Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	2012/0011(COD)	Procédure terminée

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Abrogation Directive 95/46/EC 1990/0287(COD)
Voir aussi Directive 2002/58/EC 2000/0189(COD)
Voir aussi 2012/0010(COD)
Voir aussi 2023/0202(COD)

Sujet
1.20.09 Protection de la vie privée et des données
2.80 Coopération et simplification administratives
3.45.05 Politique de l'entreprise, commerce électronique, service après-vente, distribution
4.60.06 Intérêts économiques et juridiques du consommateur

Acteurs principaux

Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	LIBE Libertés civiles, justice et affaires intérieures		12/04/2012
		Verts/ALE ALBRECHT Jan Philipp	
		Rapporteur(e) fictif/fictive	
		PPE VOSS Axel	
		S&D LAURISTIN Marju	
		ALDE IN 'T VELD Sophia	
		ECR KIRKHOPE Timothy	
		EFD WINBERG Kristina	
	Commission au fond précédente		
	LIBE Libertés civiles, justice et affaires intérieures		12/04/2012
		Verts/ALE ALBRECHT Jan Philipp	
	Commission pour avis précédente		
	ITRE Industrie, recherche et énergie		14/03/2012
		PPE KELLY Seán	
	JURI Affaires juridiques		14/06/2012
		PPE BOULLIER GALLO Marielle	
	IMCO Marché intérieur et protection des consommateurs		29/02/2012
		PPE COMI Lara	
	EMPL Emploi et affaires sociales		20/04/2012
		ALDE HIRSCH Nadja	

	ECON Affaires économiques et monétaires	La commission a décidé de ne pas donner d'avis.	
Conseil de l'Union européenne	Formation du Conseil	Réunion	Date
	Affaires économiques et financières ECOFIN	3445	12/02/2016
	Justice et affaires intérieures(JAI)	3415	09/10/2015
	Justice et affaires intérieures(JAI)	3354	04/12/2014
	Justice et affaires intérieures(JAI)	3336	10/10/2014
	Justice et affaires intérieures(JAI)	3298	03/03/2014
	Justice et affaires intérieures(JAI)	3279	06/12/2013
	Justice et affaires intérieures(JAI)	3260	07/10/2013
	Justice et affaires intérieures(JAI)	3244	06/06/2013
	Justice et affaires intérieures(JAI)	3195	25/10/2012
Commission européenne	DG de la Commission	Commissaire	
	Justice et consommateurs	REDING Viviane	
Comité économique et social européen			

Evénements clés

25/01/2012	Publication de la proposition législative	COM(2012)0011	Résumé
16/02/2012	Annonce en plénière de la saisine de la commission, 1ère lecture		
25/10/2012	Débat au Conseil	3195	Résumé
06/06/2013	Débat au Conseil	3244	
07/10/2013	Débat au Conseil	3260	Résumé
21/10/2013	Vote en commission,1ère lecture		
22/11/2013	Dépôt du rapport de la commission, 1ère lecture	A7-0402/2013	Résumé
06/12/2013	Débat au Conseil	3279	Résumé
03/03/2014	Débat au Conseil	3298	
11/03/2014	Débat en plénière		
12/03/2014	Résultat du vote au parlement		
12/03/2014	Décision du Parlement, 1ère lecture	T7-0212/2014	Résumé
03/09/2014	Ouverture des négociations interinstitutionnelles après 1ère lecture par la commission parlementaire		
10/10/2014	Débat au Conseil	3336	Résumé
04/12/2014	Débat au Conseil	3354	Résumé
17/12/2015	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture		

07/04/2016	Publication de la position du Conseil	05419/1/2016	Résumé
11/04/2016	Annonce en plénière de la saisine de la commission, 2ème lecture		
12/04/2016	Vote en commission, 2ème lecture		
12/04/2016	Dépôt de la recommandation de la commission, 2ème lecture	A8-0139/2016	Résumé
13/04/2016	Débat en plénière		
14/04/2016	Décision du Parlement, 2ème lecture	T8-0125/2016	Résumé
27/04/2016	Signature de l'acte final		
27/04/2016	Fin de la procédure au Parlement		
04/05/2016	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de procédure	2012/0011(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Règlement
	Abrogation Directive 95/46/EC 1990/0287(COD) Voir aussi Directive 2002/58/EC 2000/0189(COD) Voir aussi 2012/0010(COD) Voir aussi 2023/0202(COD)
Base juridique	Traité sur le fonctionnement de l'UE TFEU 016-p2; Traité sur le fonctionnement de l'UE TFEU 114-p1
Autre base juridique	Règlement du Parlement EP 159
Consultation obligatoire d'autres institutions	Comité économique et social européen
Etape de la procédure	Procédure terminée
Dossier de la commission parlementaire	LIBE/8/03708

Portail de documentation

Document de base législatif		COM(2012)0011	25/01/2012	EC	Résumé
Document annexé à la procédure		SEC(2012)0072	25/01/2012	EC	
Document annexé à la procédure		SEC(2012)0073	25/01/2012	EC	
Document annexé à la procédure		N7-0083/2012 JO C 192 30.06.2012, p. 0007	07/03/2012	EDPS	Résumé
Comité économique et social: avis, rapport		CES1303/2012	23/05/2012	ESC	
Projet de rapport de la commission		PE501.927	16/01/2013	EP	
Avis de la commission	IMCO	PE496.497	28/01/2013	EP	
Avis de la commission	ITRE	PE496.562	26/02/2013	EP	
Avis de la commission	EMPL	PE498.045	04/03/2013	EP	

Amendements déposés en commission		PE504.340	04/03/2013	EP	
Amendements déposés en commission		PE506.145	04/03/2013	EP	
Amendements déposés en commission		PE506.146	04/03/2013	EP	
Amendements déposés en commission		PE506.147	06/03/2013	EP	
Amendements déposés en commission		PE506.164	06/03/2013	EP	
Amendements déposés en commission		PE506.166	06/03/2013	EP	
Amendements déposés en commission		PE506.168	06/03/2013	EP	
Amendements déposés en commission		PE506.170	06/03/2013	EP	
Amendements déposés en commission		PE506.173	08/03/2013	EP	
Amendements déposés en commission		PE506.169	13/03/2013	EP	
Avis de la commission	JURI	PE494.710	25/03/2013	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A7-0402/2013	22/11/2013	EP	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T7-0212/2014	12/03/2014	EP	Résumé
Réaction de la Commission sur le texte adopté en plénière		SP(2014)455	10/06/2014	EC	
Document annexé à la procédure		52015XX0912(01) JO C 301 12.09.2015, p. 0001	27/07/2015	EDPS	Résumé
Projet de rapport de la commission		PE580.501	04/04/2016	EP	
Position du Conseil		05419/1/2016	08/04/2016	CSL	Résumé
Communication de la Commission sur la position du Conseil		COM(2016)0214	11/04/2016	EC	Résumé
Recommandation déposée de la commission, 2e lecture		A8-0139/2016	12/04/2016	EP	Résumé
Texte adopté du Parlement, 2ème lecture		T8-0125/2016	14/04/2016	EP	Résumé
Projet d'acte final		00017/2016/LEX	27/04/2016	CSL	
Document annexé à la procédure		COM(2018)0043	24/01/2018	EC	
Document de suivi		COM(2020)0264	24/06/2020	EC	
Document de suivi		SWD(2020)0115	25/06/2020	EC	

Informations complémentaires

Parlements nationaux	IPEX
Commission européenne	EUR-Lex

Acte final

Règlement 2016/679
JO L 119 04.05.2016, p. 0001 Résumé

Rectificatif à l'acte final 32016R0679R(02)
JO L 127 23.05.2018, p. 0002

Acte législatif final contenant des dispositions relatives aux actes délégués

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

OBJECTIF : protéger les droits et libertés fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel, et garantir la libre circulation de ces dernières au sein de lUnion.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

CONTEXTE : la pièce maîtresse de la législation de lUE en matière de protection des données à caractère personnel, à savoir la directive 95/46/CE, poursuivait deux objectifs : protéger le droit fondamental à la protection des données et garantir la libre circulation des données à caractère personnel entre les États membres. Elle a été complétée par la décision-cadre 2008/977/JAI destinée à protéger les données à caractère personnel dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale.

Sil demeure satisfaisant en ce qui concerne ses objectifs et ses principes, le cadre juridique actuel n'a cependant pas permis déviter une fragmentation de la mise en uvre de la protection des données à caractère personnel dans l'Union, une insécurité juridique et le sentiment, largement répandu dans le public, que des risques importants subsistent, notamment dans lenvironnement en ligne. C'est pourquoi lUnion doit se doter dun cadre juridique plus solide en matière de protection des données, assorti dune application rigoureuse des règles, afin de permettre à l'économie numérique de se développer sur tout le marché intérieur.

La protection des données à caractère personnel joue un rôle crucial dans la stratégie numérique pour l'Europe et, plus généralement, dans la stratégie Europe 2020.

L'article 16, paragraphe 1, du traité sur le fonctionnement de lUnion européenne (TFUE), introduit par le traité de Lisbonne, établit le principe selon lequel toute personne a droit à la protection des données à caractère personnel la concernant.

