COMMISSION
EUROPÉENNE

Bruxelles, le 24.1.2018
COM(2018) 43 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018

Communication de la Commission au Parlement européen et au Conseil

Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018

Introduction

Le 6 avril 2016, l'UE a convenu d'une réforme en profondeur de son cadre de protection des données en adoptant un train de mesures visant à réformer ce domaine, dont le règlement général sur la protection des données[1], en remplacement de la directive 95/46/CE[2] («directive relative à la protection des données»), en vigueur depuis vingt ans, et la directive «police»[3]. Le 25 mai 2018, le nouvel instrument de l'UE en matière de protection des données, le règlement général sur la protection des données (ci-après le «règlement»), deviendra directement applicable, deux ans après son adoption et son entrée en vigueur[4].

Le nouveau règlement renforcera la protection du droit des personnes à la protection des données à caractère personnel les concernant, reflétant la place accordée par l'Union européenne à la protection des données en tant que droit fondamental[5].

Proposant un ensemble unique de règles directement applicables dans les ordres juridiques internes des États membres, le règlement garantira le libre flux des données à caractère personnel entre les États membres de l'UE et renforcera la confiance et la sécurité des consommateurs, deux éléments indispensables en vue d'un marché unique numérique à part entière. Le règlement laisse ainsi entrevoir de nouvelles perspectives pour les entreprises et les sociétés, en particulier celles de plus petite taille, en rendant également plus claires les règles régissant les transferts internationaux de données.

Bien que le nouveau cadre de protection des données s'appuie sur la législation existante, il produira de larges effets et nécessitera des ajustements considérables pour certains points. C'est pour cette raison que le règlement prévoyait une période transitoire de deux ans - jusqu'au 25 mai 2018 - pour laisser aux États membres et aux parties prenantes le temps de se préparer minutieusement au nouveau cadre juridique.

Ces deux dernières années, toutes les parties prenantes, des administrations nationales et des autorités nationales de protection des données aux responsables du traitement et aux sous-

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016.

[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995.

[3] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016.

[4] Entré en vigueur le 24 mai 2016, le règlement sera applicable à partir du 25 mai 2018.

[5] Voir l'article 8 de la Charte des droits fondamentaux et l'article 16 du TFUE.

traitants, ont pris part à un certain nombre d'activités destinées à faire en sorte que l'importance et l'ampleur des changements introduits par la nouvelle législation en matière de protection des données soient bien comprises et que tous les acteurs soient prêts à l'appliquer. La date limite du 25 mai approchant, la Commission estime qu'il convient de faire le bilan de ces travaux et de se pencher sur toute mesure supplémentaire qui pourrait être utile pour faire en sorte que tout soit prêt pour une prise d'effet réussie du nouveau cadre[6].

La présente communication:

- fait le récapitulatif des principales innovations et perspectives entrouvertes par la nouvelle législation de l'UE en matière de protection des données;
- fait le bilan des travaux préparatoires réalisés à ce jour au niveau de l'UE;
- passe en revue les mesures que la Commission européenne, les autorités nationales de protection des données et les administrations nationales devraient encore prendre afin de mener à bien lesdits préparatifs;
- expose les mesures que la Commission compte prendre dans les prochains mois.

En outre, parallèlement à l'adoption de la présente communication, la Commission lance une boîte à outils en ligne pour aider les parties prenantes à se préparer en vue de l'application du règlement, ainsi qu'une campagne d'informations dans tous les États membres, avec le soutien des bureaux de représentation.

1. LE NOUVEAU CADRE EUROPÉEN DE PROTECTION DES DONNÉES - UNE MEILLEURE PROTECTION ET DE NOUVELLES PERSPECTIVES

Le règlement continue de suivre la même approche que la directive relative à la protection des données, mais, tirant les enseignements de vingt ans de législation de l'UE en matière de protection des données et de la jurisprudence en la matière, il apporte certaines clarifications et modernise la réglementation en question, en introduisant un certain nombre de nouveautés qui renforcent la protection des droits individuels et ouvrent de nouvelles perspectives pour les sociétés et les entreprises, en particulier:

- **un cadre juridique harmonisé aboutissant à une application uniforme des règles, au profit du marché unique numérique de l'UE**. Soit un ensemble unique de règles pour les citoyens et les entreprises, qui permettra de remédier au problème actuel, à savoir que les États membres ont mis en œuvre les dispositions de la directive de différentes façons. Un mécanisme de guichet unique est introduit afin de garantir une application uniforme et cohérente des dispositions dans tous les États membres de l'UE;

- **des conditions de concurrence équitables pour toutes les entreprises exerçant leurs activités sur le marché de l'UE.** Le règlement exige des entreprises établies en dehors de l'Union européenne qu'elles appliquent les mêmes règles que celles qui sont installées dans l'UE dans le cas où elles offrent des biens et des services dans le domaine des données à caractère personnel ou surveillent le comportement de personnes dans l'Union. Les entreprises établies à l'extérieur de l'UE et exerçant leurs activités sur le marché unique doivent, dans certaines circonstances, désigner dans l'UE un représentant auquel

[6] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_fr.pdf.

les citoyens et les autorités peuvent s'adresser en plus ou au lieu de l'entreprise basée à l'étranger;

- **les principes de protection des données dès la conception et de protection des données par défaut**, qui incitent à trouver des solutions innovantes pour remédier d'emblée aux problèmes qui se posent en matière de protection des données;

- **le renforcement des droits individuels**. Le règlement introduit de nouvelles exigences en matière de transparence; renforcement des droits à l'information, d'accès aux données à caractère personnel et à l'effacement de ces données («droit à l'oubli»); le silence ou l'absence de réaction n'auront plus valeur de consentement valable, dès lors que le consentement passera par un acte positif clair; la protection des enfants en ligne;

- **la possibilité pour les citoyens d'exercer un contrôle accru sur les données à caractère personnel les concernant.** Le règlement établit un **nouveau droit à la portabilité des données**, permettant aux citoyens de demander à une entreprise ou à une organisation de récupérer les données à caractère personnel qu'ils ont fournies à ladite entreprise ou organisation après avoir donné leur consentement ou en exécution d'un contrat; il permettra également la transmission directe de ces données à caractère personnel à une autre entreprise ou organisation, lorsque cette transmission est techniquement possible. Dès lors qu'il permet la transmission directe de données à caractère personnel d'une entreprise ou organisation à une autre, ce droit favorisera également le libre flux des données à caractère personnel au sein de l'Union, évitera leur verrouillage et encouragera la concurrence entre entreprises. Le fait que les citoyens puissent plus facilement passer d'un prestataire de services à un autre encouragera la mise au point de nouveaux services dans le cadre de la stratégie pour un marché unique numérique.

