which must be retained by operators providing electronic communications services under that legislation are, in particular, the data necessary for locating the source of a communication and its destination, for determining the date, time, duration and type of communication, for identifying the communications equipment used, and for locating the terminal equipment and communications, data which comprise, inter alia, the name and address of the user, the telephone numbers of the caller and the person called.

90 Thus, although the data which must, under the national legislation at issue, be retained for a period of one year do not cover the content of the communications concerned, they make it possible, inter alia, to identify the person with whom the user of a means of telephone communication has communicated and how, to determine the date, time and duration of the communications and the place from which those communications and connections took place, and to ascertain the location of the terminal equipment without any communication necessarily having been transmitted. In addition, those data enable the frequency of a user's communications with certain persons over a given period of time to be established. Therefore, it is necessary to take the view that those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 45 and the case-law cited).

91 As regards the objectives pursued, the purpose of the legislation at issue is, inter alia, the investigation, detection and prosecution of criminal offences, including those relating to market abuse such as insider dealing.

92 In the light of the factors set out in paragraphs 86 to 91 above, it must be held that, for the purposes, inter alia, of the investigation, detection and prosecution of criminal offences and the fight against crime, the national legislature provided, by the legislation at issue, for the general and indiscriminate retention of traffic data for one year from the day on which it was recorded.

93 It is apparent, in particular, from paragraphs 140 to 168 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and from paragraphs 59 to 101 of the judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258), that such retention cannot be justified by such objectives under Article 15(1) of Directive 2002/58.

94 It follows that national legislation, such as that at issue in the main proceedings, which requires operators providing electronic communications services, as a preventive measure, in order to combat market abuse offences including insider dealing, to retain generally and indiscriminately the traffic data of all users of means of electronic communication, with no differentiation in that regard or with no provision made for exceptions and without establishing the link required, in accordance with the case-law referred to in the previous paragraph, between the data to be retained and the objective pursued, falls outside of what is strictly necessary and cannot be considered to be

justified, in a democratic society, as is required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (see, to that effect, judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 81).

95 In the light of the foregoing, the answer to the first question in Cases C-339/20 and C-397/20 is that Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, read in conjunction with Article 15(1) of Directive 2002/58, and in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which, as a preventive measure, in order to combat market abuse offences including insider dealing, provide for the general and indiscriminate retention of traffic data for a year from the date on which they were recorded.

***The second and third questions***

96 By its second and third questions in the present cases, which it is appropriate to examine together, the referring court asks, in essence, whether EU law must be interpreted as meaning that a national court may restrict the temporal effects of a declaration of invalidity, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter.

97 At the outset, it should be recalled that the principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various provisions of EU law, since the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 118 and the case-law cited).

98 Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 119 and the case-law cited).

99 It is true that the Court has held, in a case concerning the lawfulness of measures adopted in breach of the obligation under EU law to conduct a prior assessment of the impact of a project on the environment and on a protected site, that if domestic law allows it, a national court may, by way of exception, maintain the effects of such measures where such maintenance is justified by overriding considerations relating to the need to nullify a genuine and serious threat of interruption in the electricity supply in the Member State concerned, which cannot be remedied by any other

means or alternatives, particularly in the context of the internal market, and continues only for as long as is strictly necessary to remedy the breach (see, to that effect, judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181).

100 However, unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure referred to in the preceding paragraph (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 121 and the case-law cited).

101 Maintaining the effects of national legislation such as that at issue in the main proceedings would mean that the legislation would continue to impose on operators providing electronic communications services obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been retained (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 122 and the case-law cited).

102 Therefore, the referring court cannot restrict the temporal effects of a declaration of invalidity which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 123 and the case-law cited).

103 In addition, it should be stated that a temporal restriction of the effects of the interpretation given was not imposed in the judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), and of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), with the result that, in accordance with the case-law recalled in paragraph 98 of this judgment, it should not be imposed in a judgment of the Court subsequent to those judgments.

104 Lastly, in view of the fact that the referring court is ruling on applications requesting that evidence obtained from traffic data be declared inadmissible on the ground that the national provisions at issue are contrary to EU law, both as regards the retention of data and access to those data, it is necessary to determine the effect of a finding that Article L. 621-10 of the CMF, in the version applicable to the facts at issue in the main proceedings, is incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, on the admissibility of the evidence adduced against VD and SR in the context of the main proceedings.

105 In that regard, it is sufficient to refer to the Court's case-law, in particular to the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152), from which it follows that such admissibility falls, in accordance with the principle of the procedural autonomy of the Member States, within the scope of national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

106 As regards the latter principle, it should be noted that it requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority to those data in breach of EU law, in the context of criminal proceedings against persons suspected of

having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 44 and the case-law cited).

107 In the light of the findings above, the answer to the second and third questions in the present cases is that EU law must be interpreted as precluding a national court from restricting the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of those provisions with Article 15(1) of Directive 2002/58 read in the light of the Charter. The admissibility of evidence obtained pursuant to provisions of national law that are incompatible with EU law is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

**Costs**

108 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 12(2)(a) and (d) of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6 and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, and read in the light of Articles 7, 8 and 11 and of Article 52(1) of the Charter of Fundamental Rights of the European Union**

**must be interpreted as:**

**precluding legislative measures which, as a preventive measure, in order to combat market abuse offences including insider dealing, provide for the general and indiscriminate retention of traffic data for a year from the date on which they were recorded.**

2. **European Union law must be interpreted as precluding a national court from restricting the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of those provisions with Article 15(1) of Directive 2002/58, as amended by**

**Directive 2009/136, read in the light of the Charter of Fundamental Rights of the European Union. The admissibility of evidence obtained pursuant to provisions of national law that are incompatible with EU law is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.**

[Signatures]

---

* Language of the case: French.