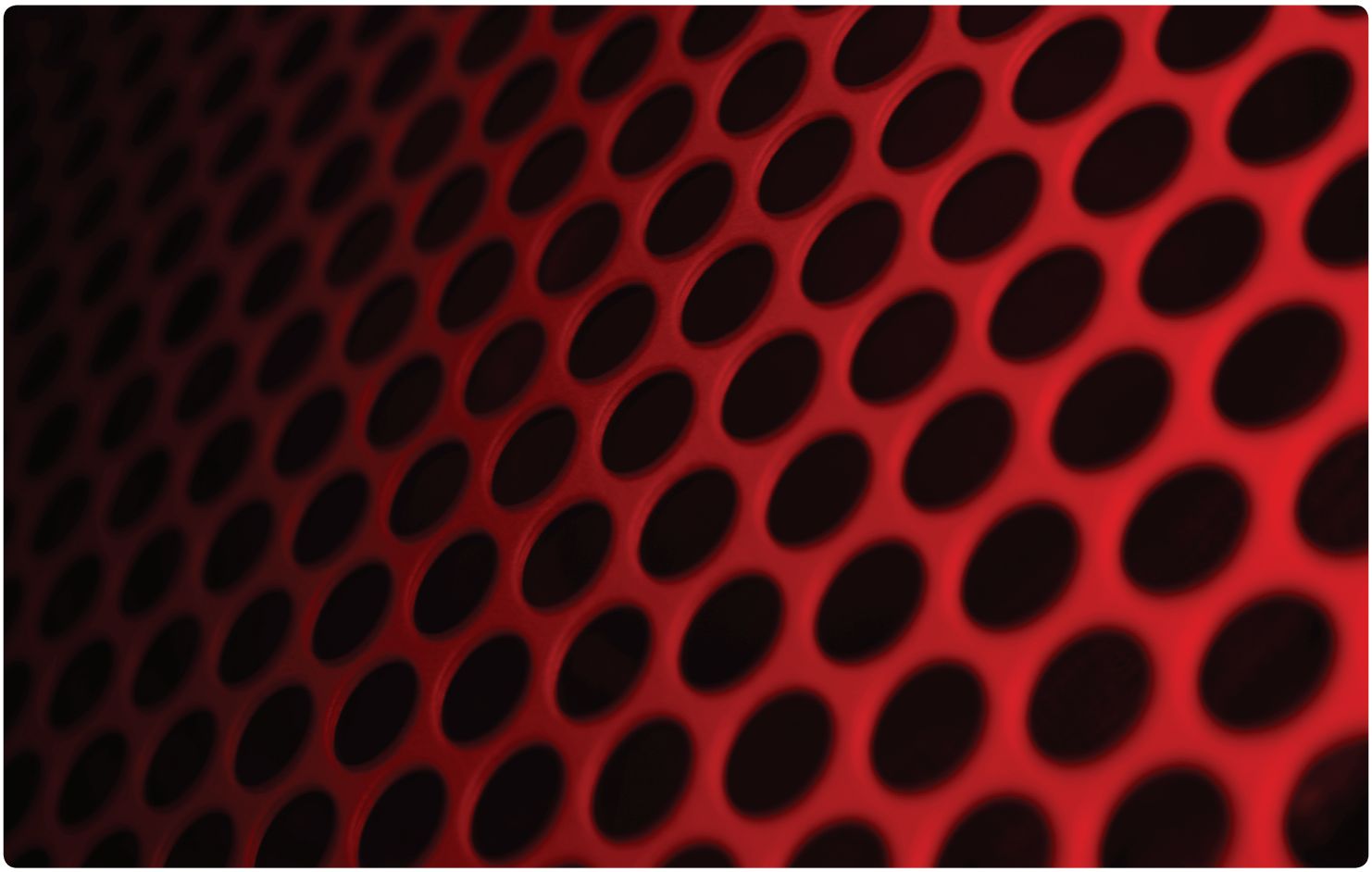
Risques de violation des données

Comment les prévenir conformément au RGPD UE



Kingston TECHNOLOGY

Introduction

La vie professionnelle au quotidien a radicalement changé, tout comme les méthodes de travail traditionnelles : Grâce aux supports de stockage mobiles, nous pouvons accéder et utiliser nos données pratiquement à tout moment et n'importe où. En plus des avantages de cette **disponibilité permanente** des informations professionnelles, nous pouvons créer des **versions opérationnelles mobiles** ou des copies de sauvegarde, pour optimiser nos heures de travail et en finalité accélérer efficacement nos opérations.

