Conseil de l'UE

PRESS
FR

COMMUNIQUÉ DE PRESSE
951/15
18/12/2015

Réforme de la protection des données dans l'UE: le Conseil confirme l'accord intervenu avec le Parlement européen

Le 18 décembre 2015, le Comité des représentants permanents (Coreper) a entériné les textes de compromis qui avaient fait l'objet d'un accord avec le Parlement européen dans le cadre de la réforme de la protection des données. L'accord entre le Conseil, le Parlement et la Commission était intervenu le 15 décembre. Il répond à la demande du Conseil européen, qui voulait que les négociations engagées en vue d'une réforme de la protection des données soient achevées pour la fin 2015.

Félix BRAZ, ministre luxembourgeois de la justice et président du Conseil, a déclaré ce qui suit: "Il s'agit d'un accord fondamental aux conséquences importantes. Cette réforme ne renforce pas seulement les droits des citoyens, elle adapte également, au profit des entreprises, les règles à l'ère du numérique, tout en réduisant les charges administratives. Il s'agit de textes ambitieux et tournés vers l'avenir. Nous pouvons avoir une totale confiance dans le résultat."

La réforme de la protection des données est un paquet législatif proposé par la Commission en 2012 afin de mettre à jour et moderniser les règles en la matière. Il se compose de deux instruments législatifs: le règlement général sur la protection des données (destiné à remplacer la directive 95/46/CE) et la directive concernant la protection des données traitées à des fins répressives (destinée à remplacer la décision-cadre de 2008 sur la protection des données).

La protection des personnes à l'égard du traitement des données à caractère personnel les concernant est un droit fondamental consacré par la Charte des droits fondamentaux de l'UE (article 8) et par le traité sur le fonctionnement de l'Union européenne (article 16).

Règlement général sur la protection des données

Le règlement général sur la protection des données vise à renforcer le niveau de protection des données pour les personnes physiques dont les données à caractère personnel sont traitées et à accroître les débouchés commerciaux dans le marché unique numérique, notamment grâce à une réduction des charges administratives.

Un niveau renforcé de protection des données

Les principes et règles en matière de traitement des données à caractère personnel des personnes physiques doivent respecter les droits et libertés fondamentaux, notamment le droit à la protection des données à caractère personnel. Ce renforcement des droits en matière de protection des données permet aux personnes concernées (les personnes physiques dont les données à caractère personnel sont traitées) de mieux contrôler leurs données à caractère personnel, grâce à:

- des règles plus précises pour autoriser les responsables du traitement des données à traiter des données à caractère personnel, avec notamment l'obligation d'obtenir le consentement des personnes physiques concernées;
- un accès plus aisé aux données à caractère personnel les concernant;
- une meilleure information sur ce qu'il advient des données à caractère personnel dès qu'elles sont partagées. 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;
- un droit à l'effacement des données à caractère personnel et "à l'oubli". Cela permet ainsi, par exemple, à une personne concernée d'exiger le retrait immédiat de données à caractère personnel collectées ou publiées sur un réseau social alors qu'elle n'était encore qu'un enfant;
- si un jeune de moins de 16 ans souhaite utiliser des services en ligne, le fournisseur de services doit vérifier que les parents ont donné leur accord. Les États membres peuvent abaisser cette limite d'âge sans toutefois descendre en dessous de 13 ans;
- un droit à la portabilité, facilitant le transfert de données à caractère personnel d'un fournisseur de services, par exemple un réseau social, à un autre. Ces mesures ne vont pas seulement renforcer les droits en matière de protection des données, elles vont aussi stimuler la concurrence entre les fournisseurs de services;
- un droit de s'opposer au traitement de données à caractère personnel en lien avec l'intérêt public ou les intérêts légitimes d'un responsable du traitement. Ce droit s'étend à l'utilisation de données à caractère personnel à des fins de profilage;
- des garanties communes couvrant le traitement de données à caractère personnel à des fins d'archivage dans l'intérêt public et à des fins scientifiques, statistiques ou de recherches historiques.

Afin de leur assurer une proximité d'accès aux voies de recours, les personnes concernées ont le droit de soumettre toute

décision de leur autorité chargée de la protection des données au contrôle de leur juridiction nationale, quel que soit l'État membre dans lequel le responsable du traitement est établi.

Des débouchés commerciaux accrus dans le marché unique numérique

Le règlement prévoit un ensemble unique de règles, valables dans toute l'UE et applicables aux entreprises européennes et non européennes proposant des services en ligne dans l'UE. Cela permet d'éviter des situations dans lesquelles des règles nationales divergentes en matière de protection de données pourraient entraver les échanges transfrontières de données. Le règlement prévoit aussi un renforcement de la coopération entre les États membres pour que les règles en matière de protection des données soient appliquées de manière cohérente dans toute l'UE. Cela créera une concurrence loyale et encouragera les entreprises, notamment les petites et moyennes, à tirer le meilleur parti du marché unique numérique.

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 de guichet unique** permet 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.

