CHAMBRE DE COMMERCE LUXEMBOURG

HOUSE OF ENTREPRENEURSHIP
powered by the Luxembourg Chamber of Commerce

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

QUI, QUOI, COMMENT ? RAPPELS ÉLÉMENTAIRES

QUI ?

TOUTES LES ENTREPRISES SONT CONCERNÉES PAR LE RGPD...

… dès lors qu'elles traitent des *« données à caractère personnel »*, c'est-à-dire des informations se rapportant à une personne physique identifiée ou identifiable directement ou indirectement (personne concernée), qu'elle agisse en qualité de *« responsable de traitement[1] »* ou de *« sous-traitant[2] »*. Sont aussi bien concernées par la mise en conformité les personnes physiques ou morales, les sociétés multinationales ou les PME, quel que soit leur secteur d'activité (assurances, banques, industrie, commerce, Horeca).

A titre d'exemples de *« traitements de données »*, l'on peut citer la collecte, l'enregistrement, la conservation, la modification, la consultation, l'utilisation, la communication par transmission, l'effacement ou encore la destruction de données peu importe que ces traitements soient effectués au moyen d'outils informatiques ou de support papier.

QUOI ?

CONNAÎTRE LES DONNÉES TRAITÉES PAR SON ENTREPRISE

Toute entreprise qui traite des données a la qualité de *« responsable de traitement »* et est donc censée connaître l'ensemble des données qu'elle traite. Il peut s'agir d'un nom, un numéro de sécurité sociale, une date de naissance, une adresse électronique, un numéro de téléphone, un compte bancaire, des données de localisation, une plaque d'immatriculation, un identifiant en ligne…

Pour cela, il convient de faire **un inventaire complet et précis** de l'ensemble des traitements de données effectués au sein de l'entreprise (salariés, clients, fournisseurs, prospects…).

COMMENT ?

NE COLLECTER QUE LES DONNÉES PERTINENTES

L'entreprise doit mettre en place de bonnes pratiques afin de ne collecter que les données pertinentes et pour une durée cohérente, afin de limiter au maximum l'impact sur la vie privée.

Il ne faut pas collecter ou conserver des données « pour le cas où… »

Concrètement, l'entreprise doit notamment mettre en œuvre les mesures techniques et organisationnelles appropriées afin de **garantir une protection par défaut** notamment en **limitant la quantité** de données collectées à ce qui est strictement nécessaire ainsi que la **durée de conservation** (principe de minimisation).

S'ASSURER QUE LES TRAITEMENTS SONT LICITES

Chaque traitement de données effectué par l'entreprise n'est licite que s'il est[3] :

- **nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie (ex : traitement de données personnelles d'un consommateur dans le cadre de l'exécution d'un contrat de vente ou encore d'un client ayant réservé une chambre ou une table dans le cadre d'une prestation hôtelière ou de restauration), *ou*
- **nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis (ex : obligation de l'employeur de procéder à la retenue d'impôt sur le revenu des salariés), *ou*
- **fondé sur le consentement libre, spécifique, éclairé et univoque de la personne concernée** (ex : données personnelles librement fournies par un client à un commerçant afin de bénéficier d'une carte de fidélité et/ou d'être informé d'offres promotionnelles ou de ventes privées).

1 Le responsable de traitement est défini comme « la personne physique ou morale (…) qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. »

2 Le sous-traitant est défini comme « toute personne physique ou morale (…) qui traite des données à caractère personnel pour le compte du responsable de traitement » (tels qu'une fiduciaire dans le cadre du traitement des salaires ou un data center pour l'archivage informatique).

3 Il existe encore trois autres fondements légaux : la sauvegarde des intérêts vitaux de la personne concernée, l'intérêt public ou l'exercice de l'autorité publique, l'intérêt légitime poursuivi par le ou un tiers.

Comme la charge de la preuve incombe au responsable de traitement, une attention particulière doit être portée au respect de cette règle.

Le consentement doit désormais être donné par un **acte positif et clair**. Il n'y a pas de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. L'obtention du consentement peut se faire notamment en cochant une case lors de la consultation d'un site internet (« *opt-in* »), ou au moyen d'une déclaration écrite. Des règles spécifiques existent pour les mineurs de moins de 16 ans.

La personne concernée a le droit de retirer son consentement à tout moment.