Mais la mobilité a aussi des inconvénients. Les clés USB perdues ou volées présentent un risque sérieux. **72%** des entreprises interrogées pendant l'enquête* ont signalé qu'elles ne pouvaient plus retrouver certaines de leurs clés USB personnelles. Ceci est d'autant plus grave car 25% des entreprises interrogées les utilisent pour stocker des **données sensibles**. De telles violations des données détériorent la **confiance des clients** envers l'entreprise concernée, qui subit donc une perte de réputation, en plus des coûts. Ces chiffres n'incluent pas les risques liés à la publication ou à l'utilisation criminelle des données.

Par conséquent, le législateur a pris des mesures pour contrer les risques croissants de violations des données. Le **règlement général de l'Union européenne sur la protection des données** (RGPD UE) oblige les entreprises à assumer et étendre davantage leurs responsabilités à partir de mai 2018. Entre autres changements, de lourdes sanctions pourront être imposées si certaines obligations ne sont pas respectées.

Ce livre blanc vous explique :

- Ce qu'il faut savoir sur la mobilité des données et les violations des données
- Les exigences du RGPD et ce que les entreprises doivent faire pour appliquer ce nouveau règlement
- Comment faire pour éviter les violations des données

SOMMAIRE

* Enquête réalisée par Kingston Technology en Allemagne, 2016 (nombre de réponses : 200)

Le RGPD UE est basé sur la prévention

Le Règlement général européen sur la protection des données (RGPD UE) remplace les anciennes réglementations nationales sur la protection des données et sera applicable à partir du 25 mai 2018 après une période de transition de deux ans. L'objectif principal du RGPD UE est d'améliorer **la protection des données et les droits fondamentaux des citoyens UE.**

Le RGPD UE concerne non seulement les entreprises européennes, mais aussi toutes les organisations qui fournissent des produits et des services (incluant les offres gratuites) aux citoyens UE et qui enregistrent leurs données personnelles pour ce faire. Le RGPD UE ne fait pas de distinction entre les grandes entreprises, les PME, ou les start-up. C'est pourquoi la protection des données doit être prise en compte dans toutes les organisations qui collectent, traitent et conservent des données personnelles.

L'objectif de la protection des données personnelles est encadré par de lourdes sanctions : les violations de la protection des données, contre lesquelles aucune mesure appropriée n'a été mise en place, peuvent faire l'objet de poursuites et de sanctions allant jusqu'à **4% du chiffre d'affaires annuel de l'entreprise ou d'une amende allant jusqu'à 20 millions d'euros**.

En outre, toutes les violations de la protection des données doivent être communiquées aux autorités de régulation responsables et aux personnes concernées. Outre les sanctions financières, les conséquences peuvent être extrêmement lourdes pour une entreprise en termes de réputation, de confiance auprès des clients et de ventes.

Ces mesures visent à éviter autant que possible les violations de données. Elles cherchent à minimiser la divulgation de données personnelles et à encourager les entreprises à mettre en œuvre des procédures préventives. Cependant, l'UE est consciente qu'une protection absolue de toutes les données n'est pas un objectif réaliste. Néanmoins, la nouvelle directive vise à atteindre la **meilleure prévention possible.**