- **le renforcement de la protection contre les violations de données.** Le règlement établit un ensemble complet de règles concernant les violations de données à caractère personnel. Il définit clairement ce qu'est une «violation de données à caractère personnel», introduit l'obligation de notifier les violations de données à l'autorité de contrôle au plus tard dans les 72 heures, lorsque ladite violation est susceptible d'engendrer un risque pour les droits et les libertés des personnes physiques. Dans certaines circonstances, il exige que la personne qui a subi une violation des données à caractère personnel la concernant en soit informée. Ces mesures permettent de renforcer considérablement la protection par rapport à la situation actuelle au sein de l'UE, dans laquelle seuls les fournisseurs de services de communications électroniques, les opérateurs de services essentiels et les fournisseurs de services numériques sont tenus de notifier les violations de données en vertu de la directive «vie privée et communications électroniques»[7] et de la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI)[8] respectivement;

---

[7] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), JO L 201 du 31.7.2002, p. 37. Conformément à l'article 95 du règlement général sur la protection des données, ledit règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE. Cela signifie, par exemple, que les entités concernées par la directive «vie privée et communications électroniques» sont soumises à l'obligation de notifier toute violation de données à

- **le règlement habilite toutes les autorités de protection des données à infliger des amendes aux responsables du traitement et aux sous-traitants.** Toutes ne possèdent pas ce pouvoir à l'heure actuelle. Une telle prérogative permettra d'améliorer la mise en œuvre des règles. Les amendes peuvent s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total;

- **une plus grande flexibilité pour les responsables du traitement et pour les sous-traitants amenés à traiter des données à caractère personnel en raison de dispositions ambigües au sujet de la responsabilité (le principe de responsabilité)**. Le règlement s'écarte d'un mécanisme de notification pour privilégier le principe de responsabilité, lequel est mis en œuvre dans le cadre d'obligations modulables en fonction du risque (par exemple, la présence d'un délégué à la protection des données ou l'obligation de réaliser des analyses d'impact relatives à la protection des données). Un nouvel instrument est introduit pour aider à évaluer le risque avant le début du traitement: il s'agit de l'analyse d'impact relative à la protection des données. Celle-ci est requise dès que le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes concernées. Le règlement mentionne trois situations de ce type en particulier: lorsqu'une entreprise procède à une évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques (profilage compris), traite à grande échelle des données sensibles ou surveille systématiquement à grande échelle des zones accessibles au public. Les autorités nationales de protection des données devront publier les listes de cas nécessitant une analyse d'impact relative à la protection des données[9];

- **une plus grande clarté en ce qui concerne les obligations incombant aux sous-traitants et la responsabilité des responsables du traitement quant à la sélection d'un sous-traitant**;

- **un système de gestion moderne pour garantir la mise en application renforcée et plus cohérente des règles.** Sont inclus des compétences harmonisées pour les autorités de protection des données, notamment en ce qui concerne les amendes, et de nouveaux mécanismes permettant auxdites autorités de coopérer au sein d'un réseau;

- **la protection des données à caractère personnel garantie par le règlement concerne aussi les données hors de l'Union européenne, ce qui garantit un niveau élevé de protection**[10]. Alors que l'architecture des dispositions du règlement relatives aux transferts internationaux demeure, pour l'essentiel, identique à celle prévue dans la directive de 1995, la réforme apporte de la clarté en ce qui concerne leur utilisation et simplifie celle-ci, tout en introduisant de nouveaux outils pour les transferts. En ce qui concerne les décisions d'adéquation, le règlement introduit une liste précise et détaillée

---

caractère personnel dès lors que celle-ci concerne un service matériellement couvert par ladite directive. Le règlement ne leur impose aucune obligation supplémentaire à cet égard.

[8] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1. Les entités relevant du champ d'application de la directive SRI doivent notifier les incidents ayant une incidence importante ou significative sur la prestation de certains de leurs services. La notification des incidents en vertu de la directive SRI est sans préjudice de l'obligation de notifier les violations des données à caractère personnel prévue par le règlement;

[9] Article 35 du règlement.

[10] Communication de la Commission intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation», COM(2017) 7 final.

d'éléments dont la Commission doit tenir compte quand elle doit déterminer si un système étranger garantit une protection adéquate des données à caractère personnel. De même, le règlement formalise et élargit le nombre d'instruments de transfert d'un autre genre, tels que les clauses contractuelles types et les règles d'entreprise contraignantes.

Le règlement révisé pour les institutions, organes et organismes de l'UE[11], et le règlement «vie privée et communications électroniques»[12], qui font actuellement l'objet de négociations, une fois qu'ils auront été adoptés, doteront l'UE d'un ensemble solide et complet de règles en matière de protection des données[13].

2. TRAVAUX PRÉPARATOIRES RÉALISÉS À CE JOUR AU NIVEAU DE L'UE

La bonne application du règlement exige la coopération de tous les acteurs de la protection des données: les États membres, notamment les administrations publiques, les autorités nationales de protection des données (APD), les entreprises, les organisations traitant des données à caractère personnel, les personnes physiques, ainsi que la Commission européenne.

2.1. Actions de la Commission européenne

Peu après l'entrée en vigueur du règlement à la mi-2016, la Commission a noué le dialogue avec les autorités des États membres, les autorités nationales de protection des données et les parties prenantes pour préparer l'application du règlement et prodiguer soutien et conseils.

a) Soutenir les États membres et leurs autorités

La Commission coopère très étroitement avec les États membres afin d'appuyer leurs travaux pendant la période de transition, dans le but de garantir le niveau de cohérence le plus élevé possible. À cette fin, la Commission a instauré un groupe d'experts chargé d'accompagner les États membres dans le cadre des actions entreprises pour se préparer au règlement. Le groupe, qui s'est déjà réuni à treize reprises, fait office de forum où les États membres peuvent partager leurs expériences et leur expertise[14]. La Commission a aussi pris langue avec les autorités des États membres dans le cadre de réunions bilatérales afin d'examiner les questions qui se posent au niveau national.

b) Soutenir les différentes autorités de protection des données et la création du comité européen de la protection des données

---

[11] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, COM(2017) 8 final.