- En 2010, le Conseil européen a invité la Commission à évaluer le fonctionnement des instruments de l'UE relatifs à la protection des données et à présenter, si besoin est, de nouvelles initiatives législatives et non législatives.
- Dans son plan d'action mettant en uvre le programme de Stockholm, la Commission insistait sur la nécessité de veiller à ce que le droit fondamental à la protection des données à caractère personnel soit appliqué systématiquement dans le cadre de toutes les politiques européennes. Dans sa communication intitulée «Une approche globale de la protection des données à caractère personnel dans lUnion européenne», elle a conclu que lUE avait besoin dune politique plus globale et plus cohérente à légard du droit fondamental à la protection des données à caractère personnel.
- Par résolution du 6 juillet 2011, le Parlement européen a adopté une résolution qui appuyait l'approche de la Commission quant à la réforme du cadre législatif régissant la protection des données.

La présente proposition sinscrit dans le nouveau cadre juridique envisagé pour la protection des données à caractère personnel dans l'Union européenne, qui est décrit dans sa communication sur ce sujet. Ce nouveau cadre juridique se compose de deux propositions législatives:

- la présente proposition de règlement relatif à la protection des personnes physiques à légard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), et
- une proposition de directive relative à la protection des personnes physiques à légard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, denquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

ANALYSE DIMPACT : cette analyse reposait sur trois objectifs, à savoir: 1) renforcer la dimension «marché intérieur» de la protection des données, 2) rendre lexercice du droit à la protection des données par les personnes physiques plus effectif et 3) instaurer un cadre global et cohérent couvrant tous les domaines de compétence de lUnion, y compris la coopération policière et la coopération judiciaire en matière pénale.

Trois options, prévoyant un degré dintervention variable, ont été évaluées:

- Option 1 : apporter un minimum de modifications législatives et recourir à des communications interprétatives et à des mesures de soutien telles que des programmes de financement et des instruments techniques ;
- Option 2 : celle-ci consistait en un ensemble de dispositions législatives répondant à chacun des problèmes mis en évidence dans l'analyse ;
- Option 3 : prévoir la centralisation de la protection des données au niveau de lUE grâce à ladoption de règles précises et détaillées pour tous les secteurs et à la création d'une agence européenne chargée de surveiller et de contrôler l'application des dispositions.

Loption privilégiée qui est fondée sur la deuxième option, en y associant quelques éléments des deux autres, devrait permettre, entre autres : i) daccroître la sécurité juridique pour les responsables du traitement des données et les citoyens, ii) de réduire la charge administrative, iii) dharmoniser lapplication des règles en matière de protection des données dans lUnion, iv) de renforcer lexercice effectif par les personnes physiques de leur droit à la protection des données les concernant au sein de lUE et v) daméliorer lefficacité de la surveillance et du contrôle de lapplication des règles en la matière.

BASE JURIDIQUE : article 16, paragraphe 2, et son article 114, paragraphe 1, du traité sur le fonctionnement de lUnion européenne.

CONTENU : le règlement proposé vise à établir des règles relatives à la protection des personnes physiques à légard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. Ses principales dispositions sont les suivantes :

Principes : la proposition énonce les principes relatifs au traitement des données à caractère personnel. Des éléments nouveaux ont été ajoutés, tels que le principe de transparence, des éclaircissements concernant le principe de minimisation des données et linstauration d'une responsabilité globale du responsable du traitement. En outre, elle définit les critères de licéité du traitement, précise les conditions auxquelles le consentement peut valablement fonder un traitement licite, et fixe dautres conditions de licéité pour le traitement des données à caractère personnel relatives aux enfants, en ce qui concerne les services de la société de linformation qui sont directement proposés à ces derniers.

Droits de la personne concernée : la proposition introduit l'obligation, pour les responsables du traitement, de fournir des informations transparentes, facilement accessibles et intelligibles. Elle oblige le responsable du traitement à prévoir des procédures et des mécanismes permettant à la personne concernée dexercer ses droits. Elle précise les informations que le responsable du traitement est tenu de fournir et en ajoute de nouvelles, notamment la durée de conservation, le droit dintroduire une réclamation, les transferts internationaux et la source des données.

En outre, la proposition confère :

- un droit d'accès aux données à caractère personnel, en y ajoutant de nouveaux éléments tels que lobligation dinformer les personnes concernées de la durée de conservation, de leur droit à rectification et à l'effacement et de leur droit de réclamation ;
- un droit à loubli numérique tout en précisant le droit deffacement prévu à la directive 95/46/CE ;
- un nouveau droit, le droit à la portabilité des données, cest-à-dire celui de transmettre des données dun système de traitement automatisé à un autre, sans que le responsable du traitement ne puisse y faire obstacle ;
- un droit dopposition tout en traitant du droit de la personne concernée de ne pas être soumise à une mesure fondée sur le profilage.

Responsable du traitement : la proposition tient compte du débat sur un «principe de responsabilité» et décrit en détail les obligations incombant au responsable du traitement pour se conformer au règlement et en apporter la preuve, notamment par l'adoption de règles internes et de mécanismes à cet effet. Elle introduit, pour les responsables du traitement et les sous-traitants, lobligation : i) de conserver une trace documentaire des opérations de traitement sous leur responsabilité ; ii) de notifier les violations de données à caractère personnel ; iii) de mettre en uvre les mesures appropriées pour assurer la sécurité du traitement ; iv) deffectuer une analyse dimpact relative à la protection des données préalablement aux traitements présentant des risques.

La proposition introduit en outre lobligation de désigner un délégué à la protection des données pour le secteur public et, dans le secteur privé, pour les grandes entreprises, ou lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui exigent un suivi régulier et systématique.

Transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale : la proposition définit les critères, conditions et procédures d'adoption d'une décision de la Commission constatant un niveau de protection adéquat. Les critères devant être pris en compte par la Commission incluent expressément lÉtat de droit, l'existence d'un droit de recours judiciaire et un contrôle indépendant.

La proposition subordonne également les transferts vers des pays tiers pour lesquels la Commission na pas adopté de décision constatant un niveau de protection adéquat, à la présentation de garanties appropriées, notamment des clauses types de protection des données, des règles d'entreprise contraignantes et des clauses contractuelles.

Autorités de contrôle indépendantes : la proposition fait obligation aux États membres de mettre en place une ou plusieurs autorités de contrôle, et d'élargir la mission de celles-ci à la coopération entre elles et avec la Commission. Elle clarifie les conditions garantissant l'indépendance des autorités de contrôle, en application de la jurisprudence de la Cour de justice de l'Union européenne.

Coopération et cohérence : la proposition instaure des règles explicites en matière d'assistance mutuelle obligatoire et prévoit notamment les conséquences en cas de refus de se conformer à la demande dune autre autorité de contrôle. Elle met en place un mécanisme de contrôle de la cohérence, en vue d'assurer une application uniforme des règles lorsqu'il s'agit de traitements qui peuvent viser des personnes concernées dans plusieurs États membres.

En outre, elle institue le comité européen de la protection des données, composé des directeurs des autorités de contrôle de tous les États membres et du contrôleur européen à la protection des données, en remplacement du groupe de protection des personnes à l'égard du traitement des données à caractère personnel créé par l'article 29 de la directive 95/46/CE.

Voies de recours et sanctions : la proposition : i) prévoit le droit de toute personne concernée de déposer une réclamation auprès d'une autorité de contrôle ; ii) précise les organismes ou associations habilités à déposer une réclamation au nom de la personne concernée ou, en cas de violation de données à caractère personnel, indépendamment de toute réclamation introduite par une personne concernée ; iii) étend le droit à réparation aux dommages causés par les sous-traitants ; iv) clarifie la responsabilité des responsables conjoints du traitement et des sous-traitants ; v) oblige les États membres à définir les sanctions pénales applicables aux infractions aux dispositions du règlement.

INCIDENCE BUDGÉTAIRE : les incidences budgétaires spécifiques de la proposition concernent les missions dévolues au contrôleur européen de la protection des données. Ces incidences nécessitent une reprogrammation de la rubrique 5 du cadre financier. Le total des crédits est estimé à 24,339 millions EUR pour la période 2014-2020. La proposition n'a pas d'incidence sur les dépenses de fonctionnement.

ACTES DÉLÉGUÉS : la proposition contient des dispositions habilitant la Commission à adopter des actes délégués conformément à larticle 290 du traité sur le fonctionnement de lUnion européenne.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

AVIS du contrôleur européen de la protection des données (CEPD) sur le paquet de mesures pour une réforme de la protection des données.

Le 25 janvier 2012, la Commission a adopté un paquet de mesures visant à réformer le cadre européen de protection des données incluant :

- la présente proposition de règlement contenant des règles générales de protection des données et
- une proposition de directive sur la protection des données dans le secteur répressif.

Le règlement : le CEPD accueille favorablement la proposition de règlement car elle constitue un grand pas en avant pour le droit à la protection des données en Europe. Les règles proposées renforceront les droits des individus et responsabiliseront davantage les responsables du traitement quant à la manière de traiter les données personnelles. En outre, le rôle et les pouvoirs des autorités nationales de contrôle (séparément et conjointement) se verront réellement renforcés.

Le CEPD salue le fait que linstrument proposé soit un règlement. Ce dernier sera directement applicable dans les États membres et mettra fin à de nombreuses complexités et incohérences découlant des différentes mesures dexécution des États membres actuellement en place.