C'est au moment de recueillir les données personnelles d'une personne que l'entreprise doit obtenir son consentement explicite. Il en va de même de l'obligation d'information des personnes concernées détaillée ci-après (en vertu des principes de transparence et de loyauté).

INFORMER LES PERSONNES CONCERNÉES

L'entreprise doit informer la personne concernée **des conditions du traitement** qu'elle compte effectuer sur ses données et notamment préciser dans quel but le traitement est réalisé, sur quel fondement légal, quelle sera la durée de conservation des données, l'existence éventuelle de transferts de données hors de l'UE et indiquer l'existence des différents droits dont elle dispose (droit d'accès, droit de rectification, droit à la limitation, droit d'opposition, droit à l'effacement - encore appelé « droit à l'oubli » -, droit à la portabilité des données).

Le **droit à l'oubli** n'est que le renforcement du droit à l'effacement qui est étendu à des hypothèses plus nombreuses afin de tenir compte de l'environnement numérique (d'où sa nouvelle dénomination). Le droit à l'oubli n'est pas un droit absolu et peut être invoqué par la personne concernée principalement si les données ont fait l'objet d'un traitement illicite, si le consentement sur lequel était fondé le traitement est retiré et qu'il n'existe pas d'autre fondement juridique au traitement ou encore si les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées.

Il convient notamment de **sensibiliser le personnel** sur l'existence de ces droits et de le préparer aux demandes des personnes concernées, d'**adapter le message d'avertissement** dans toute correspondance vis-à-vis de l'extérieur en respectant la liste exhaustive d'informations à fournir (« Vos données sont traitées conformément … »).

SÉCURISER LES DONNÉES

Les risques sont nombreux : perte de données (perte du support, effacement ou destruction volontaire ou non), vol de données, consultation illégale de données (faille informatique ou stockage non-sécurisé des données).

L'entreprise doit prendre les **précautions nécessaires tout au long du cycle de la gestion des données** qu'elle traite (depuis la collecte jusqu'à la destruction) afin de garantir la sécurité des données, notamment en sécurisant les serveurs et les postes de travail (virus) ainsi que l'informatique mobile, en archivant de manière sécurisée, en limitant les accès aux seules données dont un utilisateur a besoin, en ayant recours à la pseudonymisation ou au cryptage des données...

L'entreprise a l'obligation de réaliser une **analyse d'impact en matière de vie privée si le traitement présente un risque élevé** dans les cas où elle (i) effectue une évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé (y compris le profilage), (ii) procède à un traitement à grande échelle de catégories particulières de données (en matière de santé, pénales) ou (iii) effectue une surveillance systématique à grande échelle d'une zone accessible au public. L'analyse d'impact doit être menée avant la mise ne œuvre du traitement.

MAIS ENCORE

TENIR UN REGISTRE DES ACTIVITÉS DE TRAITEMENT[4]

C'est une obligation pour les entreprises ayant moins de 250 salariés **dès lors que le traitement n'est pas occasionnel ou est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.**

De même, c'est une obligation pour les entreprises comptant 250 salariés et plus.

A titre d'exemples, ne sont pas des traitements occasionnels, les traitements de données liés à la gestion de la clientèle, à la gestion du personnel ou encore à la gestion des fournisseurs. La prudence devrait donc conduire à recommander à tous les responsables de traitement de mettre en place un tel registre.

Ce registre doit contenir, **pour chaque traitement**, (i) le nom et les coordonnées du responsable du traitement, du représentant du responsable du traitement et du délégué à la protection des données, (ii) les finalités du traitement, (iii) une description des catégories de personnes visées par le traitement et des catégories de données, (iv) les catégories de destinataires et de sous-traitants auxquels les données ont été ou seront transmises, (v) le cas échéant, les transferts de données vers des pays tiers à l'UE, (vi) dans la mesure du possible, les délais prévus pour l'effacement des données, (vii) la description générale des mesures de sécurité techniques et organisationnelles.

Commencer par faire un inventaire de l'ensemble des traitements de données effectués au sein de l'entreprise (salariés, clients, fournisseurs, prospects…) et en étoffer le descriptif de manière à fournir les informations devant figurer dans le registre.

L'entreprise a l'obligation de mettre le registre à la disposition de la CNPD si celle-ci en fait la demande.

4 Pour le responsable de traitement mais aussi pour le sous-traitant.

AGIR EN CAS DE « VIOLATION DE DONNÉES »

La perte ou le vol de données de même que l'accès intempestif aux données constituent autant d'exemples de violation de données personnelles.

