RGPD - Règlement Général Européen sur la Protection des Données (en français)
GDPR - General Data Protection Regulation (en anglais)

par

Astove Consulting

Introduction

Le Règlement Général Européen sur la Protection des Données (RGPD) entrera en vigueur le 25 mai 2018 avec pour objectif d'assurer la sécurité et la libre circulation des données au sein de l'Union Européenne.

Toutes les entreprises utilisant des données personnelles de citoyens européens sont impactées par cette règlementation et sont passibles d'amendes en cas de non respects des dispositions pouvant atteindre 20 millions d'euros ou 4% de leur chiffre d'affaires annuel mondial.

Si vous travaillez avec des particuliers, vous entrez dans le cadre d'application de cette nouvelle règlementation.

La mise en conformité implique des changements profonds dans la gestion des données personnelles que vous collectez, dans leurs traitements et dans la transparence sur l'utilisation de ces données vis-à-vis des personnes concernées. Les collaborateurs doivent, à ce titre, être informés des droits et obligations en matière de collecte, d'accès et de rectification ou de suppression des données personnelles.

En effet, contrairement aux directives précédentes de la CNIL (Commission Nationale de l'Informatique et des Libertés), la réglementation européenne prévoit que l'entreprise soit responsabilisée par rapport aux différents traitements des données personnelles qu'elle effectue, ainsi que ses sous-traitants. Dans ce cadre, ce n'est plus aux autorités compétentes d'établir les manquements aux règles, mais à l'entreprise collectant et traitant ces données de prouver le bon respect de la règlementation.

Si vous êtes concernés, il est grand temps de prendre en considération les impacts de cette réglementation et de mettre en place, avant qu'il soit trop tard, des mesures pour préparer la mise en conformité de votre entreprise.

Cet article a pour unique vocation de vous informer et vous alerter sur cette nouvelle réglementation afin que vous preniez la mesure de l'ampleur des travaux qui sont à réaliser pour vous mettre en conformité.
Il ne constitue aucunement une référence en la matière et ne doit pas être considéré comme tel.
Nous vous invitons fortement à consulter le site de la CNIL désignée comme l'autorité compétente en France pour connaitre toutes les démarches et règlementations.

Quelles sont les entreprises concernées ?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. ». Cela concerne donc tout établissement dans l'Union européenne ou tout établissement proposant une offre de services, des biens s'adressant à des personnes qui se trouvent sur le territoire de l'Union européenne.

Quelles sont les données concernées ?

Selon le règlement, il s'agit de « toute information concernant une personne physique identifiée ou identifiable », que les données soient collectées directement ou indirectement. Ainsi, des données telles que les numéros de téléphone, adresses email… sont concernées.

Quelles sont les obligations des entreprises ?

Le règlement supprime l'obligation de déclaration préalable de la loi « Informatique et libertés », mais impose en contrepartie un certain nombre d'obligations.

L'entreprise doit en l'occurrence prouver qu'elle protège les données dès la collecte de ces dernières (CRM, géolocalisation, ERP, …), mais aussi dans les contrats passés avec les sous-traitants qui peuvent être amenés à visualiser ou utiliser les données concernées.

Les entreprises sont également soumises à des obligations de transparence sur la finalité précise des données collectées envers les personnes concernées. Le but est de réduire la collecte aux seules données exclusivement nécessaires à la finalité du traitement. Il s'agit également de limiter le délai de conservation des données personnelles.

Enfin, pour le secteur public ou les entreprises privées qui font des traitements réguliers et systématiques à grande échelle, l'obligation de nommer un DPD (Délégué à la Protection des Données) ou DPO (Data Protection Officer) qui sera le garant de la conformité au règlement.

Les nouveaux principes introduits par le RGPD

« Privacy by design » : Les données personnelles doivent être identifiées en tant que telles dans l'application ou le système qui permet de les collecter afin de limiter et sécuriser leur accès.

« Security by default » : les données utilisées doivent être réduite au strict minimum nécessaire à la finalité du traitement.