La directive : le CEPD est extrêmement déçu par la proposition de directive pour la protection des données en matière pénale. Il regrette que la Commission ait choisi de réglementer la question dans un instrument autonome qui offre un niveau de protection inadéquat, très inférieur à la proposition de règlement.

Un élément positif de la proposition de directive est le fait quelle couvre le traitement national et a dès lors un champ dapplication plus large que lactuelle décision-cadre. Toutefois, cet élargissement noffre de plus-value que si la directive renforce substantiellement le niveau de protection des données dans ce domaine, ce qui nest pas le cas.

La principale faiblesse de lensemble du paquet tient au fait quil ne remédie pas à labsence dune approche globale des règles de lUE en matière de protection des données:

- il ne produit aucun effet sur de nombreux instruments de lUE en matière de protection des données, tels que les règles de protection des données pour les institutions et organes de lUE, mais aussi tous les instruments spécifiques adoptés dans le domaine de la coopération policière et judiciaire en matière pénale, tels que la décision de Prüm et les règles relatives à Europol et Eurojust ;
- les deux instruments proposés considérés conjointement ne traitent pas complètement des situations de fait qui relèvent des deux domaines de politique, telles que lutilisation des données PNR ou de télécommunications à des fins répressives.

Commentaires généraux sur la proposition de règlement : le CEPD formule les observations suivantes :

1°) La relation entre le droit européen et le droit national : la proposition de règlement tend largement à la création dun seul droit applicable pour la protection des données dans lUE, il reste cependant davantage de place pour la coexistence et linteraction entre le droit de lUE et le droit national que lon ne pourrait le croire à première vue. Le CEPD est d'avis que le législateur devrait mieux le reconnaître.

2°) De nombreuses dispositions habilitent la Commission à adopter des actes délégués ou d'exécution : le CEPD accueille favorablement cette approche dans la mesure où elle contribue à l'application cohérente du règlement mais émet des réserves quant à la portée des délégations qui concernent des dispositions essentielles. Il estime que plusieurs de ces habilitations devraient être reconsidérées.

3°) Éléments positifs et négatifs : sur un plan détaillé, le CEPD souligne les principaux éléments positifs de la proposition de règlement qui sont:

- la clarification du champ dapplication de la proposition de règlement;
- les exigences de transparence accrue envers la personne concernée et le renforcement du droit dopposition;
- lobligation générale pour les responsables du traitement de veiller à, et dêtre capables de démontrer la conformité aux dispositions du règlement;
- le renforcement de la position et du rôle des autorités de surveillance nationales;
- les principales lignes du mécanisme de contrôle de la cohérence.

Les principaux éléments négatifs de la proposition de règlement sont:

- les nouvelles exceptions au principe de limitation de la finalité;
- les possibilités de restreindre les principes et droits de base;
- lobligation pour les responsables du traitement de conserver la documentation de toutes les opérations de traitement;
- le transfert de données vers des pays tiers par voie de dérogation;
- le rôle de la Commission dans le mécanisme destiné à garantir la cohérence;
- la nature obligatoire de limposition de sanctions administratives.

Commentaires généraux sur la proposition de directive : le CEPD est d'avis que la proposition, dans de nombreux aspects, ne rencontre pas les exigences d'un niveau de protection des données élevé et cohérent. Elle laisse inchangés tous les instruments existants dans le domaine et dans de nombreux cas, les déviations par rapport aux règles établies dans la proposition de règlement ne sont pas du tout justifiés.

Le CEPD souligne que si le domaine répressif exige certaines règles spécifiques, toute déviation des règles générales relatives à la protection des données doit être dûment justifiée, sur la base dun équilibre approprié entre lintérêt général dans le contexte répressif et les droits fondamentaux des citoyens.

Le CEPD est en particulier préoccupé par:

- le manque de clarté dans la rédaction du principe de limitation de la finalité;
- labsence dune obligation pour les autorités compétentes de démontrer la conformité avec la directive;
- les conditions insuffisantes pour les transferts vers des pays tiers;
- les pouvoirs indûment limités des autorités de contrôle.

Le CEPD formule les recommandations suivantes sur l'ensemble du processus de la réforme:

- annoncer publiquement le calendrier portant sur la deuxième phase du processus de réforme dans les plus brefs délais;
- incorporer les règles pour les institutions et organes européens dans la proposition de règlement ou, à tout le moins, veiller à ce que les règles soient en adéquation avec, et entrent en vigueur lors de lapplication de la proposition de règlement;
- présenter dans les plus brefs délais une proposition pour des règles communes pour la politique étrangère et de sécurité commune, fondées sur larticle 39 du traité UE.

Le CEPD formule également une série de recommandations détaillées tant sur la proposition de règlement que sur la proposition de directive.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Conseil a pris note de l'avancement des travaux relatifs à la proposition de règlement 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 (règlement général sur la protection des données).

La question du type d'instrument juridique choisi a été soulevée au cours du débat. Certaines délégations ont exprimé une préférence pour une directive au lieu d'un règlement, car la première autorise davantage de souplesse lorsque cela est nécessaire. Toutefois, quelques autres délégations se sont prononcées en faveur d'un règlement, conformément à la proposition de la Commission.

Les ministres avaient déjà discuté de cette proposition lors de la réunion ministérielle informelle de juillet 2012 sur la base d'un questionnaire portant sur les trois points suivants: la charge administrative, la nécessité de prévoir un traitement particulier pour le secteur public et le nombre d'actes délégués.

Cette proposition fait l'objet de travaux approfondis des experts au sein du groupe "Protection des données", qui ont commencé sous présidence danoise et continueront sous présidence irlandaise.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Conseil a tenu un débat approfondi sur la proposition en objet.

Pour rappel, en 2012, la Commission européenne a présenté un ensemble de mesures législatives destiné à actualiser et moderniser les principes de la protection des données :

- le présent projet de règlement 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 (règlement général sur la protection des données) ;
- la proposition de directive relative à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ainsi que d'activités judiciaires connexes.

Le principe du guichet unique est, avec le mécanisme de contrôle de la cohérence, l'un des aspects essentiels de la proposition de la Commission. Selon ce principe, lorsque le traitement de données à caractère personnel a lieu dans plusieurs États membres, il conviendrait qu'une seule autorité de contrôle soit compétente pour surveiller les activités du responsable du traitement ou du sous-traitant dans toute l'Union et pour prendre les décisions y afférentes.

La proposition prévoit que l'autorité compétente faisant ainsi office de guichet unique soit l'autorité de contrôle de l'État membre dans lequel le responsable du traitement ou le sous-traitant a son principal établissement.

Le Conseil a exprimé son soutien en faveur du principe selon lequel, dans des affaires transnationales importantes, le règlement devrait établir un mécanisme de guichet unique afin de parvenir à une décision de contrôle unique; celle-ci devrait être prise rapidement, assurer une application cohérente, garantir la sécurité juridique et réduire la charge administrative. Cela permettrait daméliorer l'efficacité par rapport aux coûts des règles en matière de protection des données pour les entreprises internationales, et contribuer ainsi à la croissance de l'économie numérique.

Le débat a principalement porté sur la manière de parvenir à une telle décision unique. Une majorité des États membres a indiqué que les travaux au niveau des experts devraient se poursuivre en vue d'élaborer un modèle selon lequel une décision de contrôle unique devrait être prise par l'autorité de contrôle de «l'établissement principal», le pouvoir exclusif de cette autorité pouvant être limité à l'exercice de certaines compétences.

Certains États membres ont exprimé une préférence pour le mécanisme de codécision, tandis que d'autres ont préféré, à ce stade, éviter de se prononcer sur ce point.

Le Conseil a indiqué que les experts devraient réfléchir à des méthodes permettant de renforcer la proximité entre les individus et l'autorité de contrôle décisionnaire en associant les autorités de contrôle "locales" au processus décisionnel. Cette proximité constitue en effet un aspect important de la protection des droits individuels.

Enfin, un autre élément important pouvant contribuer à favoriser une application cohérente des règles de l'UE en matière de protection des données consisterait à réfléchir aux pouvoirs et au rôle qui pourraient être confiés au comité européen de la protection des données.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

La commission des libertés civiles, de la justice et des affaires intérieures a adopté le rapport de Jan Philipp ALBRECHT (Verts/ALE, DE) sur la 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 et à la libre circulation de ces données (règlement général sur la protection des données).

La commission parlementaire a recommandé que la position du Parlement européen adoptée en première lecture suivant la procédure législative ordinaire modifie la proposition de la Commission comme suit.

Champ d'application territorial : les députés ont précisé que le règlement devrait également s'appliquer à un responsable du traitement qui n'est pas établi dans l'Union lorsque les activités de traitement sont liées à l'offre de biens ou de services à des personnes concernées dans l'Union, que ces biens ou services fassent l'objet d'un paiement ou non, ou à l'observation du comportement de ces personnes

Conditions de consentement : lorsque le traitement des données est basé sur le consentement, le rapport a confirmé que la charge de prouver que la personne concernée a consenti au traitement de ses données à caractère personnel à des fins déterminées doit incomber au responsable du traitement. Les députés ont ajouté que :

- les dispositions relatives au consentement de la personne concernée qui enfreignent partiellement le règlement seraient entièrement nulles ;
- il devrait être aussi simple de retirer son consentement que de le donner ; la personne concernée devrait être informée par le responsable du traitement si le retrait du consentement peut entraîner la cessation de la fourniture des services ou de la relation avec

le responsable du traitement ;
- le consentement serait lié à la finalité et deviendrait caduc lorsque cette finalité n'existe plus ou dès que le traitement des données à caractère personnel n'est plus nécessaire pour la réalisation de la finalité pour laquelle elles ont été initialement collectées.