[12] Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM(2017) 10 final.

[13] Tant que le règlement «vie privée et communications électroniques» n'aura pas été adopté et ne sera pas entré en application, la directive 2002/58/CE s'appliquera en tant que *lex specialis* de ce règlement.

[14] Pour une liste détaillée des réunions, des ordres du jour, un résumé des discussions et un aperçu de l'état d'avancement du processus législatif dans les différents États membres, consulter http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=FR.

La Commission soutient activement les travaux du groupe de travail «article 29» afin que le passage de témoin au comité européen de la protection des données se déroule sans heurt[15].

c) Portée internationale

Le règlement consolidera davantage la capacité de l'UE à promouvoir activement ses valeurs en ce qui concerne la protection des données et facilitera les flux transfrontières de données en favorisant la convergence des différents ordres juridiques au niveau mondial[16]. Les règles de l'UE en matière de protection des données sont de plus en plus considérées au niveau international comme les normes les plus strictes qui soient dans le domaine de la protection des données à l'échelle de la planète. La convention 108 du Conseil de l'Europe, le seul instrument multilatéral juridiquement contraignant dans le domaine de la protection des données à caractère personnel, est elle aussi en cours de modernisation. La Commission s'emploie à ce qu'elle reflète les mêmes principes que ceux consacrés dans les nouvelles règles de l'UE en matière de protection des données et contribue de cette façon à instaurer un ensemble uniforme de normes élevées en matière de protection des données. La Commission encouragera activement l'adoption rapide du texte modernisé de la convention pour que l'UE y devienne partie[17]. La Commission encourage les pays tiers à ratifier la convention 108 du Conseil de l'Europe et son protocole additionnel.

Par ailleurs, plusieurs pays et organisations régionales extérieurs à l'UE, de notre voisinage immédiat à l'Asie, l'Amérique latine et l'Afrique, adoptent de nouvelles législations en matière de protection des données ou mettent à jour leurs législations existantes afin d'exploiter les possibilités offertes par l'économie numérique mondiale et de répondre à la demande croissante d'un renforcement de la sécurité des données et de la protection de la vie privée. En dépit des différences observées entre les pays en ce qui concerne leur approche et leur niveau de développement législatif, des signes montrent que le règlement sert de plus en plus de référence et de source d'inspiration[18].

Dans ce contexte, la Commission continue d'étendre son rayon d'action sur le plan international conformément à sa communication de janvier 2017[19], en entretenant un dialogue actif avec ses principaux partenaires commerciaux, notamment en Asie de l'Est et du Sud-Est et en Amérique latine, afin d'examiner la possibilité d'adopter des décisions d'adéquation[20].

Plus particulièrement, la Commission et le Japon s'emploient à constater simultanément, pour le début de l'année 2018, que chacune des deux parties offre un niveau de protection adéquat, comme l'ont annoncé le président Juncker et le Premier ministre Abe dans leur déclaration

---

[15] C'est ainsi que, par exemple, la Commission permettra au comité européen de la protection des données d'utiliser le système d'information du marché intérieur pour la communication entre ses membres.

[16] Document de réflexion sur la maîtrise de la mondialisation COM(2017) 240.

[17] Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE nº 108) et protocole additionnel de 2001 à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE nº 181). Ouverte aux pays non membres du Conseil de l'Europe, la convention a déjà été ratifiée par 51 pays (y compris par l'Uruguay, la République de Maurice, le Sénégal et la Tunisie).

[18] Voir, par exemple, Data Protection Standards of the Ibero-American States (normes de protection des données des États ibéro-américains), http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf

[19] COM(2017) 7.

[20] COM(2017) 7 ibid, p. 10.

commune le 6 juillet 2017[21]. De même, des pourparlers ont été lancés avec la Corée du Sud en vue d'une éventuelle décision d'adéquation. L'adoption d'une décision d'adéquation garantirait le libre flux de données avec les pays tiers concernés, tout en assurant l'application d'un niveau de protection élevé lors du transfert de données à caractère personnel de l'UE vers ces pays.

Parallèlement, la Commission s'emploie, avec les parties prenantes, à tirer pleinement parti de la boîte à outils prévue par le règlement pour les transferts internationaux en concevant des mécanismes de transfert d'un autre genre, qui soient adaptés aux besoins spécifiques de certains secteurs et/ou opérateurs[22].

d) Nouer le dialogue avec les parties prenantes

La Commission a organisé plusieurs événements à l'intention des parties prenantes[23]. Un nouvel atelier ciblant les consommateurs est prévu au premier trimestre de 2018. Des discussions sectorielles spécifiques dans des domaines tels que la recherche et les services financiers ont également eu lieu.

La Commission a également mis sur pied un groupe multipartite sur le règlement, composé de représentants de la société civile et d'entreprises, d'universitaires et de professionnels. Ce groupe conseillera la Commission, notamment quant à la façon d'atteindre un niveau adéquat de sensibilisation des parties prenantes au règlement[24].

Enfin, au moyen de son programme-cadre pour la recherche et l'innovation Horizon 2020[25], la Commission européenne a financé des actions de conception d'outils visant à favoriser l'application effective des dispositions du règlement en matière de consentement et de méthodes d'analyse des données respectueuses de la vie privée, telles que l'informatique multipartite et le chiffrement homomorphe.

2.2 Actions entreprises par le groupe de travail «article 29» / le comité européen de la protection des données

Le groupe de travail «article 29», qui regroupe toutes les autorités nationales de protection des données, dont le contrôleur européen de la protection des données, joue un rôle moteur dans la préparation de la mise en œuvre du règlement en publiant des lignes directrices à l'intention des entreprises et d'autres parties prenantes. Chargées de veiller au respect du règlement et faisant office de points de contact directs pour les parties prenantes, les autorités nationales de protection des données sont idéalement placées pour apporter un surcroît de sécurité juridique concernant l'interprétation du règlement.

---

[21] http://europa.eu/rapid/press-release_STATEMENT-17-1917_fr.htm.
[22] COM(2017) 7 ibid, p. 10.
[23] Deux ateliers avec les entreprises en juillet 2016 et avril 2017, deux tables rondes entre entreprises en décembre 2016 et mai 2017, un atelier consacré aux données relatives à la santé en octobre 2017, et un atelier avec des représentants de PME en novembre 2017.
[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=FR.
[25] https://ec.europa.eu/programmes/horizon2020/h2020-sections.