« Accountability » : L'entreprise doit disposer d'un historique décrivant tous les traitements et modifications appliqués aux données personnelles afin de démontrer la protection de ces dernières.

Les actions à mener pour se préparer à la règlementation Européenne

La CNIL présente les 6 étapes primordiales pour préparer votre entreprise à ces nouvelles dispositions en matière de sécurité et de protection des données personnelles.

1. Nomination d'un DPD ou DPO (en remplacement du CIL)

DPD = Delegue a la Protection des Donnees (en français)

DPO = Data Protection Officer (en anglais)

CIL = Correspondant Informatique et Libertes

L'obligation de désigner un DPD en 2018 s'applique :

- aux organismes publics
- aux sociétés dont l'activité entraine une utilisation régulière des données personnelles à grande échelle ou des données dites « sensibles » ou faisant référence aux origines raciales ou ethniques, à la religion, aux opinions politiques, philosophiques, syndicales, à la génétique, aux données biométriques, à la santé ou la sexualité des personnes

Cependant, même si vous n'entrez pas strictement dans ce cadre, Il est toutefois recommandé de désigner une personne qui sera chargée de comprendre et faire respecter les obligations de la nouvelle réglementation européenne.

Attention, car même si vous n'êtes pas dans l'obligation de nommer un DPD, vous êtes tout de même dans l'obligation de prouver le respect de la réglementation.

Son rôle en matière de protection des données sera donc :

- Informer et conseiller les responsables des traitements des données ainsi que les sous-traitants
- Contrôler le respect de la réglementation
- Mener ou commander des études d'impact relatives à la protection des données
- Coopérer avec les autorités de contrôle

Pour réaliser cela, après s'être informé des nouvelles obligations, il devra sensibiliser les décideurs sur les impacts liés à la mise en conformité, réaliser l'inventaire des traitements de données, concevoir des actions de mise en conformité et de sensibilisation des employés et collaborateurs.

Le DPD désigné ne peut pas, et ne doit pas, être le RSI (Responsable du Système d'information) ou DI (Directeur Informatique) car il doit avoir une vision externe et indépendante par rapport aux différents traitements de collecte et d'utilisation des données. Le DPD peut être salarié de la société mais également un acteur externe (juriste par exemple).

2. Cartographie des traitements de données personnelles

La première étape consiste à répertorier tous les traitements (1) réalisés sur les données personnelles, les catégories de données personnelles (2), les objectifs du traitement (3), les acteurs (4) internes ou externes opérant sur les données et enfin les flux de données (5) (origine/destination)

(1) L'article 4 du règlement définit un traitement comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction; »

(2) Toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

(3) Objectif principal de l'utilisation des données personnelles comme par exemple : la gestion des recrutements, la gestion des clients, des enquêtes de satisfaction, surveillance des locaux, etc.

(4) Il est important d'identifier tous les acteurs, prestataires, sous-traitants ou fournisseurs avec lesquels vous échangez des données à caractère personnel afin de vérifier et mettre à jour les clauses de confidentialités des contrats qui vous lient.

(5) L'idée est de connaitre notamment les transferts de données hors de l'union européenne

Pour chaque traitement, il sera nécessaire d'établir un registre (historique) de toutes les actions réalisées sur les données.
La CNIL met à disposition un exemple de registre (ci-dessous) permettant d'établir un historique des traitements réalisés les données

Identification du traitement				Acteur(s)	Finalité du traitement	Transferts hors UE	Données sensibles
Nom	Référence ou N°	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui / Non	Oui / Non

3. Identifier et prioriser les actions à mener

En fonction de la cartographie des traitements et après avoir identifié les données personnelles utilisées, vous devrez pour chacun d'eux identifier les actions à mener pour une mise en conformité avec la règlementation actuelle et à venir.
Il faudra ensuite prioriser les actions en fonction de la nature des données utilisées et de l'impact des traitements.