Les informations fournies aux enfants, aux parents et aux tuteurs légaux, y compris en ce qui concerne la collecte et l'utilisation des données par le responsable du traitement, devraient être communiquées dans des termes clairs adaptés au public visé.

Droit à loubli numérique : les députés ont renforcé ce droit dans la mesure ou la personne concernée pourrait obtenir de tiers l'effacement de tous les liens vers les données à caractère personnel diffusées, ou de toute copie ou reproduction de celles-ci, pour l'un des motifs suivants:

- un tribunal ou une autorité réglementaire basé(e) dans l'Union a jugé que les données concernées doivent être effacées et cette décision a acquis force de chose jugée;
- les données ont fait l'objet d'un traitement illicite.

Le responsable du traitement et, le cas échant, le tiers devraient procéder à l'effacement sans délai, sauf lorsque la conservation des données à caractère personnel est nécessaire à certaines fins.

Obligation de notifier les rectifications et les effacements : le responsable du traitement devrait communiquer à chaque destinataire à qui les données ont été transférées toute rectification ou tout effacement effectué, à moins qu'une telle communication se révèle impossible ou suppose un effort disproportionné. Le responsable devrait informer la personne concernée de ces destinataires si celle-ci en fait la demande.

Politiques d'information normalisées : les députés ont introduit un nouvel article stipulant que lorsque des données relatives à une personne concernée sont collectées, le responsable du traitement devrait informer la personne concernée dune série éléments avant de fournir les informations requises par le règlement.

Ces éléments dinformation porteraient sur la question de savoir si les données : i) sont collectées et conservées ou non au-delà du minimum nécessaire pour chaque objectif spécifique du traitement; ii) sont traitées ou non à des fins autres que celles de leur collecte; iii) sont divulguées à des tiers commerciaux, vendues ou louées; iv) sont conservées ou non sous forme cryptée.

Par la suite, le responsable du traitement devrait également fournir des informations relatives à la sécurité et au traitement des données, le cas échéant, des informations relatives à l'existence d'un profilage, des informations intelligibles relatives à la logique qui sous-tend tout traitement automatisé, ainsi que des informations indiquant si les données ont été fournies aux autorités publiques au cours de la dernière période de 12 mois consécutifs.

Droit à la portabilité des données : les députés ont supprimé les dispositions proposées par la Commission sur la portabilité des données.

Le rapport prévoit que lorsque les données ont été communiquées par la personne concernée et que ces données font l'objet d'un traitement automatisé, la personne concernée devrait avoir le droit d'obtenir auprès du responsable du traitement une copie des données communiquées dans un format électronique interopérable permettant la réutilisation de ces données par la personne concernée, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle.

Lorsque cela est techniquement réalisable et matériellement possible, les données seraient transférées directement d'un responsable du traitement à un autre à la demande de la personne concernée.

Profilage : le rapport a clarifié que toute personne physique doit avoir le droit de s'opposer au profilage. La personne concernée devrait être informée de son droit de s'opposer au profilage de façon évidente.

Tout profilage ayant pour effet d'instaurer une discrimination fondée sur la race ou l'origine ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, l'orientation sexuelle ou l'identité de genre devrait être interdit. Le responsable du traitement devrait assurer une protection efficace contre les discriminations pouvant découler du profilage.

En outre, le profilage conduisant à des mesures produisant des effets juridiques pour la personne concernée ne devrait pas être fondé exclusivement sur le traitement automatisé et devrait inclure une appréciation humaine, y compris une explication de la décision prise à la suite de cette appréciation.

Transferts ou divulgations non autorisés par la législation de l'Union : un nouvel article stipule quaucune décision d'une juridiction d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il divulgue des données à caractère personnel n'est reconnue ni rendue exécutoire de quelque manière que ce soit (sans préjudice d'un accord international entre le pays tiers demandeur et l'Union ou un État membre).

Dans un considérant, il est précisé que lorsque les responsables du traitement ou les sous-traitants sont confrontés à des exigences de conformité contradictoires entre la juridiction de l'Union, d'une part, et celle d'un pays tiers, d'autre part, la Commission devrait toujours veiller à faire prévaloir la législation de l'Union.

Autorité chef de file : lorsque le traitement de données a lieu dans le cadre des activités dun responsable du traitement ou dun sous-traitant établis dans lUnion, les députés ont proposé que lautorité de contrôle de l'État membre où se situe l'établissement principal du responsable du traitement ou du sous-traitant soit l'autorité chef de file responsable du contrôle des activités de traitement des données dans tous les États membres.

Le comité européen de la protection des données émettrait, à la demande d'une autorité de contrôle compétente, un avis sur l'identification de l'autorité chef de file responsable. L'autorité prendrait les mesures qui s'imposent après consultation de toutes les autres autorités de contrôle compétentes en vue de parvenir à un consensus. Elle serait la seule autorité habilitée à prendre des décisions concernant les mesures destinées à produire des effets juridiques vis-à-vis des activités du responsable du traitement ou du sous-traitant dont elle est responsable.

Délégué à la protection des données : le rapport a proposé que le responsable du traitement et le sous-traitant désignent systématiquement un délégué à la protection des données lorsque le traitement est effectué par une personne morale et porte sur plus de 5000 personnes concernées sur une période de douze mois consécutifs. Les délégués à la protection des données seraient désignés pour une durée minimale de quatre ans lorsqu'il s'agit d'un salarié ou de deux ans lorsqu'il s'agit d'un prestataire externe.

Les délégués à la protection des données seraient tenus au secret professionnel pour ce qui est de l'identité des personnes concernées et des circonstances permettant à celles-ci d'être identifiées.

Sanctions administratives : un amendement stipule que lautorité de contrôle devrait infliger à toute personne ne se conformant pas aux obligations énoncées dans le règlement lune au moins des sanctions suivantes :

- un avertissement par écrit lors d'une première infraction non intentionnelle;
- des vérifications périodiques régulières de la protection des données;
- une amende pouvant atteindre 100 millions EUR ou au maximum 5% du chiffre d'affaire annuel mondial dans le cas d'une entreprise, le montant le plus élevé devant être retenu.

Si le responsable du traitement ou le sous-traitant est détenteur dun «label européen de protection des données» valable, lamende serait exclusivement appliquée dans les cas de manquement de propos délibéré ou par négligence.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Conseil a tenu un débat sur la proposition de règlement visant à mettre en place, au niveau de l'UE, un cadre général pour la protection des données.

Les débats ont surtout porté sur le mécanisme du guichet unique afin de parvenir à une décision de contrôle unique et sur les questions connexes du contrôle juridictionnel et du recours juridictionnel.

La réflexion des experts a porté sur des méthodes permettant de renforcer la proximité entre les individus et l'autorité de contrôle décisionnaire en associant les autorités de contrôle locales au processus décisionnel. Le débat a porté sur la nécessité de concilier deux objectifs importants : garantir à la fois aux personnes concernées la proximité souhaitée tout en garantissant aux entreprises actives sur le marché intérieur un mécanisme de guichet unique en matière de contrôle.

La présidence est parvenue aux conclusions suivantes :

- la nécessité de poursuivre les travaux techniques sur la question de savoir s'il y a lieu de conférer à l'autorité de contrôle de l'établissement principal le pouvoir exclusif limité d'adopter des mesures correctrices ;
- limportance que les autorités de contrôle coopèrent dans l'exécution des règles en matière de protection des données ;
- la nécessité d'étudier la possibilité de conférer, dans certains cas, au Comité européen de la protection des données le pouvoir d'adopter des décisions contraignantes en ce qui concerne les mesures correctrices.

Les délégations ont été invitées à dire si elles sont d'accord pour donner à l'autorité de l'établissement principal, agissant en étroite coopération avec les autorités locales, certains pouvoirs exclusifs pour adopter des mesures correctrices, en sus de certains pouvoirs exclusifs en matière d'autorisation.

Dans l'hypothèse où loption susmentionnée ne recueillerait pas un soutien suffisant, les délégations sont invitées à dire si elles pensent que le pouvoir de décider de mesures correctrices devrait rester confié dans tous les cas aux autorités de contrôle «locales» ou si elles pourraient accepter que, dans certains cas transnationaux graves, le Comité européen de la protection des données soit compétent pour adopter des mesures correctrices contraignantes.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Parlement européen a adopté par 621 voix pour, 10 contre et 22 abstentions, une résolution législative sur la 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 et à la libre circulation de ces données (règlement général sur la protection des données).

La position en première lecture adoptée par le Parlement européen suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit :

Champ d'application territorial : les députés ont précisé que le règlement devrait sappliquer que le traitement des données ait lieu ou pas dans lUnion. Il sappliquerait au traitement des données appartenant à des personnes concernées dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées.