Lignes directrices/documents de travail du groupe de travail «article 29» ayant trait à l'entrée en vigueur du règlement[26].	
Droit à la portabilité des données	Adoption les 4 et 5 avril 2017
Délégués à la protection des données	
Désignation de l'autorité de contrôle chef de file	
Analyse d'impact relative à la protection des données	Adoption les 3 et 4 octobre 2017
Amendes administratives	Adoption les 3 et 4 octobre 2017
Profilage	Travaux en cours
Violation de données	Travaux en cours
Consentement	Travaux en cours
Transparence	Travaux en cours
Certification et accréditation	Travaux en cours
Critères de référence pour l'adéquation	Travaux en cours
Règles d'entreprise contraignantes pour les responsables du traitement	Travaux en cours
Règles d'entreprise contraignantes pour les sous-traitants	Travaux en cours

Le groupe de travail «article 29» s'emploie à actualiser les avis existants, y compris en ce qui concerne les outils servant aux transferts de données vers les pays tiers.

Vu qu'il est essentiel que les opérateurs disposent d'un ensemble unique et cohérent de lignes directrices, il importe que les lignes directrices au niveau national soient soit abrogées, soit mises en conformité avec celles adoptées par le groupe de travail «article 29»/le comité européen de la protection des données sur le même sujet.

La Commission attache une grande importance au fait que ces lignes directrices fassent l'objet d'une consultation publique avant d'être finalisées. Il est capital que la participation des parties prenantes à ce processus soit aussi précise et concrète que possible, car cela contribuera à recenser les bonnes pratiques et à attirer l'attention du groupe de travail «article 29» sur les caractéristiques d'entreprises ou de secteurs donnés. La responsabilité finale de ces lignes directrices incombe au groupe de travail «article 29» et au futur comité européen de la protection des données, et les autorités de protection des données s'y référeront lors de la mise en œuvre du règlement.

Il devrait être possible de modifier les lignes directrices en fonction de l'évolution de la situation et des différentes pratiques. À cette fin, il est primordial que les autorités de

[26] Toutes les lignes directrices adoptées sont disponibles sous: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

protection des données encouragent une culture de dialogue avec toutes les parties prenantes, entreprises comprises.

Il importe de rappeler que lorsque des questions concernant l'interprétation et l'application du règlement surviendront, il appartiendra aux juridictions nationales et européennes de fournir l'interprétation finale du règlement.

3. ÉTAPES RESTANT À FRANCHIR AUX FINS D'UNE PRÉPARATION RÉUSSIE

3.1 Achèvement par les États membres du cadre juridique au niveau national

Le règlement est directement applicable dans tous les États membres[27]. Cela signifie qu'il entre en vigueur et s'applique indépendamment de toute disposition du droit national: les dispositions du règlement peuvent normalement être invoquées directement par les citoyens, les entreprises, les administrations publiques et d'autres organisations de traitement de données à caractère personnel. Toutefois, conformément au règlement, toutefois, les États membres doivent prendre les mesures requises pour adapter leur législation en abrogeant et en modifiant les lois existantes, en instituant des autorités nationales de protection des données[28], en choisissant un organisme d'accréditation[29] et en établissant des règles permettant de réconcilier liberté d'expression et protection des données[30].

Le règlement donne aussi aux États membres la possibilité de préciser davantage l'application des règles en matière de protection des données dans certains domaines spécifiques: secteur public[31], emploi et sécurité sociale[32], médecine préventive et du travail, santé publique[33], fins archivistiques dans l'intérêt public, fins de recherche scientifique ou historique ou fins statistiques[34], numéro d'identification national[35], accès du public aux documents officiels[36] et obligations de secret[37]. En outre, pour les données génétiques, les données biométriques ou les

[27] Article 288 du TFUE.
[28] Article 54, paragraphe 1, du règlement.
[29] L'article 43, paragraphe 1, du règlement dispose que les États membres doivent proposer les deux méthodes d'accréditation possibles aux organismes de certification, à savoir l'accréditation par l'autorité nationale de contrôle de la protection des données, établie en vertu de la législation sur la protection des données, et/ou par l'organisme national d'accréditation, institué par le règlement (CE) n° 765/2008 relatif à l'accréditation et à la surveillance du marché. La coopération européenne pour l'accréditation (European cooperation for Accreditation — EA, organisme reconnu en vertu du règlement n° 765/2008), qui rassemble les organismes nationaux d'accréditation et les autorités de contrôle responsables du RGPD, devrait coopérer étroitement à cet effet.
[30] Article 85, paragraphe 1, du règlement.
[31] Article 6, paragraphe 2, du règlement.
[32] Article 88 et article 9, paragraphe 2, point b), du règlement. Le socle européen des droits sociaux dispose aussi que «*les travailleurs ont droit à la protection de leurs données personnelles dans le cadre du travail*». (2017/C 428/09, JO C 428 du 13.12.2017, p. 10).
[33] Article 9, paragraphe 2, points h) et i), du règlement.
[34] Article 9, paragraphe 2, point j), du règlement.
[35] Article 87 du règlement.
[36] Article 86 du règlement.
[37] Article 90 du règlement.

données concernant la santé, le règlement autorise les États membres à maintenir leurs conditions ou à en introduire de nouvelles, y compris des limitations[38].

Les actions des États membres dans ce contexte sont encadrées par deux éléments:

1. l'article 8 de la charte, ce qui signifie que toute loi nationale visant à préciser le règlement doit satisfaire aux exigences de l'article 8 de la charte (et du règlement qui s'appuie sur l'article 8 de la charte), et
2. l'article 16, paragraphe 2, du TFUE, en vertu duquel nulle législation nationale ne peut empiéter sur la libre circulation des données à caractère personnel au sein de l'UE.

Le règlement donne l'occasion de simplifier l'environnement juridique et donc d'avoir moins de règles nationales tout en offrant plus de clarté aux opérateurs.

Lorsqu'ils adaptent leur législation nationale, les États membres doivent tenir compte du fait que toute mesure nationale qui aurait pour conséquences de faire obstacle à l'applicabilité directe du règlement et de mettre en péril son application simultanée et uniforme dans l'ensemble de l'UE serait contraire aux traités[39].