Pour chaque traitement, il est donc nécessaire de :

- s'assurer que les données collectées sont strictement nécessaires à la finalité du traitement.
  (dans le cas contraire, les données non-essentielles doivent être supprimées et ne plus être collectées)

- identifier la base juridique qui doit encadrer votre traitement
  (consentement de la personne, contrat, obligation légale…)

- mettre à jour (ou ajouter) les mentions d'information afin qu'elles soient conformes à la réglementation
  (notamment sur l'utilisation faite des données, les droits de rectification et de modification et les droits de suppression des données personnelles)

- vérifier que l'ensemble des acteurs et notamment les sous-traitants connaissent les nouvelles obligations et leurs responsabilités.
  (modification des clauses contractuelles en matière de sécurité, de confidentialité et de protection des données personnelles)

- vérifier (ou mettre en place) les modalités d'exécution des droits des personnes concernées
  (accès, rectification, suppression, portabilité…)

- vérifier (ou mettre en place) les mesures de sécurité adéquates à la protection de données personnelles

De plus, vous devez adopter des précautions et des mesures particulières dans le cas où :

- vous manipulez des données dites « sensibles » (origine raciale ou ethnique, opinions politiques, philosophiques ou religieuses, appartenance syndicale, santé ou orientation sexuelle, génétiques ou biométriques, infraction ou de condamnation pénale, concernant des mineurs)

- le traitement a pour objet ou effet la surveillance systématique à grande échelle ou l'évaluation approfondie et systématique (profilage) des personnes physiques conduisant à des actions à caractère juridique ou l'affectant de manière significative

- vous transférez des données hors de l'union européenne

4. Gérer les risques

Si des traitements de données personnelles sont susceptibles de générer des risques pour les droits et libertés des personnes physiques concernées, vous devez, pour chacun de ces traitements, mener une étude d'impact sur la protection des données PIA (Privacy Impact Assessment).

L'objectif de cette étude est d'évaluer les risques encourus par les personnes concernées et mettre en œuvre les actions correctives permettant leurs protections en adéquation avec la réglementation. Elle doit, en outre, définir le cadre d'impact sur la vie privée des personnes concernées et démontrer que les principes fondamentaux du règlement sont correctement respectés

Cette étude peut conduire à modifier vos traitements ou vos applications utilisant les données personnelles, supprimer la collecte de certaines données non pertinentes, mettre en place des systèmes de sécurité et/ou de cryptage au sein de l'entreprise et de l'hébergement des données…

5. Définition et mise en place de processus internes

Les traitements et applications doivent prendre en compte la protection des données personnelles (en minimisant la collecte de données en fonction de la finalité, gestion cookies, durée de conservation des données, mentions d'information des personnes concernées et recueil de leur consentement, sécurité et confidentialité des données).

Il est également nécessaire de sensibiliser l'ensemble des collaborateurs à la protection des données, à la collecte et remontée d'information, aux droits des personnes quant à leurs droits d'accès, de rectification, d'opposition, etc.
Dans la mesure où les données ont été collectées par voie électronique, les droits doivent également pouvoir être exercés par le même support.
Les procédures d'exercice de ces droits doivent être clairement définies et opérationnelles.

Enfin, il est indispensable de définir les procédures à appliquer en cas de violation des données, en prévoyant notamment la déclaration auprès de l'autorité de protection des données compétente dans les 72 heures après la prise de connaissance du problème et la notification des personnes concernées dans les meilleurs délais.

6. Documenter et justifier la conformité au règlement

Contrairement à la CNIL avec des directives et des sanctions guères dissuasives, le RGPD prévoit des obligations, des contrôles et des sanctions financières relativement lourdes.
Contrairement à la CNIL dans laquelle cette dernière devait démontrer le manquement aux règles, c'est maintenant aux entreprises de prouver qu'elles sont en conformité avec le règlement.