Principes relatifs au traitement des données : ces principes devraient être ceux de : i) licéité, loyauté, et transparence ; ii) limitation de la finalité ; iii) limitation des données au minimum ; iv) exactitude ; vi) minimisation de la durée de conservation ; v) effectivité pour la personne dexercer ses droits ; vi) intégrité, cest-à-dire protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, et vii) responsabilité.

Conditions de consentement : la personne concernée devrait être informée, en particulier, de l'existence du traitement des données et de ses finalités, de la durée probable pendant laquelle les données seront conservées pour chaque finalité, de la transmission éventuelle des données à des tiers ou à des pays tiers.

Lorsque le traitement des données est basé sur le consentement, le Parlement a confirmé que la charge de prouver que la personne concernée a consenti au traitement de ses données à caractère personnel à des fins déterminées doit incomber au responsable du traitement. Les députés ont ajouté que :

- les dispositions relatives au consentement de la personne concernée qui enfreignent partiellement le règlement seraient entièrement nulles ;
- il devrait être aussi simple de retirer son consentement que de le donner ; la personne concernée devrait être informée par le responsable du traitement si le retrait du consentement peut entraîner la cessation de la fourniture des services ou de la relation avec le responsable du traitement ;
- le consentement serait lié à la finalité et deviendrait caduc lorsque cette finalité n'existe plus ou dès que le traitement des données à

caractère personnel n'est plus nécessaire pour la réalisation de la finalité pour laquelle elles ont été initialement collectées.

Les informations fournies aux enfants, aux parents et aux tuteurs légaux, y compris en ce qui concerne la collecte et l'utilisation des données par le responsable du traitement, devraient être communiquées dans des termes clairs adaptés au public visé.

Seraient interdits, le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques, l'orientation sexuelle ou l'identité de genre, l'appartenance et les activités syndicales, ainsi que le traitement des données génétiques ou biométriques ou des données concernant la santé ou relatives à la vie sexuelle, aux sanctions administratives, aux jugements, à des infractions pénales ou à des suspicions ou à des condamnations.

Principes généraux en matière de droits des personnes concernées : le Parlement a proposé de renforcer, de clarifier, de garantir et, le cas échéant, de codifier ces droits qui devraient être clairs et univoques. Ces droits incluraient notamment :

- la fourniture d'informations claires et aisément compréhensibles quant au traitement des données à caractère personnel,
- le droit d'accéder à ses données, de les rectifier ou de les effacer,
- le droit d'obtenir des données,
- le droit de s'opposer au profilage, cest-à-dire toute forme de traitement automatisé de données destiné à évaluer certains aspects personnels propres à une personne physique ou à prévoir le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement ;
- le droit de déposer une réclamation auprès de l'autorité de protection des données compétente et d'engager une action en justice,
- le droit d'obtenir réparation et de percevoir une indemnisation en cas d'opération de traitement illégale.

Ces droits devraient pouvoir en général être exercés sans frais. Le responsable du traitement devrait répondre aux demandes de la personne concernée dans un délai raisonnable.

Politiques d'information normalisées : le Parlement a introduit un nouvel article stipulant que lorsque des données relatives à une personne concernée sont collectées, le responsable du traitement devrait informer la personne concernée dune manière visible et facilement lisible et dans un langage aisément compréhensible dune série éléments avant de fournir les informations requises par le règlement.

Ces éléments dinformation porteraient sur la question de savoir si les données : i) sont collectées et conservées ou non au-delà du minimum nécessaire pour chaque objectif spécifique du traitement; ii) sont traitées ou non à des fins autres que celles de leur collecte; iii) sont divulguées à des tiers commerciaux, vendues ou louées; iv) sont conservées ou non sous forme cryptée.

Droit à leffacement : les députés ont renforcé ce droit dans la mesure ou la personne concernée pourrait obtenir de tiers l'effacement de tous les liens vers les données à caractère personnel diffusées, ou de toute copie ou reproduction de celles-ci, pour l'un des motifs suivants:

- un tribunal ou une autorité réglementaire basé(e) dans l'Union a jugé que les données concernées doivent être effacées et cette décision a acquis force de chose jugée;
- les données ont fait l'objet d'un traitement illicite.

Lorsque le responsable du traitement a rendu publiques les données sans aucune justification, il devrait prendre toutes les mesures raisonnables pour procéder à l'effacement de ces données, y compris par des tiers. Il devrait informer la personne concernée, lorsque cela est possible, des mesures prises par les tiers concernés.

Profilage : le Parlement a clarifié que toute personne physique devrait avoir le droit de s'opposer au profilage. La personne concernée devrait être informée de son droit de s'opposer au profilage de façon évidente.

Tout profilage ayant pour effet d'instaurer une discrimination fondée sur la race ou l'origine ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, l'orientation sexuelle ou l'identité de genre devrait être interdit. Le responsable du traitement devrait assurer une protection efficace contre les discriminations pouvant découler du profilage.

En outre, le profilage conduisant à des mesures produisant des effets juridiques pour la personne concernée ne devrait pas être fondé exclusivement sur le traitement automatisé et devrait inclure une appréciation humaine, y compris une explication de la décision prise à la suite de cette appréciation.

Sécurité des traitements : la politique de sécurité devrait inclure la capacité : i) de garantir l'intégrité de la personne concernée; ii) de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données à caractère personnel; iii) de rétablir la disponibilité des données et l'accès à celles-ci, dans les plus brefs délais, en cas d'incident.

Transferts ou divulgations non autorisés par la législation de l'Union : un nouvel article stipule quaucune décision d'une juridiction d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il divulgue des données à caractère personnel ne serait reconnue ni rendue exécutoire de quelque manière que ce soit (sans préjudice d'un accord international entre le pays tiers demandeur et l'Union ou un État membre).

Autorité chef de file : lorsque le traitement de données a lieu dans le cadre des activités dun responsable du traitement ou dun sous-traitant établis dans lUnion, le Parlement a proposé que lautorité de contrôle de l'État membre où se situe l'établissement principal du responsable du traitement ou du sous-traitant soit l'autorité chef de file responsable du contrôle des activités de traitement des données dans tous les États membres.

Sanctions administratives : un amendement stipule que lautorité de contrôle devrait infliger à toute personne ne se conformant pas aux obligations énoncées dans le règlement lune au moins des sanctions suivantes :

- un avertissement par écrit lors d'une première infraction non intentionnelle;
- des vérifications périodiques régulières de la protection des données;
- une amende pouvant atteindre 100 millions EUR ou au maximum 5% du chiffre d'affaire annuel mondial dans le cas d'une entreprise, le montant le plus élevé devant être retenu.

Si le responsable du traitement ou le sous-traitant est détenteur dun «label européen de protection des données» valable, lamende serait exclusivement appliquée dans les cas de manquement de propos délibéré ou par négligence.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Conseil est parvenu à une orientation générale partielle sur des aspects spécifiques du projet de règlement établissant un cadre général de l'UE pour la protection des données. L'orientation générale partielle comprend le chapitre IV du projet de règlement (responsable du traitement et sous-traitant), étant entendu que:

- rien n'est décidé tant qu'il n'y a pas d'accord sur tout, et que des modifications ultérieures peuvent être apportées au texte du chapitre IV en vue d'assurer la cohérence globale du règlement;
- l'orientation est sans préjudice des questions horizontales;
- l'orientation ne constitue pas un mandat donné à la présidence pour s'engager dans des trilogues informels avec le Parlement européen sur le texte.

Le chapitre IV a fait l'objet de discussions approfondies pendant le premier semestre de 2013. Si, lors de la session du Conseil des 6 et 7 juin 2013, toutes les délégations ont félicité la présidence irlandaise pour les progrès considérables réalisés à l'égard de ce chapitre, plusieurs questions restaient en suspens, en particulier la nécessité de réduire davantage la charge administrative/les coûts de mise en conformité découlant du règlement en affinant l'approche fondée sur les risques.

Selon lorientation, la probabilité et la gravité du risque devrait être déterminée en fonction de la nature, de la portée, du contexte et des finalités du traitement de données. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque élevé.

On entend par risque élevé un risque particulier de porter atteinte aux droits et aux libertés des personnes physiques, en particulier :

- lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, [à une violation du pseudonymat] ou à tout autre dommage économique ou social important;
- lorsque les personnes concernées sont susceptibles d'être privées de la maîtrise de l'utilisation qui est faite de leurs données à caractère personnel;
- lorsque le traitement concerne des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques, l'appartenance syndicale, ainsi que des données génétiques ou concernant la santé ou la vie sexuelle ou des données relatives à des condamnations ou à des infractions pénales;
- lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse et de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements, en vue de créer ou d'utiliser des profils individuels;
- lorsque le traitement porte sur des données à caractère personnel relatives à des personnes vulnérables, en particulier des enfants;
- lorsque le traitement porte sur un volume important de données à caractère personnel et sur un nombre important de personnes concernées.

Lorientation prévoit, entre autres, que lorsqu'un responsable du traitement qui n'est pas établi dans l'Union traite des données à caractère personnel concernant des personnes résidant dans l'Union, le responsable du traitement devrait désigner un représentant, à moins que le traitement qu'il effectue soit occasionnel et peu susceptible de constituer un risque pour les droits et libertés des personnes concernées, compte tenu de la nature, de la portée, du contexte et des finalités du traitement, ou que le responsable du traitement ne soit une autorité ou un organisme public.

