L'EMM contribue à la conformité au RGPD

Dans de nombreuses régions du monde, le bon sens en matière de sécurité est en train d'être codifié dans la loi. En Europe, le règlement général sur la protection des données (RGPD), adopté en avril 2016, entrera en vigueur le 25 mai 2018. Le RGPD constituera pour l'Union européenne un cadre juridique unique et plus complet en matière de protection et de confidentialité des données. Les pénalités et les atteintes à la réputation découlant du non-respect du RGPD sont importantes : le montant maximal de l'amende peut atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'entreprise.

Le RGPD s'applique aux responsables du traitement et aux sous-traitants situés dans l'Union européenne (UE), ainsi qu'à ceux situés en dehors de l'UE si les individus dont les données à caractère personnel sont traitées sont situés dans l'UE.

MobileIron

info@mobileiron.com
www.mobileiron.com
Tél. : +1 877 819 3451
Fax : +1 650 919 8006

« L'EMM devient essentiel pour la conformité au RGPD. »

IDC (février 2017)*

Le terme « responsable du traitement » désigne l'organisation qui décide de la finalité et des moyens du traitement des données à caractère personnel. Le terme « sous-traitant » désigne l'organisation qui gère le traitement pour le responsable, suivant ses instructions. Dans le présent document, les termes « responsable du traitement » et « sous-traitant » désignent la même entité : l'entreprise ayant des employés ou des clients dans l'UE.

Un programme de gestion de la mobilité en entreprise (Enterprise Mobility Management, EMM) complet et structuré est un élément important de l'initiative de conformité au RGPD d'une entreprise. Ce document fournit aux entreprises un cadre leur permettant d'évaluer en amont leurs règles et leurs modèles d'application de la sécurité et la confidentialité mobiles. Il ne fournit pas de conseil juridique. Chaque entreprise doit s'assurer de la conformité du déploiement de l'EMM avec son cadre juridique et sa structure de conformité internes.

Les principes qui régissent le traitement des données à caractère personnel dans le cadre du RGPD reposent sur des normes et sont conformes aux cadres de protection qui émergent dans d'autres régions.

Principes du RGPD

Chaque employeur détient des données à caractère personnel. Le principe de bon sens de la conformité au RGPD est de détenir le minimum de données à caractère personnel nécessaires et de prendre toutes précautions raisonnables limitant les risques pour les personnes concernées.

Bien que, au niveau mondial, l'Europe soit à l'avant-garde dans le domaine de la protection des données, les principes qui régissent le traitement des données à caractère personnel dans le cadre du RGPD reposent sur des normes et sont conformes aux principes de confidentialité qui émergent dans d'autres régions. Ces principes sont :

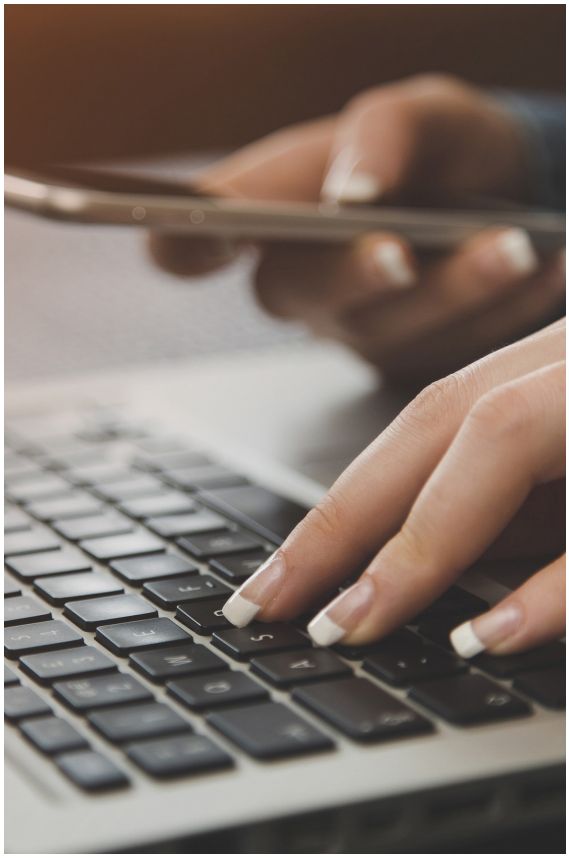
- **Licéité, loyauté, transparence :** les entreprises doivent avoir des motifs valables de traiter des données à caractère personnel et doivent en informer les personnes concernées.
- **Limitation des finalités :** il doit exister une finalité claire et explicite du traitement des données à caractère personnel. Les données ne doivent être traitées qu'aux fins pour lesquelles elles ont été collectées.
- **Consentement :** les personnes dont les données font l'objet d'un traitement doivent généralement donner leur consentement.
- **Minimisation des données :** les données traitées doivent être limitées à ce qui est nécessaire au regard de la finalité spécifique. L'accès doit être accordé uniquement aux personnes qui en ont besoin au regard de cette finalité spécifique.
- **Exactitude :** les données doivent être exactes et les inexactitudes doivent pouvoir être facilement corrigées. Les personnes concernées doivent avoir le droit de demander de telles corrections.

