SOMMAIRE

LE RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 avril 2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

Le règlement général sur la protection des données adopté le 27 avril 2016 a pour principal objet le renforcement du niveau de protection des données à caractère personnel, *via* l'accentuation de la responsabilité des entreprises collectrices/utilisatrices de ces données.

Ce règlement s'appliquera dans toute l'Union européenne à partir du 25 mai 2018. Aussi, les traitements déjà mis en œuvre devront, d'ici là, être conformes aux dispositions du règlement.

Certaines des dispositions du règlement sont en réalité déjà effectives en droit positif français depuis l'adoption de **la Loi n°2016-1321 pour la République Numérique du 7 octobre 2016**, laquelle a réformé la Loi Informatique et Liberté du 6 janvier 1978.

Quel que soit leur secteur d'activité, les entreprises doivent avoir à l'esprit la responsabilisation posée par le règlement et la mise en conformité autonome, en amont et tout au long de la durée de vie des traitements, et ainsi revoir leur processus interne à cet égard.

1. Sur le plan organisationnel et institutionnel

- Les entreprises seront en contact avec un « **guichet unique** », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal » (l'autorité « *chef de file* »). En France, il s'agit de **la CNIL**.
- Les autorités de protection nationales vont être regroupées au sein d'un Comité européen de la protection des données (CEPD) lequel veillera à l'application uniforme du droit et aura ainsi vocation à remplacer l'actuel G29[1] : les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne lorsqu'elles mettront en œuvre des traitements transnationaux.

2. Consentement renforcé et transparence exigée

Le consentement de l'internaute dont les données sont collectées, est au centre du règlement : les utilisateurs doivent **être informés de l'usage de leurs données** et doivent **donner leur accord pour le traitement** de leurs données, ou **pouvoir s'y opposer**. La matérialisation de ce consentement doit être claire.
La charge de la preuve du consentement incombe au Responsable de traitement.

3. De nouveaux droits :

Le droit à la portabilité des données : toute personne pourra récupérer les données qu'elle a fournies, sous une forme réutilisable et les transférer ensuite à un tiers. Les personnes doivent ainsi pouvoir retrouver la maîtrise de leurs données.

Droit d'action des associations : les associations auront désormais la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages : Toute personne ayant subi un dommage du fait de la violation du règlement, pourra demander au Responsable du traitement ou au Sous-traitant une réparation du préjudice subi.

4. Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles qu'ils traitent, les Responsables de traitements et les Sous-traitants devront **mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment** (« *accountability* »).

Conséquences :

- Suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.
- S'agissant des traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

Aussi, apparition de nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduite
- le Délégué à la Protection des Données (**DPO**)
- les Études d'Impact sur la Vie Privée (**EIVP**)

4.1 Les « Études d'Impact sur la Vie Privée » (EIVP ou PIA)

Pour tous les traitements à risque, **le Responsable de traitement** devra conduire une **étude d'impact complète**, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées.

- **Concrètement**, il s'agit notamment des **traitements de données sensibles** (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques) et de traitements reposant sur « *l'évaluation systématique et approfondie d'aspects personnels des personnes physiques* », c'est-à-dire notamment **de profilage**.

4.2 Changements concernant les transferts de données hors UE

Les Responsables de traitement et les Sous-traitants peuvent transférer des données hors UE **à la condition d'encadrer ces transferts avec des outils assurant un niveau de protection suffisant et approprié des personnes**.

En outre, les données transférées hors Union seront soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.

Ainsi, et hormis les transferts fondés sur une décision d'adéquation de la Commission Européenne, les Responsables de traitement et les Sous-traitants peuvent mettre en place :

- des règles d'entreprises contraignantes (BCR) ;
- des clauses contractuelles types approuvées par la Commission Européenne ;
- des clauses contractuelles adoptées par une autorité et approuvées par la Commission européenne.

De nouveaux outils sont aussi prévus :

- pour les Sous-traitants : la possibilité de mettre en place des **règles d'entreprises contraignantes** ;
- pour les autorités publiques : le recours à des **accords contraignants** ;
- pour les Responsables de traitement et les Sous-traitants : l'adhésion à **des codes de conduite ou à un mécanisme de certification**. Ces deux outils doivent contenir des engagements contraignants.

Enfin, une autorisation spécifique de la CNIL n'est plus requise.

5. La désignation d'un délégué parfois obligatoire

Les responsables de traitement et les Sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions

En dehors de ces cas, la désignation d'un délégué à la protection des données sera également possible (mutualisé ou externe).

Le délégué est chargé :

- **d'informer et de conseiller le Responsable de traitement ou le Sous-traitant, ainsi que ses employés ;**
- **de contrôler le respect du règlement européen et du droit national en matière de protection des données ;**
- **de conseiller l'organisme sur la réalisation d'une analyse d'impact (EIVP) et d'en vérifier l'exécution ;**
- **de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.**

6. Principe dit de « minimisation » à la charge des Responsables de traitement

Les Responsables de traitement (organismes qui déterminent les finalités et les modalités de traitement de données personnelles) devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.
Ils devront surtout veiller à limiter la quantité de données traitée dès le départ (principe de « minimisation »)

7. Obligations spécifiques aux sous-traitants

Ces obligations concernent **tous les organismes qui traitent des données personnelles pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation.** Sont notamment concernés :

- les prestataires de services informatiques (hébergement, maintenance, …),
- les intégrateurs de logiciels,
- les sociétés de sécurité informatique,
- les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données,
- les agences de *marketing* ou de communication qui traitent des données personnelles pour le compte de leurs clients.