Le représentant devrait être expressément désigné par un mandat écrit du responsable du traitement le chargeant d'agir en son nom pour remplir les obligations qui lui incombent en vertu du règlement. Le responsable du traitement ou le sous-traitant devrait tenir des registres pour toutes les catégories d'activités de traitement relevant de sa responsabilité.

Dans le cadre de l'évaluation des risques pour la sécurité des données, un considérant souligne la nécessité d'apprécier les risques que présente le traitement de données, tels que la destruction, la perte, l'altération, accidentelles ou illicites, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière, qui sont susceptibles d'entraîner des dommages physiques, matériels ou moraux.

Afin de mieux garantir le respect du règlement dans les cas où les traitements sont susceptibles de comporter un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement [ou le sous-traitant] devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Conseil a dégagé une orientation générale partielle sur certaines questions spécifiques du projet de règlement fixant un cadre général de l'UE pour la protection des données, étant entendu que lorientation générale partielle:

- est dégagée sous réserve du principe selon lequel il n'y a d'accord sur rien tant qu'il n'y a pas d'accord sur tout (des modifications ultérieures pouvant être apportées au texte des articles faisant l'objet d'un accord provisoire en vue d'assurer la cohérence globale du règlement);
- est sans préjudice des questions horizontales;
- ne charge pas la présidence d'engager des trilogues informels avec le Parlement européen sur le texte.

Orientation générale partielle : celle-ci comprend certains articles qui sont cruciaux pour la question du public secteur, à savoir larticle 1er (objet et objectifs du règlement), l'article 6 (licéité du traitement des données à caractère personnel) et l'article 21 (limitations).

Le texte de l'article 1er, de l'article 6, paragraphes 2 et 3, et de l'article 21 ainsi que les considérants correspondants qui a fait l'objet d'un

accord prévoit maintenant clairement le cadre dans lequel les États membres pourront maintenir et d'adopter une législation au titre du présent règlement. La présidence estime que ce texte est équilibré en ce qu'il accorde aux États membres une mesure appropriée de flexibilité tout en gardant une structure cohérente du règlement.

Lorientation générale comprend également le chapitre IX portant sur les dispositions relative à des situations particulières de traitement de données spécifiques (ex : traitements des données en lien avec la liberté d'expression et d'information, avec laccès du public aux documents officiels, avec la réutilisation des informations du secteur public, avec des fins liées à la santé, en matière demploi, à des fins de protection sociale ; les dérogations applicables au traitement de données à caractère personnel à des fins d'archivage et à des fins scientifiques, statistiques et historiques).

La question consistant à savoir si le règlement général sur la protection des données doit couvrir, et selon quelles modalités, le traitement des données à caractère personnel réalisé par le secteur public est particulièrement sensible et importante pour les délégations. Lors de la réunion informelle des ministres qui a eu lieu à Milan le 9 juillet 2014, les États membres ont, dans leur grande majorité, préconisé le recours à un règlement en tant qu'instrument juridique. Toutefois, ils ont également souligné la nécessité de prévoir une marge de manuvre suffisante pour les États membres pour qu'ils fixent les exigences relatives à la protection des données qui sont applicables au secteur public.

Mécanisme du «guichet unique» : le Conseil a également tenu un débat sur le «one stop shop» ou mécanisme du «guichet unique» sur la base d'une proposition présentée par la présidence. La majorité des ministres a approuvé l'architecture générale de la proposition et a conclu que les travaux devaient se poursuivre sur la base des orientations formulées lors du Conseil JAI d'octobre et de décembre 2013, à savoir que :

- dans les affaires transnationales importantes, le projet de règlement devrait établir un mécanisme de guichet unique afin de parvenir à une décision de contrôle unique, qui serait rapide, assurerait une application cohérente, garantirait la sécurité juridique et réduirait la charge administrative;
- les experts devraient réfléchir à des méthodes permettant de renforcer la «proximité» entre les personnes physiques et l'autorité de contrôle décisionnaire en associant les autorités de contrôle locales au processus décisionnel ;
- dans le cadre des travaux qui se poursuivront au niveau technique, il conviendrait d'examiner la possibilité d'octroyer dans certains cas au comité européen de la protection des données le pouvoir d'adopter des décisions contraignantes en matière de mesures correctrices.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Recommandations du Contrôleur européen de la protection des données (CEPD) relatives aux options de l'UE en matière de réforme de la protection des données.

Pour rappel, le 24 juin 2015, le Parlement européen, le Conseil et la Commission européenne ont engagé des négociations de codécision («trilogue informel») relatives à la proposition de règlement général sur la protection des données. Les trois institutions se sont engagées à traiter le règlement général sur la protection des données dans le cadre du train de réformes élargi de la protection des données qui inclut la proposition de directive relative aux activités policières et judiciaires.

Le présent avis met à jour l'avis publié en mars 2012 (lequel reste valide) pour soutenir plus directement les positions des colégislateurs et proposer des recommandations spécifiques de façon à permettre aux participants au trilogue de trouver un consensus à temps.

Une rare opportunité : le CEPD rappelle que la réforme de la protection des données revêt une importance capitale :

1°) L'UE est dans le dernier kilomètre d'un marathon visant à réformer ses règles sur les données à caractère personnel. Le règlement général sur la protection des données affectera potentiellement, pour les décennies à venir, toute la population de l'UE, toutes les organisations de l'UE qui traitent des données à caractère personnel et les organisations extérieures à l'UE qui traitent les données à caractère personnel de personnes physiques vivant dans l'EU.

2°) Une protection efficace des données responsabilise les personnes physiques et galvanise les entreprises responsables et les pouvoirs publics. Les législations en vigueur dans ce domaine sont complexes et techniques. Les textes de chacune des institutions prêchent clarté et intelligibilité dans le traitement des données à caractère personnel: le règlement général sur la protection des données doit donc mettre en pratique ce qu'il préconise, en étant aussi clair et compréhensible que possible.

3°) L'UE a besoin d'un nouvel accord sur la protection des données. Le reste du monde suit de près ce qui se passe actuellement. La qualité de la nouvelle législation et la manière dont elle interagit avec les systèmes juridiques et les tendances du monde entier revêtent une importance capitale.

Les recommandations du CEPD : parmi les options qui se présentent sous la forme des textes spécifiques préconisés par les trois institutions, toutes contiennent des dispositions valables, mais chacune peut être améliorée. Les recommandations du CEPD sont inspirées par trois préoccupations majeures:

1) Un meilleur compromis pour les citoyens : pour le CEPD, le point de départ est la dignité de la personne qui transcende les questions de simple conformité juridique. Les principes qui se trouvent au cur de la protection des données, à savoir l'article 8 de la charte des droits fondamentaux, constituent le point de référence. Dans ce contexte, le CEPD insiste sur les points suivants :

- clarifier la notion d'informations à caractère personnel : les personnes doivent pouvoir exercer plus efficacement leurs droits concernant toute information susceptible de les identifier ou de les distinguer, même si l'information est considérée comme «pseudonymisée»;
- tout traitement de données doit être licite et justifié : par exemple, i) les données à caractère personnel ne devraient être utilisées que de manière compatible avec les fins initiales de collecte ; ii) le consentement constitue un fondement juridique éventuel du traitement, mais il faut empêcher toute contrainte visant à faire en sorte qu'une personne coche des cases lorsqu'elle n'a pas de choix véritable et que le traitement des données n'est pas nécessaire du tout ; iii) l'UE ne doit pas laisser la porte ouverte à un accès direct par des autorités de pays tiers à des données situées dans l'UE;
- une surveillance plus indépendante, plus sûre : i) les autorités doivent être en mesure d'examiner les plaintes et les réclamations

introduites par des personnes concernées ou par des organisations et associations ; ii) lapplication des droits individuels nécessite un système efficace de responsabilité et d'indemnisation en cas de dommages causés par le traitement illicite des données.

2) Des règles applicables en pratique : chacun des trois textes exige une clarté et une simplicité accrues de la part des responsables du traitement des informations à caractère personnel. Les contraintes techniques doivent être concises et faciles à comprendre pour être correctement mises en uvre par les responsables du traitement. Cela implique :

- des garanties efficaces, pas des procédures : les recommandations du CEPD visent à trouver des voies de simplification administrative, en réduisant les prescriptions pour la documentation et les formalités superflues. Il est recommandé de ne légiférer qu'en cas de véritable nécessité;
- un meilleur équilibre entre l'intérêt public et la protection des données à caractère personnel : les règles de protection des données ne devraient pas entraver la recherche historique, statistique et scientifique qui sert réellement l'intérêt général;
- de faire confiance aux autorités de contrôle et leur donner les moyens d'agir : ces autorités devaient fournir des orientations aux responsables du traitement de données et élaborer leurs propres règles de procédure internes dans le sens d'une application simplifiée, facilitée du règlement général sur la protection des données par une autorité de contrôle unique (le «guichet unique») proche des citoyens («proximité»).

3) Des règles qui dureront le temps d'une génération : il est raisonnable de supposer que la prochaine grande révision des règles en matière de protection des données ninterviendra peut-être pas avant la fin des années 2030. Longtemps avant cela, on pourra s'attendre à ce que les technologies axées sur les données aient convergé avec les systèmes biométriques, d'intelligence artificielle et de traitement du langage naturel.