Le DPD devra donc constituer et regrouper la documentation nécessaire en présentant notamment les éléments suivants :

Sur les traitements des données personnelles

- Registre des traitements (ou catégories d'activités de traitements pour les opérations en sous-traitances)
- Analyse d'impact sur la protection des données (PIA) pour les données « sensibles » ou présentant un risque important pour le respect de la vie privée
- L'encadrement des transferts de données hors de l'Union Européenne

Sur l'information des personnes

- Les mentions d'information
- Les modèles de recueil du consentement des personnes
- Les procédures mise en place pour l'exercice des droits

Sur les contrats qui régissent les rôles et responsabilités des acteurs

- Contrats avec les sous-traitants
- Procédures internes en cas de violation des données
- Preuves que les personnes concernées ont donné leur consentement

Conclusion

La mise en conformité à cette règlementation européenne, en application au 25 mai 2018, devient une réalité inéluctable pour chaque entreprise qui collecte des données à caractère personnel, même s'il s'agit uniquement des informations contenu dans votre gestion commerciale ou votre CRM et même s'il s'agit de données indispensables à votre activité.
Compte-tenu de la volonté de l'Union européenne de s'adapter aux nouvelles réalités du numérique et des contrôles et sanctions annoncées, il est important de préparer votre entreprise afin d'être en conformité le plus rapidement possible.

Nous vous conseillons de consulter le site de la CNIL (www.cnil.fr) afin de prendre connaissance de toutes les dispositions relatives à cette règlementation.

En tant qu'éditeur ASTOVE Consulting est directement concernée par cette réglementation, afin de vous aider à anticiper les différentes problématiques et vous fournir des outils respectueux des règlementations en vigueur.
Si vous vendez des produits ou services à des particuliers, plusieurs de nos solutions Fileco® (VD, ERP, CRM) peuvent être utilisées dans la collecte et le traitement de données concernant vos clients qui entrent dans le cadre d'application de cette règlementation.

Concernant nos prestations et les opérations de maintenance : Notre collaboration et nos contrats de maintenance comprennent une clause de confidentialité. Tous nos collaborateurs ont également accepté et validé une clause de confidentialité dans leur contrat de travail. Dans ce cadre, nous vous garantissons sans équivoque la confidentialité de vos données, la non-utilisation et la non-divulgation de ces données à des tiers. Sur votre demande, si vous le jugez nécessaire, nous pourrons réaliser un avenant au contrat si vous souhaitez préciser certains points sur ce sujet.

Concernant les données enregistrées dans nos bases de données : Nos solutions utilisent la base de données Microsoft SQL/Server réputée fiable et robuste. Nous nous efforçons d'appliquer les mises à jour et services packs recommandés sur les versions que vous utilisez, notamment en matière de sécurité. Les accès aux données sont protégés par des codes et mot de passe cryptés (algorithme RC5 sur 128 bits).
Les données relatives aux clients et aux contacts sont strictement limitées aux besoins induits par l'application. ASTOVE ne saurait être tenu responsable de toute information de quelque nature que ce soit figurant dans les zones d'observations ou de commentaires et qui sont à la libre appréciation des utilisateurs. De la même manière, ASTOVE ne saurait être tenu responsable de l'utilisation ou interprétation faite sur les données par la société via les différentes extractions (tableaux de bord, statistiques, export Excel…).

Concernant les hébergements : Les serveurs sont hébergés par notre partenaire AGOM garant de la sécurité. Les serveurs sont sécurisés par des accès contrôlés via des Firewall avec des restrictions de port et de plage d'adresse IP.

Nous restons à votre écoute et à votre disposition pour répondre vos questions (ou remarques) sur nos prestations ou solutions : contact@astove.com

Sources utilisées pour ce document

CNIL
https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

ZDNet
http://www.zdnet.fr/dossier/rgpd-tout-comprendre-4000237620.htm

DAF Mag
http://www.daf-mag.fr/Thematique/droit-fiscalite-1031/Breves/Reglement-europeen-protection-donnees-nouvelles-regles-gestion-donnees-311739.htm