RGPD : Le Règlement Européen sur la Protection des Données (RGPD) : quel impact pour votre développement international ?

Réunion d'information - avril 2018

Mis à jour le 07/09/2022

/

Une information d'information sur le RGPD a été proposée sur Rennes par le cabinet Fidal et la société Doptim.

Que faut-il retenir ?

Retour de Cindy Le Guern – Conseillère en Développement International

Ce sujet d'actualité brûlante a suscité l'intérêt de nombreuses entreprises bretonnes.

Le cœur de cette réglementation est la sécurisation des données.

L'objectif de ce nouveau règlement est de responsabiliser les sociétés et réguler le traitement des données et non de les empêcher de faire du business.

Ce qu'il faut retenir :

Le Règlement Général sur la Protection des Données (RGPD) ou GPDR (en anglais), sera appliqué dans l'Union européenne à partir du **25 mai 2018**.

Ce nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel, ces informations sur lesquelles les entreprises s'appuient pour proposer des services et des produits. Ce texte couvre l'ensemble des résidents de l'Union européenne.

Pour rappel, une donnée personnelle (ou donnée à caractère personnel) est une information qui permet d'identifier une personne physique, directement ou indirectement. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc.

Le RGPD introduit une nouvelle approche pour tous ceux qui détiennent de gros fichiers. Il met fin à l'obligation de les déclarer préalablement à la Commission nationale de l'Informatique et des libertés (Cnil).

Les entreprises doivent faire face à de nouveaux enjeux :

© Propriété de BCI – Reproduction interdite

BRETAGNE COMMERCE INTERNATIONAL
Avec le soutien de / With the support of
CCI BRETAGNE

– obligation de transparence renforcée

– constitution d'une gouvernance et d'un inventaire interne des données

– mise en place de nouveaux outils et d'organisation pour s'y conformer

-communication auprès des différents métiers dans l'entreprise afin de donner une culture commune de la protection des données

Concrètement, ce que vont devoir faire les entreprises :

Protéger les données personnelles :

– Mise en place du « privacy by design »: réfléchir en amont d'un projet au traitement des données personnelles (site web, objets connectés, services en ligne…)

– Obtenir un accord des intéressés pour collecter leurs informations personnelles

– N'exploiter ces données qu'à des fins en rapport avec le service rendu

– Garantir la sécurité de ces données

– Permettre leur effacement

Nommer un délégué à la protection (DPO) des données chargé de faire respecter le règlement européen. Il peut être interne ou être externalisé. Il doit avoir une bonne connaissance du SI, être de la DSI, avoir des connaissances juridiques et des contacts avec les commerciaux, les Ressources Humaines (un profil hybride)

Tenir un registre de traitement des données

– Obligatoire pour les entreprises de plus de 250 salariés (même si moins de salariés, il sera à faire si vous traitez des données sensibles, à grande échelle qui présentent un risque pour les droits et libertés fondamentales. Cela peut être un fichier excel)

– Co-responsabilité entre le responsable du traitement et son sous-traitant

-Offrir la possibilité à chacun de refuser le profilage, qui repose sur un traitement automatisé de ces données par un algorithme.

Gérer les risques

Analyse d'impact relative à la protection des données (DPIA) : nécessaire quand le risque est estimé élevé pour les droits et libertés des personnes

En cas de vol de données ou de faille de sécurité dans votre système d'information, le détenteur du fichier devra le notifier à la Cnil dans les 72 heures.

Droit à la portabilité des données

Si c'est techniquement possible, pouvoir transférer les données d'un client qui le demande vers un concurrent

© Propriété de BCI – Reproduction interdite

BRETAGNE COMMERCE INTERNATIONAL
Avec le soutien de / With the support of
CCI BRETAGNE

– Après le 25 mai, tout traitement en infraction avec le RGPD pourra déboucher sur des sanctions. Les amendes administratives pourront être très lourdes et seront fonction des manquements constatés.