L'analyse prédictive des risques est un avantage

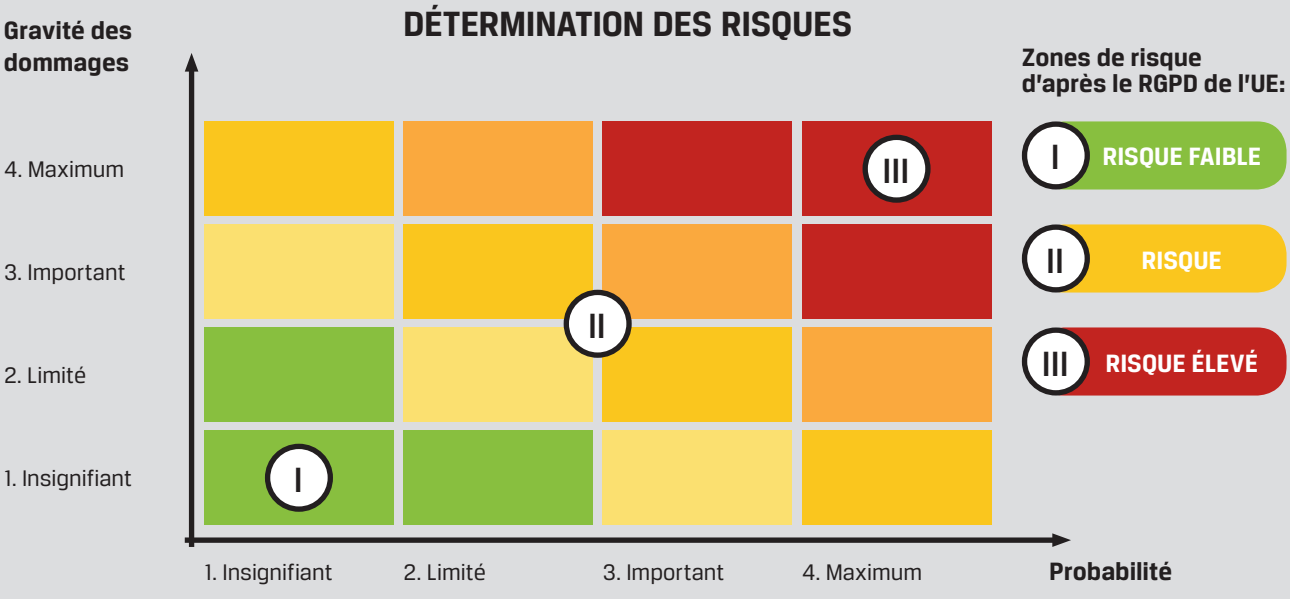
Pour prévenir les violations de la protection des données, vous devez savoir où elles peuvent survenir. Les risques potentiels doivent donc être identifiés et analysés. Tous les domaines d'une entreprise qui utilisent des données doivent être examinés en détail. Où sont collectées les données personnelles ? Comment sont-elles traitées et conservées ?

Cette analyse des risques est exigée par le RGPD UE. La probabilité et la gravité des dommages possibles doivent être examinées. Le **Responsable de la protection des données** peut utiliser ces informations pour prendre des mesures appropriées spécifiques.

Une **matrice des risques** peut faciliter l'identification des risques potentiels associés au stockage des données. Cela permet de reconnaître les points qui nécessitent une action spécifique. Chaque risque peut être localisé et identifié avec précision en fonction de sa probabilité et de la gravité des dommages. Les trois catégories de risques Faibles – Moyens – Élevés indiquent la nécessité des mesures à prendre et de la sécurité requise.

L'Article 32 Paragraphe 1 du RGPD UE stipule :

"Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques,le responsable du traitement et le sous-traitant mettent en oeuvre les mesures techniques et organisationnelles appropériées afin de garantir un niveau de sécurité adapté au risque[.]"



Une **évaluation exhaustive** de tous les points de stockage contenant des données personnelles facilite les analyses, indiquant avec précision les points nécessitant des mesures correctives urgentes. Les **raisons** de l'évaluation des risques sont disponibles dans les colonnes : sources de risques, probabilité et étendue des dommages. Ainsi, les risques peuvent être efficacement supprimés pour bénéficier d'une préparation optimale à la date de mise en application du 24 mai 2018.

Le RGPD UE propose ces mesures de sécurité

L'objectif principal du RGPD UE concernant le traitement des données personnelles est de « garantir un niveau de sécurité adapté au risque » (Article 32 Paragraphe 1). En fonction des résultats de l'analyse des risques, des mesures de protection doivent être mises en œuvre et adaptées à la situation d'une part, et doivent garantir la sécurité d'autre part.