Il est également interdit de répéter le texte des règlements dans le droit national (répéter des définitions ou les droits des individus, par exemple), sauf si ces répétitions sont absolument nécessaires à des fins de cohérence et afin de rendre la législation nationale compréhensible pour ceux auxquels elle s'applique[40]. La reproduction du texte du règlement mot pour mot dans la loi nationale visant à préciser le règlement devrait être exceptionnelle et justifiée et ne saurait servir à ajouter des conditions ou interprétations supplémentaires au texte du règlement.

L'interprétation du règlement est laissée aux juridictions européennes (aux juridictions nationales et en dernier recours à la Cour européenne de justice) et non aux législateurs des États membres. Le législateur national ne peut dès lors ni copier le texte du règlement, lorsque cela ne s'impose pas à la lumière des critères fournis par la jurisprudence, ni l'interpréter, ni ajouter de conditions supplémentaires aux règles directement applicables en vertu du règlement. Si tel était le cas, les opérateurs de toute l'Union seraient à nouveau confrontés à une situation fragmentée et ne sauraient pas à quelles règles se plier.

À ce stade, seuls deux États membres ont déjà adopté la législation nationale pertinente[41]; les autres États membres en sont à des stades divers de leurs procédures législatives[42] et ont programmé une adoption de la législation d'ici au 25 mai 2018. Il est important de donner aux opérateurs suffisamment de temps pour se préparer à l'ensemble des dispositions auxquelles ils doivent se conformer.

---

[38] Article 9, paragraphe 4, du règlement.
[39] Affaire 94/77 *Fratelli Zerbone Snc/Amministrazione delle finanze dello Stato* ECLI:EU:C:1978:17 et 101.
[40] Considérant 8 du règlement.
[41] Autriche (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf); Allemagne (https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1513091793362).
[42] Pour un aperçu de l'état d'avancement du processus législatif dans les différents États membres, voir http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461.

Si les États membres ne prennent pas les mesures nécessaires en application du règlement, tardent à les prendre ou utilisent les clauses de spécification prévues par le règlement d'une manière qui est contraire à celui-ci, la Commission fera usage de tous les outils à sa disposition, dont le recours à la procédure d'infraction.

3.2 Les autorités nationales de protection des données doivent veiller à ce que le nouveau comité européen de la protection des données, qui est un comité indépendant, soit pleinement opérationnel

Il est essentiel que le nouvel organe créé par le règlement, le comité européen de la protection des données[43], qui succède au groupe de travail «article 29», soit pleinement opérationnel à compter du 25 mai 2018.

Le contrôleur européen de la protection des données, qui est l'autorité chargée de la protection des données responsable du contrôle des institutions et organes de l'UE, assurera le secrétariat du comité européen de la protection des données afin de renforcer les synergies et pour plus d'efficacité. Au cours des mois passés, le contrôleur européen de la protection des données a entamé les préparatifs nécessaires à cette fin.

Le comité européen de la protection des données sera au cœur de la protection des données en Europe. Il contribuera à l'application cohérente de la législation en matière de protection des données et fournira une base solide à la coopération entre les autorités de protection des données, dont fait partie le contrôleur européen de la protection des données. Non seulement le comité européen de la protection des données publiera des lignes directrices sur la manière d'interpréter les concepts fondamentaux du règlement, mais il sera aussi appelé à publier des décisions contraignantes sur les différends en matière de traitement transfrontière. Cela garantira l'application uniforme des règles de l'UE et permettra d'éviter que le même cas reçoive un traitement différent d'un État membre à l'autre.

Le fonctionnement harmonieux et efficient du comité européen de la protection des données est dès lors nécessaire au bon fonctionnement du système dans son ensemble. Plus que jamais, le comité européen de la protection des données devra créer une culture commune de la protection des données parmi toutes les autorités nationales de protection des données, de manière à garantir l'interprétation cohérente des dispositions du règlement. Le règlement encourage la coopération entre les autorités de protection des données en leur donnant les moyens de coopérer de manière effective et efficace: elles seront notamment à même de mener des opérations conjointes, d'adopter des décisions d'un commun accord et de régler les éventuelles divergences d'interprétation du règlement au sein du comité au moyen d'avis et de décisions contraignantes. La Commission encourage les autorités de protection des données à faire ces changements et à ajuster leur fonctionnement, leur financement et leur culture de travail, afin de pouvoir s'acquitter des nouveaux droits et obligations.

[43] Organisme de l'UE doté de la personnalité juridique, le comité européen de la protection des données sera chargé de veiller à l'application cohérente du règlement. Il se composera du chef de chaque autorité de protection des données et du contrôleur européen de la protection des données, ou de leurs représentants.

3.3 Fourniture par les États membres des ressources financières et humaines nécessaires aux autorités nationales de protection des données

La mise en place d'autorités de contrôle pleinement indépendantes dans chaque État membre est essentielle pour assurer la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel dans l'UE[44]. Les autorités de contrôle ne peuvent toutefois véritablement préserver les libertés et les droits individuels que si elles agissent en complète indépendance. Le fait de ne pas leur accorder leur indépendance et de ne pas les laisser exercer effectivement leurs pouvoirs a une incidence très négative sur le contrôle de l'application de la législation en matière de protection des données[45].

Le règlement codifie l'obligation faite à toute autorité de protection des données d'agir en complète indépendance[46]. Il renforce l'indépendance des autorités nationales de protection des données et les dote de pouvoirs uniformes dans toute l'UE, de sorte qu'elles soient à même de traiter les réclamations de manière effective, de mener des enquêtes efficaces, de prendre des décisions contraignantes et d'infliger des sanctions effectives et dissuasives. Il leur donne aussi le pouvoir d'infliger aux responsables du traitement et aux sous-traitants des amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Les autorités de protection des données sont les interlocuteurs naturels et les premiers points de contact pour le grand public, les entreprises et les administrations publiques pour les questions relatives au règlement. Le rôle des autorités de protection des données consiste notamment à informer les responsables du traitement et les sous-traitants de leurs obligations et à favoriser la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement des données. Cela ne signifie pas pour autant que les responsables du traitement et les sous-traitants doivent attendre des autorités de protection des données qu'elles leur fournissent le type d'avis juridique sur mesure et individualisé que seul un avocat ou un délégué à la protection des données est en mesure de leur procurer.