Sur les transferts de données hors UE

Avec la mondialisation et l'utilisation croissante des nouvelles technologies, le nombre de transferts de données hors de France ne cesse de croître. Or, en principe, les transferts de données à caractère personnel hors du territoire de l'UE (y compris l'Islande, le Liechtenstein et la Norvège), sont interdits à moins que le pays ou le destinataire n'assure un niveau de protection suffisant.

Pour les transferts de données personnelles vers ces pays, plusieurs outils ont été développés pour permettre aux acteurs d'apporter un niveau de protection suffisant : les r**ègles internes d'entreprise (ou BCR)**, les **Clauses Contractuelles Types (CCT).**

La loi prévoit également des exceptions permettant de transférer des données vers des pays tiers sans qu'il n'existe pour autant un niveau de protection suffisant.

Dans la majorité des cas, **il est préconisé aux entreprises, d'encadrer leur transfert des données à caractère personnel hors UE par les CCT**. En effet, si vous signez avec votre partenaire situé hors de l'UE les CCT élaborées par la Commission européenne sans les modifier, vous n'aurez qu'à les tenir à disposition de la CNIL, en cas de contrôle, pour que votre transfert soit valablement encadré juridiquement, à charge cependant pour vous de vous assurer que votre partenaire respecte bien les stipulations desdites CCT.

Enfin, si vous souhaitez transférer des données à caractère personnel vers les Etats-Unis, vous pouvez également vérifier si l'entité destinataire desdites données à adhérer au « Privacy Shield ».

En tout état de cause, il convient pour chaque entreprise souhaitant transférer des données hors de l'UE de choisir et utiliser la base légale qui encadrera valablement ce type de transfert.

Mon conseil avant le 25/05 :

" Commencer à devenir *RGPD Compliant* . C'est un travail continu ! "

Le RGPD est là pour raisonner, sécuriser le traitement des données. Il faut le voir comme un outil de valorisation. Pour justifier qu'on est conforme au RGPD, le plus important est de mettre en place des actions et de prouver par une documentation écrite que vous assurez une protection des données en continu.

Les entreprises sont « surchargées » de données. Demain, l'idée est d'avoir l'essentiel et donc de faire le ménage afin d'avoir un traitement conforme à la nouvelle réglementation.

On ne peut pas garder éternellement des données. Il va falloir déterminer des intérêts légitimes et raisonner le traitement des données essentielles.

Pour que ce soit moins opaque, voici un exemple pour aller vers la conformité au RGPD :

– Faire un inventaire des traitements de données au sein de chaque service

© Propriété de BCI – Reproduction interdite

BRETAGNE COMMERCE INTERNATIONAL
Avec le soutien de / With the support of
CCI BRETAGNE

– Evaluer les pratiques dans votre société pour être compliant

– Enlever les données obsolètes dans les SI

– Vigilance sur les terminaux des personnes en déplacement (les commerciaux doivent avoir très peu de données dans leurs mobiles lors de leurs déplacements).

– Mise en place du registre, qui devra vivre en fonction des traitements que vous faites

– Il y aura des évolutions, la réglementation est mouvante. Il y a certes ce règlement européen mais la loi Française va aussi rajouter d'autres éléments.

– Modifier vos CGV, votre politique de confidentialité

– Revoir les clauses de confidentialité passées avec les sous-traitants

Vous rendre sur le site de la CNIL : les outils sont très didactiques

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

En conclusion, l**a finalité est clairement de créer une Union Européenne sans barrières sur le terrain de la donnée personnelle et avoir aussi une force de frappe face aux Gafa**.

Typiquement, même si la maison mère de Facebook n'est pas au sein de l'UE, ils vont être soumis à cette nouvelle réglementation européenne et vont devoir s'y conformer. Aussi, des entreprises américaines comme Uber ou les sites de e-commerce chinois doivent donc respecter le RGPD dès lors qu'il cible les résidents européens.

© Propriété de BCI – Reproduction interdite

BRETAGNE COMMERCE INTERNATIONAL
Avec le soutien de / With the support of
CCI BRETAGNE

© Propriété de BCI – Reproduction interdite

BRETAGNE COMMERCE INTERNATIONAL
Avec le soutien de / With the support of
CCI BRETAGNE