Ces technologies posent un défi aux principes de la protection des données. Une réforme orientée vers l'avenir devrait reposer sur la dignité de la personne et être guidée par l'éthique. Elle devrait réduire le déséquilibre entre l'innovation dans la protection des données à caractère personnel et son exploitation, en renforçant l'efficacité des garanties au sein dune société numérisée.

Face à ces défis, le CEPD :

- estime que la réforme devrait inverser la tendance récente à la surveillance secrète et à la prise de décision sur la base de profils cachés de la personne ; une plus grande transparence des responsables du traitement est préconisée;
- soutient l'introduction des principes de protection des données dès la conception et de protection des données par défaut comme un moyen de lancer des solutions axées sur le marché dans l'économie numérique;
- recommande de permettre un transfert direct des données d'un responsable du traitement à un autre, à la demande de la personne concernée, et d'autoriser les personnes concernées à recevoir une copie des données qu'ils pourront eux-mêmes transférer à un autre responsable du traitement.

Questions en suspens : le CEPD note que l'adoption du train de réformes européen des données sera une réalisation impressionnante mais néanmoins incomplète.

- La directive 2002/58/CE (la «directive vie privée et communications électroniques») devra ainsi être modifiée.
- L'UE exige également un cadre précis pour la confidentialité des communications qui régisse l'ensemble des services permettant les communications, pas seulement les fournisseurs de services de communications électroniques accessibles au public. Cela devra se faire au moyen d'un règlement juridiquement sûr et harmonisé.

À un moment où la confiance des personnes dans les entreprises et les gouvernements a été ébranlée par des révélations sur la surveillance de masse et les violations de données, le CEPD insiste sur la responsabilité considérable des législateurs de l'UE dont les décisions devraient avoir des répercussions au-delà de l'Europe.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Conseil a adopté sa position en première lecture en vue de l'adoption du règlement général sur la protection des données. Le règlement proposé, en harmonisant les règles en vigueur dans l'Union européenne en matière de protection des données, a pour objectifs de renforcer les droits des personnes physiques en matière de protection des données, de faciliter le libre flux des données à caractère personnel dans le marché unique et de réduire la charge administrative.

La position du Conseil en première lecture conserve les objectifs de la directive 95/46/CE, à savoir: la préservation des droits en matière de protection des données et le libre flux des données. Parallèlement, elle s'efforce d'adapter les règles actuellement en vigueur pour tenir compte du volume sans cesse croissant de données à caractère personnel qui font l'objet d'un traitement en raison des évolutions technologiques et de la mondialisation.

Les éléments clés de la position du Conseil en première lecture sont les suivants :

Champ d'application : la position du Conseil prévoit que le règlement général s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés.

De plus, la position du Conseil renforce la responsabilité des responsables du traitement (chargés de déterminer les finalités et les moyens du traitement de données à caractère personnel) et des sous-traitants (chargés de traiter des données à caractère personnel pour le compte du responsable du traitement). Elle met les responsables du traitement et les sous-traitants sur un pied d'égalité en prévoyant un champ d'application territorial couvrant tous les responsables de traitement et tous les sous-traitants, qu'ils soient ou non établis dans l'Union.

Principes relatifs au traitement des données à caractère personnel : s?agissant du principe de licéité du traitement, la position du Conseil s'appuie sur la directive 95/46/CE pour préciser que le traitement de données à caractère personnel n'est licite que si au moins une des conditions suivantes est remplie:

- la personne concernée a consenti clairement et explicitement au traitement pour une ou plusieurs finalités spécifiques; un régime de

protection particulier est prévu lorsque des enfants donnent leur consentement dans le cadre d'une offre de services de la société de l'information ;
- le traitement est nécessaire : i) à l'exécution d'un contrat; ii) au respect d'une obligation légale; iii) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique; iv) à l'exécution d'une mission d'intérêt public ; v) aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

La position du Conseil :

- permet aux États membres de maintenir ou d'introduire des dispositions plus spécifiques pour adapter l'application des règles énoncées dans le règlement si les données font l'objet d'un traitement pour respecter une obligation légale ou si ce traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- prévoit qu'un traitement pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées initialement n'est licite que si ce traitement ultérieur est compatible avec les finalités pour lesquelles les données à caractère personnel ont été traitées initialement.

Renforcement des moyens d'action des personnes concernées : la position du Conseil accorde des droits renforcés en matière de protection des données et soumet les responsables du traitement à des obligations. Les droits des personnes concernées englobent :

- le droit à l'information: ces informations doivent être fournies de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée à un enfant ;
- le droit d'accès aux données à caractère personnel, c?est-à-dire le droit d'obtenir du responsable du traitement la confirmation que des données la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès aux informations énumérées dans le règlement ;
- le droit de rectification ;
- le droit à l'effacement des données à caractère personnel, y compris le «droit à l'oubli» ;
- le droit à la limitation du traitement ;
- le droit à la portabilité des données : les personnes concernées auraient le droit de recevoir les données les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé, lisible par machine et interopérable, et de transmettre ces données à un autre responsable du traitement ;
- le droit d'opposition et le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage. À cet égard, il est précisé que, lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée aurait le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant.

Responsable du traitement et sous-traitant : la position du Conseil établit le cadre juridique régissant la responsabilité concernant tout traitement de données à caractère personnel effectué par un responsable du traitement ou, pour son compte, par un sous-traitant.

Conformément au principe de responsabilité, le responsable du traitement serait tenu de mettre en ?uvre des mesures techniques et organisationnelles appropriées et d'être en mesure de démontrer la conformité de ses opérations de traitement avec le règlement. À cet égard, le règlement fixe des règles relatives aux responsabilités du responsable du traitement concernant :

- les analyses d'impact, lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ;
- la tenue de registres des activités de traitement,
- les violations de données,
- la désignation d'un délégué à la protection des données et
- les codes de conduite, les mécanismes de certification, les labels et les marques en matière de protection des données.

Transfert de données à caractère personnel vers des pays tiers : le niveau de protection garanti par l'Union ne devrait pas être compromis lorsque des données à caractère personnel de citoyens de l'UE sont transférées vers des pays tiers. En règle générale, tout transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ne pourrait être effectué que si les responsables du traitement et les sous-traitants se conforment aux règles prévues par le règlement.

Autorités de contrôle : chaque État membre devrait prévoir qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du règlement sur leur territoire. Les autorités de contrôle et leurs membres devraient exercer en toute indépendance et avec intégrité les missions et les pouvoirs dont ils sont investis.

Comité européen de la protection des données : la position du Conseil institue le comité européen de la protection des données en tant qu'organe de l'Union possédant la personnalité juridique, en vue d'assurer l'application correcte et cohérente du règlement

Voies de recours, responsabilité et sanctions : un ensemble détaillé de règles est prévu en vue de permettre aux personnes concernées de disposer de plusieurs voies de recours, notamment de réclamer réparation en cas de préjudice résultant d'une violation du règlement.

En vue de garantir le respect des dispositions du règlement, la position du Conseil prévoit que les autorités de contrôle peuvent imposer des amendes administratives pouvant aller jusqu'à 20 millions EUR ou 4 % du chiffre d'affaires mondial total d'une entreprise.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

La Commission souscrit à laccord politique conclu le 15 décembre 2015 entre le Parlement européen et le Conseil lors de trilogues informels, étant donné qu'il est conforme aux objectifs de sa proposition.

La proposition de règlement vise à renforcer les droits des personnes et le marché intérieur de lUE, garantir un contrôle accru de lapplication de la réglementation, simplifier les transferts internationaux de données à caractère personnel et instaurer des normes mondiales en matière de protection des données. Les nouvelles règles prévoient à cette fin les mesures suivantes:

- faciliter l'accès à ses propres données: les personnes recevront des informations plus nombreuses, plus claires et plus

compréhensibles sur la façon dont leurs données sont traitées;
- bénéficier d'un «droit à l'oubli»: si une personne ne souhaite plus que ses données soient traitées, et pour autant qu'aucun motif légitime ne justifie de les conserver, ces données seront supprimées;
- permettre à une personne de savoir que ses données ont été piratées: les entreprises devront signaler à lautorité de contrôle les violations de données qui font courir un risque aux personnes concernées et communiquer dès que possible à ces dernières toutes les violations présentant des risques élevés;
- garantir la portabilité des données: les personnes pourront plus facilement transférer des données à caractère personnel dun prestataire de services à un autre.

Le règlement proposé contribue également à réaliser le potentiel du marché unique, grâce aux mesures suivantes:

- lapplication du principe «un continent, une législation» ;
- la mise en place d'un «guichet unique» pour les entreprises ;
- des conditions de concurrence équitables: les entreprises ayant leur siège en dehors de lEurope devront appliquer les mêmes règles lorsquelles proposeront des biens ou des services sur le marché de lUE;
- la neutralité technologique : linnovation pourra ainsi continuer à se développer au sein du nouveau cadre réglementaire.