Les autorités nationales de protection des données jouent en conséquence un rôle central, mais le relatif déséquilibre existant entre les ressources humaines et financières qui leur sont allouées dans les différents États membres peut nuire à leur efficacité et, en définitive, à la complète indépendance requise en vertu du règlement. Il peut également porter préjudice à la manière dont les autorités de protection des données sont capables d'exercer leurs pouvoirs, notamment leurs pouvoirs d'enquête. Les États membres sont encouragés à s'acquitter de leur obligation légale de procurer à leur autorité nationale de protection des données les ressources humaines, techniques et financières ainsi que les locaux et l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs[47].

3.4 Les entreprises, les administrations publiques et d'autres organisations de traitement de données doivent se préparer à l'application des nouvelles règles

---

[44] Considérant 117 et précédemment cité au considérant 62 de la directive 95/46.

[45] Communication de la Commission au Parlement européen et au Conseil - Suivi du Programme de travail pour une meilleure mise en application de la directive sur la protection des données [COM(2007) 87 final du 7 mars 2007].

[46] Article 52 du règlement.

[47] Article 52, paragraphe 4, du règlement.

Le règlement n'a pas modifié de manière substantielle les concepts et les principes fondamentaux de la législation sur la protection des données mise en place en 1995. La grande majorité des responsables du traitement et des sous-traitants, pour autant qu'ils respectent déjà la législation existante de l'UE en matière de protection des données, ne devraient donc pas avoir à apporter des modifications importantes à leurs opérations de traitement de données pour se conformer au règlement.

Le règlement a surtout une incidence sur les opérateurs dont l'activité principale est le traitement de données et/ou le traitement de données sensibles. Il influe également sur ceux qui effectuent un suivi régulier et systématique des personnes physiques à grande échelle. Ces opérateurs devront très probablement nommer un délégué à la protection des données, procéder à une analyse d'impact relative à la protection des données et notifier les violations de données s'il existe un risque pour les droits et libertés des personnes physiques. En revanche, les opérateurs, en particulier les PME, dont l'activité principale ne comprend pas de traitement à haut risque ne seront normalement pas soumis à ces obligations spécifiques du règlement.

Il est important que les responsables du traitement et les sous-traitants examinent en détail leur politique en matière de données afin de déterminer clairement les données qu'ils détiennent, à quelles fins et sur quelle base juridique (par exemple, environnement en nuage; opérateurs du secteur financier). Ils doivent également évaluer les contrats existants, en particulier ceux conclus entre responsables du traitement et sous-traitants, les possibilités de transferts internationaux et la gouvernance globale (les mesures informatiques et organisationnelles à mettre en place), y compris la nomination d'un délégué à la protection des données. Un élément essentiel de ce processus est de veiller à ce que le plus haut niveau de la direction soit associé à ces examens, apporte sa contribution et soit régulièrement tenu au courant des changements apportés à la politique de l'entreprise en matière de données et consulté à ce sujet.

À cette fin, certains opérateurs recourent à des listes de contrôle de la conformité (internes ou externes), sollicitent l'avis de sociétés de conseil et de cabinets d'avocats et cherchent des produits susceptibles de respecter les exigences propres à la protection des données dès la conception et par défaut. Chaque secteur doit définir les modalités appropriées à sa spécificité et adaptées à son modèle commercial.

Les entreprises et d'autres organisations de traitement de données pourront également tirer parti des nouveaux instruments prévus par le règlement, tels que les codes de conduite et les mécanismes de certification, en vue de démontrer le respect des obligations. Il s'agit d'approches ascendantes qui proviennent du monde des entreprises, d'associations ou d'autres organismes représentant des catégories de responsables du traitement ou de sous-traitants et qui reflètent les bonnes pratiques et les évolutions importantes dans un secteur donné ou qui peuvent apporter des informations sur le niveau de protection des données requis par certains produits et services. Le règlement prévoit un ensemble rationalisé de règles pour ces mécanismes tout en tenant compte des réalités du marché (certification par un organisme de certification ou par une autorité de protection des données, par exemple).

Toutefois, alors que les grandes entreprises se préparent activement à l'application des nouvelles règles, de nombreuses PME ne sont pas encore pleinement informées des futures règles en matière de protection des données.

En résumé, les opérateurs devraient se préparer et s'adapter à l'application des nouvelles règles et voir le règlement comme:

- une occasion de mettre de l'ordre dans leur gestion en ce qui concerne les données à caractère personnel qu'ils traitent et leur manière de les gérer;
- une obligation de concevoir des produits favorisant le respect de la vie privée et la protection des données ainsi que de construire une nouvelle relation avec leurs clients, fondée sur la transparence et la confiance; et
- une occasion de redéfinir leurs relations avec les autorités de protection des données, par l'obligation de rendre des comptes et une conformité proactive.

3.5 Informer les parties prenantes, en particulier les citoyens et les petites et moyennes entreprises

Le succès du règlement passe par une connaissance adéquate des nouvelles règles par toutes les parties concernées (le monde des entreprises et d'autres organisations de traitement de données, le secteur public et les citoyens). Au niveau national, la tâche de sensibilisation incombe en premier lieu aux autorités de protection des données, qui sont le premier point de contact pour les responsables du traitement, les sous-traitants et les personnes physiques. En tant qu'instances qui veillent au respect des règles en matière de protection des données sur leur territoire, lesdites autorités sont également les mieux placées pour expliquer les changements introduits par le règlement aux entreprises et au secteur public, ainsi que pour familiariser les citoyens avec leurs droits.

Les autorités de protection des données ont commencé à informer les parties prenantes conformément à l'approche nationale adoptée. Certaines autorités organisent des séminaires avec les administrations publiques, y compris aux niveaux régional et local, ainsi que des ateliers avec les différents secteurs d'activité afin de les sensibiliser aux principales dispositions du règlement. D'autres lancent des programmes de formation spécifiques à l'intention des délégués à la protection des données. La plupart mettent à disposition du matériel d'information en différents formats sur leur site web (listes de contrôle, vidéos, etc.).

Cependant, les citoyens ne sont pas encore suffisamment sensibilisés aux changements qu'introduisent les nouvelles règles en matière de protection des données et au renforcement des droits qu'elles apportent. Les actions de formation et de sensibilisation lancées par les autorités de protection des données devraient être poursuivies et intensifiées, une attention particulière devant être accordée aux PME. Par ailleurs, les administrations sectorielles nationales peuvent soutenir les activités des autorités de protection des données et mener leurs propres actions de sensibilisation auprès des différentes parties prenantes sur la base de leurs contributions.