Ces sous-traitants :

- **doivent prendre en compte la protection des données dès la conception du service ou du produit et par défaut, et mettre en place des mesures permettant de garantir une protection optimale des données,**
- **sont tenus de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability,**
- **ont notamment une obligation de conseil auprès du Responsable de traitement pour la conformité à certaines obligations du règlement (EIVP, failles, sécurité, destruction des données, contribution aux audits),**
- **doivent tenir un registre des activités de traitement effectuées pour le compte de leurs clients et désigner un DPO dans les mêmes conditions qu'un responsable de traitement.**

8. Des sanctions renforcées

Les amendes administratives sont plus sévères : elles pourront s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, **de 2% à 4% du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.
A cet égard, les Responsables de traitement et les Sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

***

La ligne de conduite des entreprises doit donc être la suivante : s'assurer qu'elles disposent des outils et de la documentation qui leur permettront d'intégrer la nouvelle logique de leur responsabilisation et de respecter les nouveaux droits des utilisateurs dont les données sont collectées et traitées.
Leurs devoirs sont donc :

- de vérifier que leurs activités de traitement sont soumises aux dispositions du règlement,
- d'auditer leur processus actuel de protection des données,
- d'encadrer par écrit leurs relations avec leurs partenaires commerciaux et/ou les entreprises du groupe,
- de désigner si nécessaire un Délégué à la protection des données,
- et de mettre en place - si besoin - un registre de traitements des données.

Gwendal Barbaut et Anne Rossoux
Avocats à la Cour IPSIDE AVOCAT

MISE EN PLACE D'UNE PROCEDURE SIMPLIFIEE DE DELIVRANCE DES BREVETS AU BRESIL

En raison d'un important arriéré accumulé par l'Office des Brevets brésilien depuis plusieurs années, l'examen au fond de la brevetabilité d'une demande de brevet par cet Office ne débute à l'heure actuelle qu'au bout de 10 ans en moyenne.

Pour remédier à cela, le Brésil va très prochainement adopter un règlement instaurant **une délivrance automatique des brevets, sans examen au fond de la brevetabilité**, pour certaines demandes actuellement en instance.

Le texte final de ce règlement n'est pas encore connu, mais il est vraisemblable que les demandes concernées seront celles déposées / entrées en phase brésilienne avant le 31 décembre 2016, qui auront été publiées et pour lesquelles la requête en examen aura été déposée avant l'entrée en vigueur du nouveau règlement (un délai de 30 jours à partir de cette date d'entrée en vigueur devrait toutefois être ouvert pour ce faire). Cette **procédure simplifiée** ne devrait toutefois pas s'appliquer aux demandes portant sur les produits et procédés pharmaceutiques, aux certificats d'addition et aux demandes divisionnaires.

En outre, il devrait être possible de requérir qu'une demande de brevet soit exclue de cette procédure simplifiée, dans les 90 jours à partir de la publication par l'Office des Brevets brésilien de la mention de l'admission de cette demande dans la procédure simplifiée.

Si vous ne souhaitez pas bénéficier de cette procédure simplifiée, il est par conséquent conseillé d'identifier dès à présent vos demandes de brevet en instance au Brésil susceptibles de bénéficier de la procédure simplifiée, afin de pouvoir déposer une requête en exclusion dans le délai prévu de 90 jours.

Par ailleurs, le dépôt d'observations concernant une demande de brevet d'un tiers, dans les 90 jours à partir de la publication de la mention de l'admission de cette demande dans la procédure simplifiée, devrait mener à l'exclusion de cette demande de brevet de la procédure simplifiée. Aussi, il est recommandé de considérer dès à présent le dépôt de telles observations pour toute demande de brevet de tiers en instance au Brésil qui pourrait vous sembler gênante.

Nous ne manquerons pas de vous tenir informés des dispositions exactes qui seront finalement adoptées, afin de vous permettre d'établir la meilleure stratégie à mettre en œuvre concernant la protection par brevet au Brésil.

Emmanuelle FOURCADE
Conseil en Propriété Industrielle Brevets

Nouvelle année

*A l'occasion de cette nouvelle année, recevez au nom du président et de l'ensemble des collaborateurs d'**IPSIDE** nos meilleurs vœux de bonheur, de santé et de prospérité.*

Que l'année 2018 vous donne à réaliser, selon vos espérances, ce que vous désirez, tant pour vous que pour vos proches.

Nos engagements : vous accompagner, rester à votre écoute et améliorer continuellement les services et la qualité que vous attendez de notre société.

ipside
Innovative IP for Creative companies

6 impasse Michel Labrousse
31100 TOULOUSE
Tél : 05 31 50 00 22

29 rue de Lisbonne
75008 PARIS
Tél : 01 80 40 08 02

7-9 Allées Haussmann
33300 BORDEAUX
Tél : 05 33 10 00 20

4 rue du Kérogan
29330 QUIMPER
Tél : 02 98 10 24 00

Centre d'affaire ACTIVA
4 allée Catherine Bourbon
64000 Pau
Tél : 05 31 50 00 22

39 rue Grange Galand
37554 St AVERTIN Cedex
Tél : 02 40 80 49 15

14, rue Raoul Perpère
Le Forum
64100 Bayonne
Tél : 05 59 15 29 25

Centre d'affaire SIAM
81 rue de SIAM
29200 BREST
tél : 02 98 05 08 07