Heureusement, le GRPD UE fournit des informations spécifiques sur la portée des mesures de sécurité applicables aux données critiques. L'Article 32 Paragraphe 1 stipule aussi : « [Ces mesures incluent [...] : [...] la **pseudonymisation** et le **cryptage** des données à caractère personnel ». Ces deux procédures peuvent par conséquent être appliquées pour obtenir une sécurité conforme au RGPD UE.

Pour pseudonymiser des données personnelles, les noms sont remplacés **par des codes numériques aléatoires** et la clé est stockée dans une **table principale**. Ce processus à l'avantage essentiel d'offrir une automatisation complète. La table principale doit néanmoins être constamment disponible. Elle ne doit jamais être perdue ni modifiée. Il est également indispensable que d'autres éléments que le nom permettent d'identifier une personne. Par exemple, une identité peut aussi être définie par le sexe, la date de naissance et le lieu de résidence. Par conséquent, un **risque résiduel** demeure. Le cryptage est une autre mesure recommandée par le RGPD UE. Quelle que soit leur condition, toutes les données doivent être cryptées en tout point de chaque transmission.

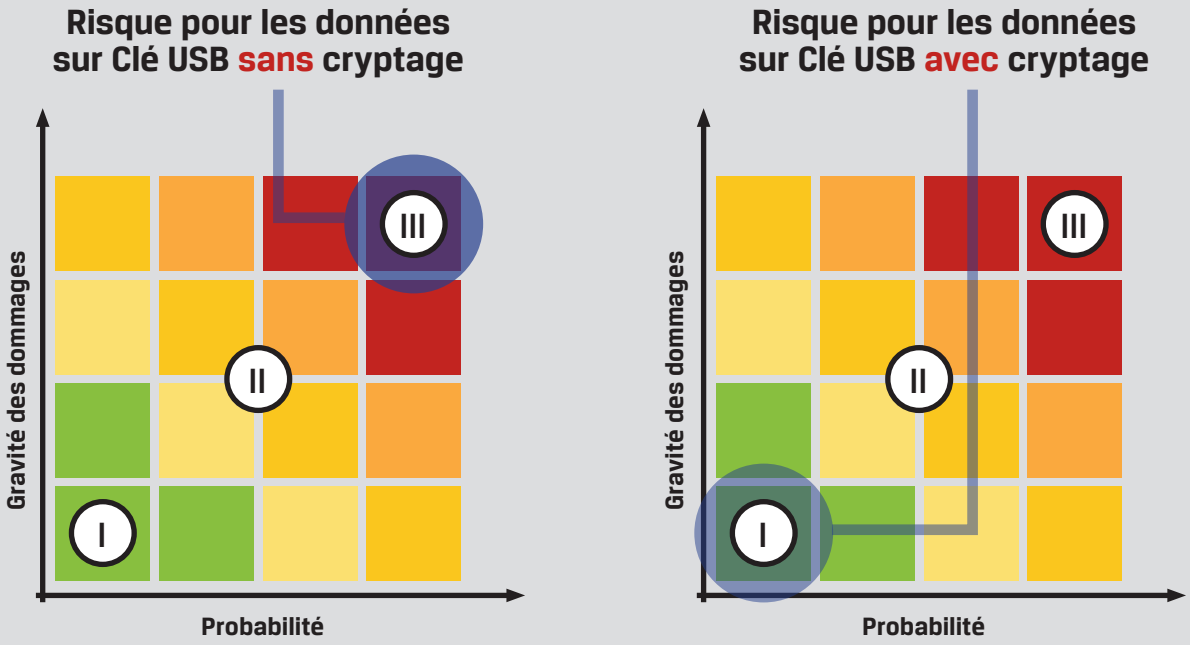
Les **certifications de fabricant volontaires telles que FIPS 197 ou 140 – Niveau 3** sont la référence d'un cryptage de haute qualité. Elles garantissent un certain standard de sécurité et joueront à l'avenir un rôle encore plus important en tant que preuve dans le contexte de l'application du RGPD UE.

