LIVRE BLANC RGPD

Règlement Général européen sur la Protection des Données

Axilis

xerox Concessionnaire

Your Team Group

Résumé

Le RGPD concerne la protection des données personnelles dans l'Union Européenne. Celui-ci définit un cadre strict à la collecte, au traitement et à la gestion des informations privées. Désormais, les établissements publics et les entreprises doivent intégrer la protection des données et des documents confidentiels dans la conception et l'organisation de leurs systèmes d'information sous peine de se voir infliger une lourde amende.

Décidé en 2015, le RGPD entrera en vigueur le 25/05/2018. Les entreprises doivent se tenir prêtes dès à présent !
Ce document a pour ambition de vous informer sur cette nouvelle réglementation, sur l'importance de positionner la protection des données au centre des préoccupations de sécurité.
A l'heure où les volumes d'informations échangées et stockées croissent de façon exponentielle, il apparaît nécessaire et primordial de protéger ses informations sensibles ou de les détruire de manière sécurisée.

De prime abord, il est important de rappeler que lorsque l'on parle de données personnelles, on inclut les informations concernant les :

- Employés
- Clients
- Prospects
- Partenaires
- Fournisseurs

La réglementation s'applique aussi bien aux données numériques qu'aux documents papier.

Le RGPD en quelques mots

Ce nouveau règlement Européen à destination des entreprises harmonise, simplifie et accroît la protection des données sensibles. Il a pour but de renforcer et d'unifier la protection des données à caractère personnel des individus des 28 Etats Membres.
Celui-ci s'appliquera à tous les établissements publics ou privés, qui collectent, traitent et stockent des documents confidentiels dont l'utilisation peut directement ou indirectement identifier une personne.
Enfin, ce dernier repose sur le droit fondamental inaliénable que constitue, pour chaque citoyen, la protection de sa vie privée et de ses données personnelles. La notion d'identification a ici toute son importance : si une entreprise ne peut déterminer directement l'identité d'un individu, un tiers peut potentiellement le faire...

Axilis xerox Concessionnaire
Your Team Group

4 principales directives du RGPD

- Oblige les organisations à demander l'autorisation explicite de collecte d'informations privées auprès de l'utilisateur final. Il devra être possible de prouver que l'accord a bien été donné.

- Impose aux responsables des données de prendre en compte les exigences relatives à la protection des données personnelles. De plus, ces derniers doivent mettre en œuvre toutes les règles techniques et d'organisation, indispensables pour sécuriser ces informations, et ce dès la conception des produits, services ou systèmes exploitant des données à caractère personnel (Privacy by design).

- L'obligation de déclarer les piratages ou fuites de données dans les 72 h qui suivent l'incident (aux autorités et personnes concernées).

- L'obligation de désigner un « Data Protection Officer » (DPO) ou Délégué à la protection des données en charge du contrôle de la conformité des traitements (pour les entreprises de plus de 250 salariés).

De plus, l'entreprise veillera à ce que les données secrètes soient en permanence — c'est-à-dire à tout moment et en tous lieux — sécurisées, afin de lutter contre les risques de :

- Perte
- Vol
- Divulgation

A qui s'adresse le RGPD ?

A tous les acteurs économiques, voire sociaux, à savoir :

- Entreprises
- Associations
- Administrations
- Collectivités locales
- Syndicats d'entreprises

Axilis xerox Concessionnaire
Your Team Group

Quels sont les objectifs du RGPD ?

L'objectif général est de redonner aux citoyens le contrôle de leurs informations confidentielles, tout en unifiant les réglementations relatives à la protection de la vie privée dans l'Union Européenne.

L'entreprise ne pourra transférer en dehors de l'Union Européenne les documents confidentiels que selon un cadre strictement défini par le règlement et n'engager pour le traitement de ces données que des entreprises tierces offrant les garanties nécessaires pour répondre à ces obligations.

Les derniers ajouts et récentes modifications vont entraîner de profonds changements en matière de collecte de traitement des données personnelles et auront probablement un impact global sur le fonctionnement des entreprises.

La protection des données : un enjeu clé

De nos jours, les pertes et vols de données personnelles sont, à l'image de l'évolution du stockage, de plus en plus nombreux, ce qui motive le renforcement du règlement appuyé par des amendes dissuasives (jusqu'à 4 % du chiffre d'affaires annuel mondial).

Le RGPD sanctuarise ainsi de nombreuses dispositions qui doivent être suivies, faute d'être sanctionnées. Il s'agit précisément du traitement et de la sécurisation des données.

Le RGPD implique aussi de nommer un délégué à la protection des données : un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle. Ce personnage-clé occupe donc un rôle central et veille à la bonne application des règles définies par la loi. On notera que les sociétés peuvent désigner un délégué interne ou externe à leur structure. Ce référent devra ensuite mettre en œuvre une démarche globale visant à cartographier l'existant, prioriser les actions à mener pour se conformer aux obligations, gérer les risques, mettre en place des procédures internes garantissant la prise en compte de la protection des données à tout moment et enfin documenter les traitements des données personnelles.