En vue de réduire les coûts administratifs, le règlement applique une approche fondée sur le risque: les responsables du traitement des données peuvent mettre en œuvre des mesures en fonction du risque associé aux opérations de traitement qu'ils effectuent. Les entreprises sont différentes, les activités sont différentes; dès lors, les risques que ces activités font peser sur la vie privée peuvent varier. Le règlement ne prévoit pas de solution unique: plus les risques résultant des activités sont importants pour les données à caractère personnel, plus les obligations sont strictes.

Des outils plus nombreux et de meilleure qualité pour faire appliquer les règles en matière de protection des données

Le règlement prévoit une série de mesures pour renforcer la responsabilité des responsables du traitement et l'obligation de rendre des comptes qui leur incombe, l'objectif étant d'assurer un respect absolu des nouvelles règles en matière de protection des données. Les responsables du traitement doivent mettre en œuvre un certain nombre de mesures de sécurité, avec l'obligation dans certains cas de notifier les violations de données à caractère personnel. Pour veiller à ce que le règlement soit à l'épreuve du temps, les principes de la protection des données dès la conception et de la protection des données par défaut sont introduits. Les autorités publiques et les entreprises qui effectuent certains traitements de données à risques doivent désigner un **délégué à la protection des données** pour garantir le respect des règles.

Les personnes concernées ainsi que, dans certaines conditions, les organismes de protection des données peuvent introduire une réclamation auprès d'une autorité de contrôle ou former un recours juridictionnel dans les cas où les règles en matière de protection des données ne sont pas respectées. Les responsables d'un traitement peuvent s'exposer à des amendes d'un montant maximal de 20 millions d'euros ou correspondant à 4 % de leur chiffre d'affaires annuel mondial.

Garanties concernant les transferts de données à caractère personnel en dehors de l'UE

Le règlement fixe les règles de transfert de données à caractère personnel vers les pays tiers et les organisations internationales. Des transferts peuvent intervenir à condition que différentes conditions et garanties soient respectées, en particulier lorsque la Commission a décidé qu'un niveau adéquat de protection existe. Les nouvelles décisions relatives à l'adéquation du niveau de protection des données devront être revues au moins tous les quatre ans. Les décisions relatives à l'adéquation et les autorisations existantes resteront en vigueur jusqu'au moment où elles seront modifiées, remplacées ou abrogées.

Directive sur la protection des données traitées à des fins répressives

Cette directive vise à protéger les données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Il est indispensable de garantir un niveau élevé et systématique de protection des données à caractère personnel des personnes physiques tout en facilitant en parallèle l'échange de ces données entre les services répressifs des différents États membres.

Champ d'application élargi

Outre les activités menées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, le champ d'application de la nouvelle directive a été étendu à la protection contre les menaces pour la sécurité publique et à la prévention de telles menaces.

La nouvelle directive s'appliquerait aussi bien au traitement transfrontière des données à caractère personnel qu'au traitement de ce type de données par les autorités policières et judiciaires au niveau strictement national. La décision-cadre, qui sera

remplacée, ne portait que sur l'échange transfrontière de données.

Droits des personnes concernées

Les règles instaurent un équilibre entre le droit à la protection de la vie privée et la nécessité que la police ne soit pas tenue de révéler dès le début d'une enquête que des données sont traitées. Cela étant, le texte énumère les informations que la personne concernée est toujours en droit de recevoir afin de protéger ses droits si elle craint que ses données aient fait l'objet d'une violation.

Les nouvelles règles couvriront aussi le transfert de données à caractère personnel vers des pays tiers et des organisations internationales.

Respect des dispositions

La nouvelle directive prévoit qu'un **délégué à la protection des données** soit nommé pour aider les autorités compétentes à faire respecter les règles en matière de protection des données.

L'analyse d'impact constitue un autre outil permettant d'assurer le respect des dispositions. Lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, les autorités compétentes doivent procéder à une analyse de l'impact potentiel dudit traitement, en particulier en cas de recours à une nouvelle technologie.

Contrôle et compensation

Le texte de la directive est aligné sur celui du règlement pour que, dans les grandes lignes, les mêmes principes généraux s'appliquent. Par ailleurs, les règles relatives à l'autorité de contrôle sont dans une large mesure similaires car l'autorité de contrôle instituée dans le règlement général sur la protection des données peut aussi se saisir de matières relevant de la directive. La nouvelle directive donnerait également le droit aux personnes concernées d'obtenir une compensation si elles subissent un préjudice du fait d'un traitement ne respectant pas les règles.

PROCHAINES ÉTAPES

Le 17 décembre, lors d'une réunion extraordinaire, la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen a entériné les textes approuvés pendant les trilogues. Le Coreper a ainsi été en mesure aujourd'hui de confirmer les textes de compromis définitifs du règlement et de la directive. Après leur mise au point par les juristes-linguistes, ces textes seront soumis pour adoption au Conseil, puis au Parlement européen. Le règlement et la directive devraient entrer en vigueur au printemps 2018.

Bureau de presse - Secrétariat général du Conseil de l'UE
Rue de la Loi 175 - B-1048 BRUXELLES - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press