Lorsque des données personnelles sont correctement cryptées – la norme de cryptage AES 256 bits est actuellement à la pointe de la technologie – elles ne peuvent pas être utilisées même après un vol ou une violation de données. L'obligation d'informer la ou les personnes concernées, de faire une annonce publique, n'est plus applicable puisque le risque n'existe plus.

L'autorité de régulation responsable doit néanmoins être notifiée.

Clés USB cryptées à tout moment, partout : Kingston Technology

Selon le sondage mentionné ci-dessus, les entreprises qui enregistrent des données personnelles sur des clés USB non-cryptées se placent à haut risque, car elles sont souvent perdues, volées ou ne peuvent pas être localisées. Ces risques doivent donc être classés comme élevés, puisque la probabilité et la gravité potentielle des dommages peuvent être considérées comme élevées. Ces deux facteurs peuvent être considérablement réduits en utilisant des clés USB cryptées, ce qui permet aussi de reclasser le risque général comme « Insignifiant ».



Avec ses gammes DataTraveler DTVP3.0 et DT4000G2, IronKey D300 et S1000, Kingston Technology offre un choix de clés USB qui répond aux plus hautes normes de sécurité mentionnées ci-dessus. Les données stockées sont cryptées à 100% et une protection par mot de passe complexe avec des caractéristiques minimales bloque les accès non-autorisés. Par exemple, après dix tentatives d'accès infructueuses, l'accès aux données est bloqué.

Les clés USB de Kingston sont cryptées conformément à la norme de sécurité **AES-256** en mode XTS. Cet algorithme correspond aux normes de sécurité actuelles. Les certifications conformes **FIPS 197** et **FIPS 140-2** garantissent que vos données sont absolument sécurisées, même en cas de vol ou de perte. Les versions DataTraveler 4000G2, IronKey D300 et IronKey S1000 offrent aussi

une protection physique conforme FIPS 140-2. Avec certaines de ses clés USB (DTVP3.0, DTVP3.0AV, DT4000G2 avec Management et D300), Kingston offre aussi un **programme de personnalisation** qui permet de les intégrer dans une solution de gestion de terminaux, afin d'utiliser des numéros de série, des identifiants de produits par exemple, ou de définir le nombre de tentatives de saisie du mot de passe avant blocage.

Kingston Technology s'est allié à **DataLocker** pour offrir également des solutions de gestion intégrées à ses clés USB cryptées. DataLocker fournit le logiciel SafeConsole et l'Enterprise Management System (EMS) pour les clés USB cryptées DataTraveler et IronKey de Kingston, qui vous permettent de gérer de manière centralisée les clés USB utilisées dans votre entreprise.

DataTraveler Vault Privacy 3.0 et DataTraveler 4000 G2 de Kingston sont disponibles en versions Managed (Management en option). Les deux supportent la gestion centralisée avec SafeConsole de DataLocker. IronKeys D300 et S1000 sont aussi disponibles en version Managed. Les deux permettent d'utiliser IronKey EMS de DataLocker.

Ces solutions permettent de répondre plus facilement aux **exigences de conformité**. Un **support supplémentaire** peut être fourni aux employés. Par exemple, avec des fonctions de réinitialisation de mot de passe à distance ou de scanner anti-logiciel malveillant automatisé. Elles simplifient aussi la conformité à des directives de sécurité exhaustives parce qu'elles permettent à l'administrateur du système de contrôler facilement toutes les clés de l'entreprise.

Par conséquent, la perte d'une clé USB cryptée de Kingston n'implique pas automatiquement une violation des données. Les supports de stockage mobiles cryptés éliminent donc un risque de sécurité bien connu des entreprises, mais qu'elles sous-estiment ou ignorent trop souvent. Eliminez les petites mais dangereuses failles de sécurité grâce aux clés USB cryptées, **évitant ainsi les violations de la protection des données conformément au RGPD de l'UE.**

AVEZ-VOUS DES QUESTIONS ?

N'hésitez pas à nous contacter :

+44 (0) 1932 738888

EncryptedUSB@kingston.eu

www.kingston.com

Ce livre blanc a été créé par le B2B Media Group GmbH
au nom de Kingston Technology Europe Co LLP
et Kingston Digital Europe Co LLP.
http://www.b2bmg.de / kontakt@b2bmg.de