La Commission européenne constate que laccord :

- respecte la nature de linstrument juridique proposé par la Commission, à savoir un règlement plutôt quune directive ;
- garantit un niveau dharmonisation suffisant, tout en laissant aux États membres une marge de manuvre en ce qui concerne les spécifications des règles de protection des données dans le secteur public ;
- confirme lapproche de la Commission concernant le champ dapplication territorial du règlement, qui sappliquera également aux responsables du traitement ou aux sous-traitants établis dans un pays tiers, lorsque les activités de traitement sont liées à l'offre de biens ou de services à des personnes résidant dans l'Union ou à l'observation de ces personnes ;
- maintient lapproche de la Commission, en renforçant les principes relatifs au traitement des données (minimisation des données, p. ex.) et aux droits des personnes concernées, en consacrant le droit à loubli et le droit à la portabilité, et en continuant à développer les droits existants, tels que le droit à linformation ou le droit daccès ;
- préserve et développe lapproche fondée sur le risque qui exige que les responsables du traitement et, dans certains cas, les sous-traitants, tiennent compte de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du degré de probabilité et de gravité des risques pour les droits et libertés des personnes concernées ;
- prévoit un mécanisme solide de «guichet unique» sur le plan juridique et institutionnel et conserve les principaux éléments de simplification, qui consistent à instaurer le principe d'une décision unique au niveau de lUE et d'un seul interlocuteur pour les entreprises et les personnes ;
- clarifie et précise les règles relatives aux transferts internationaux ;
- autorise les autorités de contrôle à infliger des sanctions financières en cas d'infraction au règlement, à concurrence de 2 à 4% du chiffre daffaires annuel mondial de lentreprise.

Toutefois, contrairement à la proposition de la Commission, la position du Conseil ne considère pas le règlement comme un développement de lacquis de Schengen. La Commission juge par conséquent nécessaire de faire une déclaration à cet égard. Dans cette déclaration, la Commission estime en particulier qu'en ce qui concerne les visas, les contrôles aux frontières et le retour, le règlement général sur la protection des données constitue un développement de lacquis de Schengen pour les quatre pays associés à la mise en uvre, à lapplication et au développement de cet acquis.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

La commission des libertés civiles, de la justice et des affaires intérieures a adopté la recommandation pour la deuxième lecture contenue dans le rapport de Jan Philipp ALBRECHT (Verts/ALE, DE) concernant la position du Conseil en première lecture en vue de l'adoption du règlement du Parlement européen et du Conseil 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).

La commission parlementaire a recommandé que le Parlement européen approuve la position du Conseil en première lecture sans y apporter damendements.

Pour rappel, le règlement proposé établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. Il est destiné à remplacer la directive de 1995 sur la protection des données.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

Le Parlement européen a adopté une résolution législative relative à la position du Conseil en première lecture en vue de l'adoption du règlement du Parlement européen et du Conseil 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).

Suivant la recommandation pour la deuxième lecture de sa commission des libertés civiles, de la justice et des affaires intérieures, le Parlement a approuvé la position du Conseil en première lecture sans y apporter d?amendements.

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

OBJECTIF : moderniser les règles existantes en matière de protection des données en vue dassurer un niveau équivalent de protection des personnes physiques et le libre flux des données à caractère personnel dans l'ensemble de l'Union (réforme de la protection des données).

ACTE LÉGISLATIF : Règlement (UE) 2016/679 du Parlement européen et du Conseil 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)

CONTENU : le nouveau règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. Il protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel. La réforme de la protection des données comprend également une directive concernant la protection des données traitées à des fins répressives (destinée à remplacer la décision-cadre de 2008 sur la protection des données).

Les principaux éléments du règlement sont les suivants :

Champ dapplication : le règlement sapplique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Il sapplique au traitement des données effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

Principes relatifs au traitement des données à caractère personnel : les données à caractère personnel doivent être :

- traitées de manière licite, loyale et transparente au regard de la personne concernée,
- collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
- adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de façon à garantir une sécurité des données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.

Licéité du traitement des données : le traitement ne sera licite que si :

- la personne concernée a consenti clairement et explicitement au traitement de ses données ;
- le traitement est nécessaire : i) à l'exécution d'un contrat; ii) au respect d'une obligation légale; iii) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique; iv) à l'exécution d'une mission d'intérêt public ; v) aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Un régime de protection particulier est prévu lorsque des enfants donnent leur consentement dans le cadre d'une offre de services de la société de l'information : si un enfant de moins de 16 ans souhaite utiliser des services en ligne, le fournisseur de services devra vérifier que les parents ont donné leur accord. Les États membres pourront abaisser cette limite d'âge sans toutefois descendre en dessous de 13 ans.

En principe, le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique seront interdits. Ces données pourront toutefois être traitées sous certaines conditions énumérées dans le règlement.

Droits de la personne concernée : le règlement accorde des droits renforcés en matière de protection des données et soumet les responsables du traitement à des obligations. Les droits des personnes concernées englobent :

- le droit à l'information: ces informations doivent être fournies de façon concise, transparente, compréhensible et aisément accessible, en particulier pour toute information destinée à un enfant ; les personnes physiques doivent notamment être informées de la politique en vigueur en matière de protection des données, en termes clairs et simples; cela peut également se faire au moyen d'icônes normalisées ;
- le droit d'accès aux données à caractère personnel, cest-à-dire le droit d'obtenir du responsable du traitement la confirmation que des données la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, le droit daccéder aux informations concernant par exemple les finalités du traitement, les catégories de données concernées, les destinataires auxquels les données ont été ou seront communiquées et lorsque cela est possible, la durée de conservation des données ;
- le droit de rectification des données inexactes;
- le droit à l'effacement des données à caractère personnel, y compris le «droit à l'oubli»;
- le droit à la limitation du traitement ;
- le droit à la portabilité des données, facilitant le transfert de données à caractère personnel d'un fournisseur de services, par exemple un réseau social, à un autre ;
- le droit d'opposition et le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage. À cet égard, il est précisé que, lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée aura le droit de s'opposer à tout moment au traitement des données la concernant.

Ces droits pourront être limités lorsquune telle limitation respecte les libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire dans une société démocratique pour garantir la sécurité nationale, la défense nationale ou la sécurité publique.

Responsable du traitement et sous-traitant : le règlement établit le cadre juridique régissant la responsabilité concernant tout traitement effectué par un responsable du traitement ou, pour son compte, par un sous-traitant. Le responsable du traitement sera tenu de mettre en uvre des mesures techniques et organisationnelles appropriées et d'être en mesure de démontrer la conformité de ses opérations de traitement avec le règlement.

Sécurité des données : afin de garantir la sécurité et de prévenir tout traitement effectué en violation du règlement, le responsable du traitement ou le sous-traitant devra évaluer les risques inhérents au traitement et mette en uvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devront assurer un niveau de sécurité approprié, y compris la confidentialité.

Le responsable du traitement devra communiquer une violation de données à caractère personnel à la personne concernée dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent. Il devra notifier la violation en question à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance.

Délégué à la protection des données : les autorités publiques et les entreprises qui effectuent certains traitements de données à risques devront désigner un délégué à la protection des données pour garantir le respect des règles. Les personnes concernées pourront prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice de leurs droits.

Transfert de données en dehors de lUE : en règle générale, tout transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ne pourra être effectué que si les responsables du traitement et les sous-traitants se conforment aux règles prévues par le règlement.

La Commission pourra décider, par voie d'actes d'exécution, qu'un pays tiers ou une organisation internationale assure un niveau de protection adéquat. Les décisions relatives à l'adéquation du niveau de protection des données devront être revues au moins tous les quatre ans.

Contrôle : afin de réduire les coûts et d'offrir une sécurité juridique, dans des affaires transfrontières importantes faisant intervenir plusieurs autorités de contrôle nationales, une décision de contrôle unique sera prise. Ce mécanisme permettra à une entreprise active dans plusieurs États membres de ne traiter qu'avec l'autorité de protection des données de l'État membre dans lequel elle a son établissement principal. Ce mécanisme prévoit aussi une décision unique applicable à l'ensemble du territoire de l'UE en cas de litige.

Voies de recours, responsabilité et sanctions : le règlement fixe un ensemble détaillé de règles en vue de permettre aux personnes concernées de réclamer réparation ou de former un recours juridictionnel en cas de préjudice résultant d'une violation du règlement.

Les autorités de contrôle pourront imposer aux responsables d'un traitement des amendes administratives pouvant aller jusqu'à 20 millions EUR ou 4% du chiffre d'affaires mondial total d'une entreprise en cas de non-respect du règlement.

ENTRÉE EN VIGUEUR : 24.5.2016.

APPLICATION : à partir du 25.5.2018.

ACTES DÉLÉGUÉS : la Commission peut adopter des actes délégués, particulièrement en ce qui concerne les critères et exigences applicables aux mécanismes de certification, les informations à présenter sous la forme d'icônes normalisées ainsi que les procédures régissant la fourniture de ces icônes. Le pouvoir dadopter de tels actes est conféré à la Commission pour une durée indéterminée à compter du 24 mai 2016. Le Parlement européen ou le Conseil peuvent formuler des objections à l'égard d'un acte délégué dans un délai de trois mois à compter de la date de notification (ce délai pouvant être prolongé de trois mois). Si le Parlement européen ou le Conseil formulent des objections, l'acte délégué n'entre pas en vigueur.