* « Market Analysis Perspective: Western Europe Enterprise Mobility, 2017 », IDC Europe, février 2017.

- **Limitation de la conservation :** les données doivent être conservées uniquement pendant la durée requise au regard de la finalité spécifique.
- **Intégrité et confidentialité :** les données doivent être traitées d'une manière qui garantit la sécurité appropriée des données à caractère personnel, notamment la protection contre le traitement non autorisé et la perte accidentelle.
- **Responsabilité :** l'entreprise doit être en mesure de prouver le respect des principes de conformité et de correction susmentionnés.

Une entreprise doit être en mesure de démontrer que des mesures de sécurité appropriées sont mises en place et que la conformité est surveillée de façon appropriée.

La protection des données ne peut pas être pensée après coup.



Protection des données dès la conception et par défaut – Article 25 du RGPD

La protection des données ne peut pas être pensée après coup. L'article 25 du RGPD définit le concept de « protection des données dès la conception et [de] protection des données par défaut », également désigné sous le terme de « protection dès la conception et par défaut ».

Protection des données dès la conception : l'entreprise doit assurer la confidentialité des données tout au long du cycle du processus, dès le premier stade et la conception des systèmes jusqu'au dernier stade et à la suppression des données.

Protection des données par défaut : l'entreprise doit garantir que, par défaut, seules les données à caractère personnel nécessaires sont collectées et traitées. L'utilisateur ne doit pas avoir à refuser de donner des informations complémentaires. L'entreprise ne peut pas collecter des informations complémentaires dans la simple éventualité de les utiliser ultérieurement.

État des connaissances – Article 32 du RGPD

L'article 32 du RGPD souligne l'importance de l'utilisation de techniques récentes et de premier plan pour prendre en charge la gouvernance des informations :

*« Compte tenu de l'**état des connaissances**..., le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. »*

Bien que le RGPD ne prescrive pas de techniques spécifiques, l'article 32 cite quelques exemples de mesures telles que le chiffrement, l'intégrité, la disponibilité et les tests pour lesquelles les entreprises doivent évaluer les solutions de pointe.

Création d'un cadre EMM pour le RGPD

Les solutions d'EMM, comme MobileIron, sont un élément important d'un programme de sécurité conforme au RGPD. Une entreprise qui, dans les faits, n'utilise pas de solution EMM aura du mal à expliquer aux autorités concernées pourquoi elle n'applique pas de mesures techniques à la pointe de la technologie pour atténuer le risque de perte de données.

Une entreprise qui, dans les faits, n'utilise pas de solution EMM aura du mal à expliquer aux autorités concernées pourquoi elle n'applique pas de mesures techniques à la pointe de la technologie.

