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

2012/0011(COD) - 27/04/2016 - Acte final

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.