Si la violation de données présente un **risque pour les droits et libertés des personnes concernées**, l'entreprise doit la notifier à la CNPD dans les 72 heures au plus tard après en avoir pris connaissance et dans les meilleurs délais à l'égard de la personne concernée.

Les informations demandées dans le formulaire de notification à la CNPD peuvent servir de base pour déterminer si la violation présente un risque pour les personnes concernées.

Mettre en place des procédures de détection de toute violation de données (remontée et centralisation de l'information) mais aussi des procédures de notification (auprès de la CNPD et de la personne concernée) et d'enquête post-incident (afin d'identifier les causes et responsabilités).

Prévoir une sensibilisation du personnel afin qu'il acquiert le réflexe de signaler tout incident plutôt que de l'étouffer.

RECOURIR À DES SOUS-TRAITANTS QUI PRÉSENTENT DES GARANTIES SUFFISANTES

L'entreprise doit, dans un premier temps, identifier l'ensemble des sous-traitants qui traitent des données personnelles pour son compte (ex : fiduciaire pour les salaires, prestataire spécialisé dans l'archivage, société de gardiennage…) et s'assurer que le traitement de données est bien régi par un contrat écrit (ou tout autre acte juridique) liant le sous-traitant au responsable de traitement.

Dans ce contexte, elle doit revoir le contenu du contrat de manière à définir l'objet, la durée, la nature et la finalité du traitement ainsi que le type de données et les catégories de personnes concernées. L'entreprise doit également vérifier si le sous-traitant a lui-même recours à un « sous sous-traitant » pour tout ou partie du traitement et si, le cas échéant, cela implique un transfert de données hors de l'UE.

Le sous-traitant ne doit pas recourir à un « sous sous-traitant » sans l'autorisation écrite préalable du responsable de traitement.

DÉSIGNER UN « DATA PROTECTION OFFICER » (DPO) : OUI OU NON ?

Désigner un DPO est une obligation pour le responsable de traitement et le sous-traitant lorsque les activités de base consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou leurs finalités, exigent un **suivi régulier et systématique à grande échelle des personnes concernées.**

Les autorités nationales de contrôle ont une interprétation large des notions d'*« activité de base »* et *« à grande échelle »*, et étendent autant que possible les hypothèses de désignation à retenir. Il convient notamment de prendre en considération le nombre de personnes concernées, le volume de données et/ou le spectre des catégories de données, la durée ou la permanence de l'activité de traitement, l'étendue géographique de l'activité de traitement.

Dans tous les cas, l'entreprise doit faire l'analyse de savoir si la désignation d'un DPO est obligatoire ou non et **documenter la conclusion** qui en ressort. Si oui, il est recommandé de le désigner au plus vite afin de l'associer dès que possible au processus de mise en conformité.

Le DPO peut être **interne** (salarié répondant à un profil particulier) ou **externe** (prestataire spécialisé), ce dernier devra alors travailler avec une personne de contact au sein de l'entreprise.

A NOTER ENCORE : À COMPTER DU 25 MAI 2018

ABROGATION DE LA LOI MODIFIÉE DU 2 AOÛT 2002, CE QUI IMPLIQUE LA DISPARITION :

>> des procédures de notification et d'autorisation préalable auprès de la CNPD

>> des sanctions pénales en cas d'infractions à la loi modifiée du 2 août 2002

CHANGEMENT DE PARADIGME AVEC L'ENTRÉE EN VIGUEUR DES NOUVELLES DISPOSITIONS, MARQUÉ PAR :

>> **le principe d'*« accountability »*** qui responsabilise le responsable de traitement et le sous-traitant qui doivent être en mesure de démontrer (si la CNPD le demande) que les traitements de données personnelles qu'ils effectuent sont conformes au RGPD

>> les **sanctions financières** lourdes en cas de non-respect des dispositions du RGPD, pouvant aller 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 (le montant le plus élevé étant retenu)

HOUSE OF ENTREPRENEURSHIP
powered by the Luxembourg Chamber of Commerce

HOUSE OF ENTREPRENEURSHIP
14, rue Erasme
L-1468 Luxembourg-Kirchberg
T. (+352) 42 39 39 330
info@houseofentrepreneurship.lu
houseofentrepreneurship.lu