4. PROCHAINES ÉTAPES

Au cours des mois à venir, la Commission continuera d'aider activement tous les acteurs à se préparer à l'application du règlement.

a) Collaboration avec les États membres

La Commission continuera de collaborer avec les États membres jusqu'en mai 2018. À compter de cette date, elle surveillera la manière dont ils appliquent les nouvelles règles et prendra au besoin les mesures appropriées.

b) Nouvelles orientations en ligne dans toutes les langues de l'UE et activités de sensibilisation

La Commission met à disposition des orientations pratiques[48] pour aider les entreprises, en particulier les PME, les autorités publiques et les citoyens à se conformer aux nouvelles règles en matière de protection des données et à en bénéficier.

Les orientations se présentent sous la forme d'un outil pratique en ligne disponible dans toutes les langues de l'UE. Cet outil sera régulièrement mis à jour et cible essentiellement trois publics: les citoyens, les entreprises (en particulier les PME) et d'autres organisations, et les administrations publiques. Il comprend des questions et des réponses sélectionnées sur la base du retour d'informations des parties prenantes, avec des exemples pratiques et des liens vers diverses sources d'information (par exemple, des articles du règlement, les lignes directrices adoptées par le groupe de travail «article 29»/le comité européen de la protection des données, ainsi que le matériel élaboré à l'échelle nationale).

La Commission mettra régulièrement l'outil à jour, en ajoutant des questions et en actualisant les réponses, sur la base du retour d'information obtenu et à la lumière des éventuelles nouvelles questions résultant de la mise en œuvre.

Les orientations seront promues au moyen d'une campagne d'information et d'activités de diffusion dans tous les États membres, ciblant les entreprises et les citoyens.

Le règlement prévoyant un renforcement des droits individuels, la Commission mènera également des actions de sensibilisation et participera à des événements dans l'ensemble des États membres pour informer les citoyens des avantages et de l'incidence du règlement.

c) Soutien financier pour des campagnes nationales et des actions de sensibilisation

La Commission soutient les efforts déployés au niveau national en matière de sensibilisation et de mise en conformité en attribuant des subventions qui peuvent servir à dispenser des formations à l'intention des autorités de protection des données, des administrations publiques, des professions juridiques et des délégués à la protection des données[49], ainsi qu'à les familiariser avec le règlement.

Quelque 1 700 000 EUR seront alloués à six bénéficiaires couvrant plus de la moitié des États membres de l'UE. Les fonds seront destinés à des pouvoirs publics locaux, y compris à des délégués à la protection des données au sein desdits pouvoirs publics, à des autorités publiques, au secteur privé, à des juges et à des avocats. Les subventions serviront à produire du matériel de formation destiné aux autorités de protection des données, aux délégués à la protection des données et à d'autres professionnels, ainsi qu'à élaborer des programmes de «formation des formateurs».

La Commission a également lancé un appel à propositions visant spécifiquement les autorités de protection des données. Il sera doté d'un budget total maximal de 2 000 000 EUR et aidera

---

[48] Ces orientations contribueront à une meilleure compréhension des règles de l'UE en matière de protection des données, mais seul le texte du règlement a force de loi. En conséquence, seul le règlement est susceptible de créer des droits et des obligations pour les personnes physiques.

[49] Subventions accordées dans le cadre du programme de financement «Droits et citoyenneté» de 2016 https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c,topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc).

lesdites autorités à nouer des contacts avec les parties prenantes[50]. L'objectif est de cofinancer à hauteur de 80 % les mesures prises par les autorités de protection des données en 2018-2019 afin de sensibiliser les entreprises, en particulier les PME, et de répondre à leurs questions. Les fonds peuvent également servir à sensibiliser le grand public.

d) Évaluation de la nécessité de faire appel aux pouvoirs conférés à la Commission

Le règlement[51] autorise la Commission à adopter des actes d'exécution ou des actes délégués pour soutenir davantage la mise en œuvre des nouvelles règles. La Commission ne fera usage de ces pouvoirs que s'ils apportent une valeur ajoutée clairement démontrée et sur la base du retour d'informations des parties prenantes. En particulier, elle examinera la question de la certification sur la base d'une étude réalisée par des experts externes ainsi que des contributions et des conseils du groupe multipartite sur le règlement mis en place fin 2017. Les travaux effectués par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) dans le domaine de la cybersécurité seront aussi pertinents dans ce contexte.

e) Intégration du règlement dans l'accord EEE

La Commission poursuivra ses travaux avec les trois États de l'AELE membres de l'Espace économique européen (EEE - Islande, Liechtenstein et Norvège) en vue d'intégrer le règlement dans l'accord EEE[52]. Ce n'est que lorsque l'intégration du règlement dans l'accord EEE sera en vigueur que les données à caractère personnel pourront circuler librement entre les pays de l'UE et de l'EEE de la même manière qu'entre les États membres de l'UE.

f) Retrait du Royaume-Uni de l'UE

Dans le cadre des négociations entre l'UE et le Royaume-Uni sur l'accord de retrait du Royaume-Uni conformément à l'article 50 du traité sur l'Union européenne, la Commission poursuivra l'objectif visant à faire en sorte que les dispositions du droit de l'Union sur la protection des données à caractère personnel applicables le jour précédant la date du retrait continuent de s'appliquer aux données à caractère personnel au Royaume-Uni traitées avant la date du retrait[53]. Par exemple, les personnes concernées devraient continuer à avoir le droit d'être informées, le droit d'accès aux données, le droit de rectification, le droit d'effacement, le droit à la limitation du traitement, le droit à la portabilité des données ainsi que le droit de s'opposer au traitement de données et le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, sur la base des dispositions pertinentes du droit

---

[50] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html

[51] Acte délégué adopté aux fins de déterminer les informations à présenter sous la forme d'icônes ainsi que les procédures régissant la fourniture d'icônes normalisées (article 12, paragraphe 8, du règlement); acte délégué adopté aux fins de préciser les exigences à prendre en considération en ce qui concerne le mécanismes de certification (article 43, paragraphe 8, du règlement); acte d'exécution visant à fixer des normes techniques pour les mécanismes de certification, les labels et les marques en matière de protection des données, ainsi que les mécanismes aux fins de la promotion et de la reconnaissance de ces mécanismes de certification, labels et marques (article 43, paragraphe 9, du règlement); acte d'exécution visant à préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent (article 47, paragraphe 3, du règlement); acte d'exécution visant à préciser la forme et les procédures de l'assistance mutuelle ainsi que les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle (article 61, paragraphe 9, et article 67 du règlement).