Un cadre d'EMM pour le RGPD doit inclure les fonctionnalités MobileIron suivantes :

1. La plateforme MobileIron permet à l'entreprise de **mettre en place le chiffrement des données** sur l'appareil en surveillant les paramètres de ce dernier et en fournissant un deuxième chiffrement des applications et des données d'entreprise.
2. La plateforme MobileIron permet à l'entreprise de **définir une limite claire entre les données personnelles et professionnelles** sur l'appareil. L'entreprise n'a pas accès au contenu des applications personnelles ni des comptes de messagerie personnels. Chaque entreprise doit également évaluer si l'accès à d'autres types de données personnelles, comme l'inventaire des applications ou l'emplacement de l'appareil, a une finalité justifiable en termes de sécurité ou d'exploitation. Le cas échéant, la finalité doit être clairement exposée et communiquée, et les mesures appropriées de protection des données par défaut et de consentement doivent être établies en amont.
3. La plateforme MobileIron permet à l'entreprise de **mettre en place un accès sécurisé aux services professionnels.** MobileIron Access fournit à l'entreprise une visibilité sur les appareils mobiles et les applications qui tentent de se connecter aux services back-end. Les accès non autorisés peuvent ainsi être bloqués. MobileIron Sentry protège le trafic de données et peut également l'acheminer par le jeu de passerelles de sécurité et d'inspection supplémentaires au besoin.
4. La plateforme MobileIron permet à l'entreprise d'**utiliser des journaux d'audit** pour déterminer les actions à l'origine d'un vol de données et, le cas échéant, les actions prises à la suite. Dans certains cas, la période de notification obligatoire du RGPD est de 72 heures seulement et impose une réponse rapide.
5. La plateforme MobileIron permet à l'entreprise d'**appliquer des contrôles de prévention contre la perte des données (DLP).** Ces contrôles offrent la possibilité de supprimer à distance les données confidentielles sur un appareil perdu et de s'assurer que les applications professionnelles installées sur un appareil ne partagent aucune donnée avec des applications non autorisées. Ils identifient également les attaques de l'intégrité du système d'exploitation mobile qui tentent de déverrouiller l'appareil (via jailbreak ou root). En cas de problème de conformité, l'entreprise peut utiliser la plateforme MobileIron pour prendre l'action corrective appropriée, comme la notification, la mise en quarantaine ou la suppression de données.

Les appareils mobiles non gérés ne prennent en charge aucune stratégie de défense en profondeur.

Déployer l'EMM pour le RGPD

Toutes les entreprises concernées par le RGPD doivent évaluer leur déploiement EMM et leur modèle de configuration. Cette évaluation permet, en premier lieu, d'identifier les cas où l'EMM n'est pas suffisamment exploitée pour assurer correctement la conformité au RGPD. Elle permet ensuite de poser les bases de la conception et de la mise en œuvre d'un programme de contrôle continu de la conformité et de correction.

Voici quelques principes de base pour déployer l'EMM dans le cadre d'un programme de sécurité conforme au RGPD :

1. Mettez en place une gestion de tous les appareils mobiles ayant accès aux données professionnelles. Les appareils mobiles non gérés ne prennent en charge aucune stratégie de défense en profondeur permettant d'assurer un niveau de sécurité raisonnable des données en cas de perte ou de piratage.
2. Appliquez des profils de configuration à jour. Instaurez des règles pour les mots de passe, le chiffrement, la sécurité des appareils, la connectivité et toutes les autres fonctions pertinentes nécessaires à l'activité.
3. Distribuez toutes les applications professionnelles sous la forme d'applications gérées via un magasin d'applications d'entreprise pour qu'elles s'exécutent dans une infrastructure sécurisée contrôlée par l'entreprise.
4. Instaurez des stratégies appropriées de prévention contre la perte des données (DLP) pour protéger les données d'application sur l'appareil.
5. Mettez en place un accès sécurisé aux services professionnels. Bloquez l'accès des appareils, des applications et des utilisateurs non autorisés, non gérés ou non conformes. Interdisez le stockage des données confidentielles sur un appareil hors de la visibilité et du contrôle de l'entreprise.
6. Définissez des règles de confidentialité et de sécurité, et communiquez-les clairement et régulièrement aux employés.
7. Collectez les journaux d'inventaire, d'utilisation et d'audit appropriés pour alimenter un processus de réponse rapide aux infractions.

Conclusion

Une entreprise n'est pas en mesure d'assurer une sécurité suffisante des données personnelles, sauf à prouver qu'elle a mis en œuvre les contrôles et les procédures EMM appropriés. Ces garanties assurent la protection des données personnelles utiles à l'entreprise contre les menaces externes et l'utilisation ou la divulgation non autorisée. La plateforme MobileIron fournit un cadre solide pour la conformité aux principes du RGPD : minimisation des données, intégrité et confidentialité, et responsabilité.