Qui dit obligations dit sanctions !

Que risquent les entreprises en cas de non-respect de la réglementation ?

Attention ! Les entreprises doivent d'ores et déjà se tenir prêtes. Sans quoi, elles s'exposent à de lourdes conséquences financières qui pourront ternir leur réputation et leur image.

Des amendes ou sanctions sévères sont prévues en cas d'infraction : **l'entreprise encourt une amende pouvant atteindre 4% du chiffre d'affaires annuel mondial limité à 20 millions d'euros**, ce qui représente un coût colossal pour la plupart des organisations.

Les obligations du RGPD supposent qu'une entreprise doit à tout moment savoir de quelles données elle dispose et connaître leur localisation. De plus, la société doit également connaître l'objectif de la collecte de ces données, leur mode de gestion, de stockage, de sécurisation, de transfert et d'effacement.

Au-delà du traitement administratif, ces différentes obligations imposent à l'entreprise d'adopter une approche résolument proactive en intégrant la sécurité au cœur de son traitement des données, sous peine de sanctions bien plus élevées.

L'entreprise doit donc se préparer à d'éventuelles attaques, pour lesquelles la question n'est plus de savoir "si" mais "quand" elles se produiront et être vigilante à toute négligence de la part des collaborateurs envers les documents confidentiels.

Cette gestion des risques étendue liée à la protection des données devra être partagée par et avec l'ensemble des membres de l'entreprise, à savoir : depuis les dirigeants en passant par les différents métiers et bien entendu jusqu'aux responsables de la sécurité des systèmes d'informations.

Le RGPD confère au responsable de la protection des données un rôle beaucoup plus important en raison de l'impact des amendes et sanctions potentielles en cas d'infractions.

Afin d'éviter une sanction, se mettre en conformité avec les exigences du RGPD est indispensable.
Pour cela il faut, dans un premier temps, détecter d'éventuels dysfonctionnements et mettre en place une démarche permettant d'intégrer l'ensemble des exigences du RGPD.

Il s'avère nécessaire et indispensable de s'appuyer sur une méthodologie industrielle prenant en compte différents points à la fois techniques et organisationnels.

Pour trouver des informations complémentaires, consultez le site de la Commission Européenne :
http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

Axilis xerox Concessionnaire
Your Team Group

Maintenant, à vous de jouer : 3 étapes à suivre !

Première étape : « Suis-je en règle ? » Avant tout, réalisez un audit de conformité !

6 éléments à vérifier :

- Le type de données collectées et traitées
- Les mesures actuelles mises en place et leur niveau de maturité
- La réalisation de tests d'intrusion et d'audits de configuration : sur les bases et systèmes traitant des données personnelles
- L'identification des scénarios de risques majeurs et leurs possibilités de couverture
- Les nouveaux aspects, à savoir : le consentement explicite, le droit à l'oubli, le droit à la portabilité des données et le droit d'objection
- ... Et bien entendu le rapport de mise en conformité avec les exigences du RGP

Organisez régulièrement des audits de conformité afin de vérifier que vous êtes en règle.

Deuxième étape : « Quelles sont les bonnes pratiques pour sécuriser les données confidentielles ? »

4 actions inévitables à mener afin de protéger au mieux les documents sensibles au sein des organisations :

- Sensibilisez les collaborateurs à la problématique des informations personnelles.
- Organisez l'entreprise afin de garantir la sécurité des données qui revêtent un caractère secret : envisagez de désigner un responsable de la protection des données.
- Equipez-vous de destructeurs de documents coupe croisée afin de détruire de manière sécurisée les données dont vous n'avez plus besoin.
- Enfin, mettez à jour les systèmes et documents et préparez une nouvelle documentation détaillée et des registres en vue des inspections réglementaires.

Troisième étape : « Je sécurise quotidiennement les données en ma possession »

PROTECTION DES DONNEES :

- Réduire l'exposition du réseau et prévenir les risques de fuites de données grâce à une infrastructure informatique sécurisée

SAUVEGARDE DES DOCUMENTS :

- Sécuriser le stockage pour garantir l'intégrité et la confidentialité des données.

ASSURER LA REPRISE D'ACTIVITE

- Optimiser la sauvegarde afin de pouvoir restaurer rapidement les données en cas de perte ou de destruction non désirée.

CONTACTEZ NOUS

Nous vous accompagnons dans vos démarches de mise en conformité

Axilis

xerox Concessionnaire

Your Team Group

24 Rue de la Gare, 69009 Lyon
Tel : 04 37 64 64 00

Web : www.axilis.fr
Mail : axilis@axilis.fr