[52] Pour en savoir plus sur l'état d'avancement des travaux, voir http://www.efta.int/eea-lex/32016R0679.

[53] https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en

de l'Union applicables à la date du retrait. Les données à caractère personnel susmentionnées devraient être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles ont été traitées.

À compter de la date du retrait, et sous réserve des dispositions transitoires qui pourraient figurer dans un éventuel accord de retrait, les dispositions du règlement relatives aux transferts de données à caractère personnel vers des pays tiers s'appliqueront au Royaume-Uni[54].

g) Bilan en mai 2019

Après le 25 mai 2018, la Commission suivra de près l'application des nouvelles règles et se tiendra prête à prendre des mesures en cas de problème majeur. Un an après l'entrée en vigueur du règlement (2019), la Commission organisera un événement pour dresser le bilan de l'expérience des différentes parties prenantes en ce qui concerne sa mise en œuvre. Cela sera également intégré dans le rapport sur l'évaluation et le réexamen du règlement que la Commission est tenue d'élaborer pour le mois de mai 2020. Ce rapport portera en particulier sur les transferts internationaux et les dispositions relatives à la coopération et à la cohérence qui s'appliquent aux autorités de protection des données.

Conclusion

Le 25 mai, un nouvel ensemble unique de règles en matière de protection des données entrera en vigueur dans toute l'UE. Ce nouveau cadre procurera des avantages importants aux citoyens, aux entreprises, aux administrations publiques et à d'autres organisations similaires. C'est également l'occasion pour l'UE de devenir un acteur de premier plan au niveau mondial en matière de protection des données à caractère personnel. Toutefois, cette réforme ne sera couronnée de succès que si tous les acteurs concernés s'acquittent de leurs droits et de leurs obligations.

Depuis l'adoption du règlement en mai 2016, la Commission a collaboré activement avec tous les acteurs concernés (gouvernements, autorités nationales, entreprises, société civile) en vue de l'application des nouvelles règles. Un travail important a été accompli pour garantir une large sensibilisation et une préparation complète, mais il reste encore du chemin à parcourir. Les préparatifs progressent à un rythme différent d'un État membre à l'autre et en fonction des divers acteurs. En outre, la connaissance des possibilités et des avantages liés aux nouvelles règles n'est pas répartie de manière uniforme. Il est nécessaire en particulier de renforcer la sensibilisation et d'accompagner les efforts de mise en conformité pour les PME.

En conséquence, la Commission invite tous les acteurs concernés à intensifier les travaux en cours en vue de garantir une application et une interprétation cohérentes des nouvelles règles dans toute l'UE et de sensibiliser tant les entreprises que les citoyens. La Commission appuiera ces efforts au moyen d'un financement et d'un soutien administratif et contribuera à sensibiliser l'opinion publique, notamment en publiant des orientations sous la forme d'une boîte à outil en ligne.

---

[54] Voir la communication de la Commission aux parties prenantes: retrait du Royaume-Uni et règles de l'UE dans le domaine de la protection des données (Commission Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection, http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

Les données acquièrent une grande valeur dans l'économie d'aujourd'hui et sont essentielles dans la vie quotidienne des citoyens. Les nouvelles règles offrent une occasion unique aux entreprises comme aux citoyens. Les entreprises, en particulier les plus petites, pourront bénéficier de cet ensemble unique de règles favorables à l'innovation et mettre de l'ordre dans leur gestion concernant les données à caractère personnel afin de rétablir la confiance des consommateurs et d'en tirer un avantage compétitif dans l'ensemble de l'UE. Les citoyens pourront bénéficier d'une protection accrue des données à caractère personnel et mieux contrôler la manière dont les données sont traitées par les entreprises.

Dans un monde moderne à l'économie numérique en plein essor, l'Union européenne, ses citoyens et ses entreprises doivent être pleinement équipés pour profiter des avantages de l'économie des données et en comprendre les conséquences. Le nouveau règlement offre les outils nécessaires pour adapter l'Europe au 21e siècle.

La Commission entreprendra les actions suivantes:

À l'égard des États membres

- La Commission continuera de coopérer avec les États membres pour promouvoir la cohérence et limiter la fragmentation dans l'application du règlement, en tenant compte de la marge dont disposent les États membres pour apporter des précisions en vertu de la nouvelle législation.

- Après le mois de mai 2018, la Commission suivra de près l'application du règlement dans les États membres et prendra, au besoin, les mesures appropriées, dont le recours aux procédures d'infraction.

À l'égard des autorités de protection des données

- Jusqu'en mai 2018, la Commission appuiera les travaux des autorités de protection des données dans le cadre du groupe de travail «article 29» et du passage de relais au futur comité européen de la protection des données; après cette date, elle contribuera aux travaux dudit comité.

- En 2018-2019, la Commission cofinancera (budget total pouvant atteindre 2 000 000 EUR au maximum) des actions de sensibilisation menées par les autorités de protection des données au niveau national (projets mis en œuvre à partir de la mi-2018).

À l'égard des parties prenantes

- La Commission publiera des orientations sous la forme d'une boîte à outils en ligne, comportant des questions et des réponses à l'intention des citoyens, des entreprises et des administrations publiques. La Commission entend en faire la promotion auprès des publics cibles par l'intermédiaire d'une campagne d'information en faveur des entreprises et du grand public d'ici au mois de mai 2018 et après cette date.

- En 2018 et au-delà, la Commission continuera à coopérer activement avec les parties prenantes, notamment dans le cadre du groupe multipartite sur la mise en œuvre du règlement et le niveau de sensibilisation aux nouvelles règles.

À l'égard de l'ensemble des acteurs

- En 2018-2019, la Commission évaluera la nécessité de faire usage du pouvoir qui lui est conféré d'adopter des actes délégués ou des actes d'exécution.

- En mai 2019, elle fera le point sur la mise en œuvre du règlement et fera rapport sur l'application des nouvelles règles en 2020.