Lire cet article en ligne

Nouveau règlement européen sur la protection des données (Partie II)

Le très attendu Règlement n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (autrement appelé le « Règlement général sur la protection des données » ou « RGPD ») vient de paraître au Journal officiel de l'Union européenne (JO, L 119, 4 mai 2016).

Sur proposition de la Commission européenne en date du 25 janvier 2012, ce Règlement adopté conjointement par le Parlement européen et le Conseil remplace la directive 95/46/CE et instaure un cadre général et unique pour la protection des données en Europe.

Le présent article (Partie II ; Partie I parue le mois dernier) se propose d'identifier les principales innovations apportées par le Règlement.

Responsable de traitement et sous-traitant (chapitre IV)

Les définitions du responsable de traitement, « *personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* », et du sous-traitant, « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* », restes inchangées (articles 4, 7° et 4,8°).

La volonté affichée de renforcer les obligations des sous-traitants, qui jouent un rôle considérable dans le traitement des données, se traduit clairement dans les dispositions du règlement.

Les règles actuelles prévoient en effet seulement que « *la réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que : – le sous-traitant n'agit que sur la seule instruction du responsable du traitement, – les obligations visées au paragraphe 1[1], telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci.* » (article 17, 3° de la directive 95/46).

Le règlement, s'il reprend le même principe, impose un contenu détaillé pour ce contrat ou acte juridique conclu entre le responsable de traitement et son sous-traitant (article 28) et aligne les droits et obligations du sous-traitant et du responsable de traitement en ce qui concerne notamment la tenue d'un registre de toutes les activités de traitement (article 30), la sécurité (article 32), la désignation du délégué à la protection des données (article 37), l'application de codes de conduite (articles 40 et 41), la certification (article 42), le transfert des données (chapitre V), le droit à un recours et à réparation des personnes concernées (articles 79 et 82) et les sanctions administratives (article 83).

Notification des violations de données personnelles (articles 33 et 34)

Il existe aujourd'hui au sein de l'Union européenne une obligation de notifier aux autorités nationales de contrôle (et sous certaines conditions aux personnes concernées) les violations de données à caractère personnel. Il s'agit des « failles » dans la sécurité des fichiers de données qui peuvent entraîner la fuite ou la perte de ces données (article 4, 12°). Les statistiques démontrent que ces failles sont de plus en plus nombreuses et à l'origine de dommages de plus en plus importants pouvant aller du simple spam à l'usurpation d'identité.[2]

Prévue par la directive 2009/136/CE du 25 novembre 2009 modifiant notamment la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, cette obligation de notification ne concerne pour l'instant que le secteur des télécommunications[3].

Lorsque le Règlement général sera applicable, cette obligation s'appliquera à tous les responsables de traitement et aux sous-traitants (article 33, 1° et 2°) et non plus seulement aux fournisseurs de services de télécommunications électroniques.

Que ce soit dans le cadre actuel de la directive 2002/58 et des mesures nationales de transposition ou dans le cadre futur du Règlement général, toutes les violations de données doivent être notifiées aux autorités nationales de contrôle.

Dans la mesure où la directive laissait à ces autorités le soin d'adopter des lignes directrices et d'édicter des instructions pour la mise en œuvre de cette obligation, le contenu et la forme de cette notification, ainsi que le délai dans lequel elle doit avoir lieu varient cependant d'un Etat membre à un autre.[4] Le Règlement général

exige une notification « *dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance* » (article 33,1°) et en définit le contenu minimal seulement (article 33, 3°).

La question la plus complexe en matière de failles de sécurité est de déterminer le seuil à partir duquel la notification aux personnes concernées est nécessaire.

La directive 2002/58 prévoit une obligation de notification « *lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier.* » (article 4, 3°). La loi française prévoit une obligation de notification « *lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique* » (article 34 bis, II de la loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés). Le Règlement général prévoit que cette obligation s'appliquera « *lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique* » (article 34, 1°).

Reste à voir comment les autorités nationales des Etats membres vont appliquer cette disposition, et notamment interpréter le caractère « élevé » d'un risque même éventuel.

A noter que le Règlement général reprend et développe les cas d'exemption de cette obligation de notification aux personnes concernées, dont la mise en œuvre de mesures de protection techniques ou organisationnelles ou la communication publique (article 34, 3°).

Transfert de données (chapitre V)

Les principes gouvernant le transfert international de données demeurent : le pays destinataire doit présenter des garanties appropriées et adéquates.

Le caractère adéquat du niveau de protection assuré par le pays destinataire peut être constaté par la Commission européen dans une « décision d'adéquation » (article 45, 1°).

Si le pays destinataire n'est pas listé dans la décision d'adéquation de la Commission, il faudra mettre en œuvre des garanties spéciales (article 45, 2°). Pour cela, les clauses Contractuelles Types de la Commission européenne restent applicables. De nouvelles options seront disponibles : codes de conduite, mécanismes de certification, labels et marques, et règles d'entreprise.

Si l'un de ces mécanismes est mis en place, l'accomplissement de formalités auprès d'une autorité nationale ou l'obtention d'une autorisation de sa part n'est pas nécessaire.

Si le traitement est basé sur le consentement, celui-ci doit être explicite et la personne concernée doit avoir été informée des risques que représente le transfert (article 49, 1°, a).

Comme indiqué ci-dessus, ces règles conditionnant les transferts de données internationaux s'appliqueront également aux sous-traitants (article 44).

Recours et sanctions (chapitre VIII)

Pour l'instant, la directive se contente d'imposer aux Etats de prévoir dans leurs législations que :

- *« toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question »* (article 22) ;
- *« toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi »* (article 23).

Les personnes concernées doivent donc s'en remettre aux différentes voies de recours et régimes de responsabilité prévus par les Etats membres, ce qui peut entraîner des différences de traitement d'un Etat à un autre pour une même violation.

Le Règlement général prévoit à la place que chaque personne concernée dispose d'un véritable « droit à un recours effectif » face au responsable de traitement ou à son sous-traitant mais également à l'autorité nationale compétente (articles 78 et 79), ainsi que d'un « droit à réparation » (article 82).

Il prévoit directement les règles permettant de déterminer la juridiction compétente ; les règles de droit international privé des Etats membres n'auront donc plus de s'appliquer (articles 78 et 79).

Surtout, là où la directive donnait carte blanche aux Etats membres pour prendre « *les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive* », le Règlement général contient des conditions générales sur l'imposition d'amendes administratives par les autorités nationales de contrôle (article 83, 2°).

En fonction des obligations qui n'auront pas été respectées (par le responsable de traitement ou le sous-traitant), ces amendes pourront s'élever jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent (article 83, 4°), voire jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent (article 83, 5°).

A titre de comparaison, la loi française permet pour l'instant à la Commission nationale Informatique et Liberté d'imposer des amendes de 150 000 euros et, en cas de récidive, de 300 000 euros ou s'agissant d'une entreprise 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros (article 47 de la loi Informatique et Liberté).

[1] Le paragraphe 1 prévoit l'obligation pour le responsable de traitement de « *mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés,*

notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ».

[2] Analyse d'impact de la Commission européenne sur le projet de règlement en date du 25 janvier 2012, SEC (2012) 72 final, pp. 29-32 (en anglais seulement : http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf)

[3] Cf. article intitulé « Failles de sécurité : une nouvelle obligation de déclaration bientôt à la charge des entreprises » publié dans notre enewsletter de juin 2011.

[4] Pour la France : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles