Kensington The Professionals' Choice™

Pourquoi la sécurité physique est-elle indispensable à la **conformité avec le RGPD ?**

Avertissement : *Aucune des informations citées dans ce présent livre blanc ne doit être interprétée comme un conseil juridique. Les organisations doivent consulter un conseiller juridique en ce qui concerne le respect du Règlement général sur la protection des données ou toutes autres lois ou réglementations en vigueur.*

DONNÉES PROTÉGÉES

Sommaire

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

À propos de **ce document**

Ce livre blanc vous donnera un aperçu des objectifs du RGPD et des problèmes qu'il peut présenter pour les organisations.

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Ce livre blanc a pour objectif de vous donner un aperçu du Règlement Général sur la Protection des Données de l'UE (le « RGPD ») et de vous en expliquer les impacts sur diverses entreprises. Vous pourrez ainsi élaborer une politique de sécurité du matériel informatique avant l'entrée en vigueur du RGPD en mai 2018.

En quoi consiste le RGPD ? Le RGPD exige que les organisations mettent en œuvre des pratiques efficaces de protection des données numériques et imprimées sur papier, et qu'en cas de violation de données, elles avisent les personnes affectées ou susceptibles de l'être. Il s'applique à l'international à toutes les organisations, indépendamment de leur couverture géographique, qui contrôlent ou traitent des données à caractère personnel relatives à des personnes résidant dans l'Union européenne. En outre, les dispositions du RGPD s'appliquent aux données personnelles numériques et aux données imprimées sur papier. Par conséquent, toutes les organisations qui traitent des données à caractère personnel en provenance de l'UE doivent respecter ces dispositions.

Alors que de nombreuses organisations placent, à juste titre, la protection des données contre le piratage et les logiciels malveillants au premier rang de leurs préoccupations, beaucoup d'entre elles ne se soucient pas suffisamment de la sécurité physique de leurs matériels informatiques. Plus de la moitié d'entre elles n'utilisent pas de câble de sécurité pour protéger leurs appareils informatiques.[1] Elles risquent ainsi d'enfreindre le RGPD, expose les données au risque de fraude voire à l'usurpation d'identité. Sachant cela, Kensington encourage les organisations à revoir leurs politiques et pratiques en matière de protection des données numériques.

Un **aperçu**

Bien que le RGPD ait pour objectif principal le renforcement des droits à la vie privée sur Internet, la sécurité physique du matériel a un rôle important à jouer.

Il vise essentiellement à relever les défis grandissants concernant la protection des données et de la vie privée, comme l'exposition aux violations de données, le piratage et d'autres infractions.

*Les points ci-contre décrivent les **différents aspects du RGPD** qui sont nouveaux ou sont des droits renforcés pour les individus.*

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

1

Portabilité des données et droit à l'oubli

- Chaque individu a maintenant le droit de transmettre ses données personnelles d'une organisation à une autre.
- Les données personnelles doivent être fournies dans un format structuré et lisible par une machine.
- Une personne peut exiger l'effacement ou la suppression de ses données personnelles.

2

Inventaire

- Les autorités locales n'ont plus à être informées du traitement des données personnelles.
- Mais les organisations doivent tenir un inventaire des activités de traitement des données dont elles sont responsables.

3

Sécurité et évaluation d'impact sur la protection des données

- Ces évaluations d'impact constituent un moyen d'identifier les risques importants d'atteinte à la vie privée.
- Les exigences et recommandations en matière de sécurité doivent être basées sur une évaluation des risques.

4

Notification des violations de données

- Toute violation de données doit être notifiée à l'autorité de contrôle.
- Les personnes concernées par la violation de données doivent également en être informées.

5

Gestion des données et responsabilité

- Les organisations doivent aussi être en mesure de démontrer leur conformité au RGPD.

À qui **le RGPD s'applique-t-il ?**

Toute organisation qui détient des données sur les citoyens européens (qu'elle soit basée au sein de l'UE ou non) doit respecter le RGPD. Il concerne toute personne traitant de telles données.

Le RGPD s'applique aux organisations situées au sein et en dehors de l'Union européenne, qui traitent ou contrôlent des données se rapportant à des résidents ou ressortissants actuels de l'Union européenne.

Il concerne principalement :

les responsables du traitement – ils déterminent comment et pourquoi les données personnelles sont traitées ;

les sous-traitants – ils agissent sous le contrôle du responsable du traitement.

Il appartient à ces personnes de faire en sorte que leurs clients respectent pleinement tous les aspects du RGPD, afin que ces derniers ne se voient pas imposer d'amendes.

Tous les membres d'une organisation qui ont des informations personnelles sensibles doivent s'assurer de l'application efficace et démontrable du RGPD. Par exemple, l'ordinateur portable d'un commercial renferme des informations confidentielles sur ses clients et doit être physiquement sécurisé lorsqu'il travaille en dehors de l'entreprise.

Un sous-traitant ou un responsable du traitement devra peut-être **nommer un délégué à la protection des données** et tenir un inventaire de toutes les activités de traitement effectuées pour le compte des clients.

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Le RGPD s'applique aux **données personnelles** et **aux données personnelles sensibles** en formats numérique et physique.

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Avant d'élaborer une politique de conformité pour votre organisation, il est important de savoir à quels types de données le RGPD s'appliquera.

Les données personnelles auxquelles s'applique le RGPD comprennent toutes les informations à caractère personnel et relèvent de deux catégories :

Données personnelles – Elles comprennent les données comme une adresse e-mail ou une adresse postale, ainsi que les informations pouvant servir d'identifiant en ligne, comme une adresse IP.

Données personnelles sensibles – Elles concernent les informations à caractère plus intime comme l'origine ethnique, les opinions politiques, la religion et les données sur la santé. En général, les organisations doivent justifier le traitement de ces informations par des motifs plus importants que s'il s'agissait de données personnelles « normales ».

Le RGPD s'applique au traitement par les organisations de données personnelles en **formats numérique et physique.**

Un cadre pour **se conformer au RGPD**

En évaluant leur personnel, leurs processus et leur technologie, les organisations seront en mesure d'élaborer une politique bien définie de protection des données, qui les aidera à respecter toutes les sections du RGPD.

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Pour garantir le respect du RGPD, les organisations doivent évaluer trois aspects principaux :

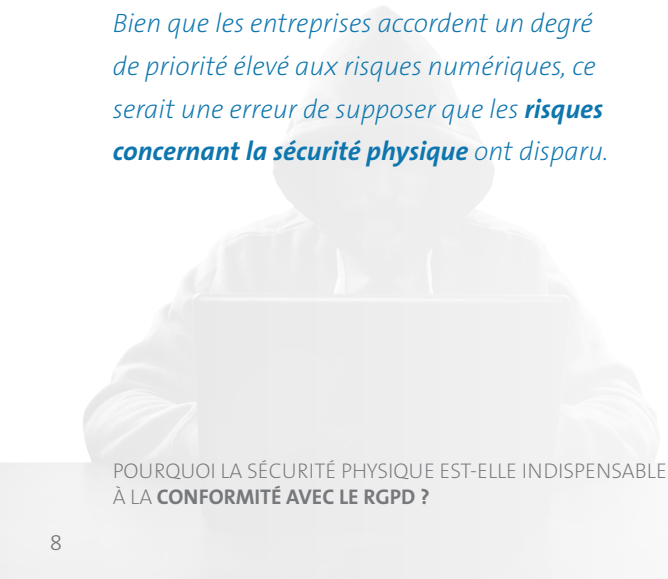
Les personnes – Il est indispensable que le personnel assume la responsabilité des données qu'il traite au sein de son organisation. Une organisation doit élaborer des règles bien définies destinées à chacun de ses employés en vue de garantir la bonne gestion de toutes les données numériques qu'elle détient. Ces règles doivent être conformes aux dispositions du RGPD dans le cadre du traitement de toutes les données. Par exemple, peut-être souhaiterez-vous adopter des règles bien définies sur l'utilisation des données sensibles détenues sur les ordinateurs portables du personnel, et sur le processus d'effacement des données.

Les procédures – Il s'agit des procédures mises en place au sein de l'organisation, comme la gestion de l'utilisation des données et notamment le traitement et la conservation des données sur les clients. Il est essentiel que les entreprises évaluent tous leurs processus actuels se rapportant aux données. Une fois les lacunes et faiblesses des procédures existantes identifiées, l'entreprise doit élaborer un plan-cadre permettant de les éliminer ou de les remplacer, le cas échéant, en vue d'assurer le respect du RGPD.

La technologie – Les capacités et exigences informatiques actuelles doivent également être évaluées et modifiées en conséquence avant mai 2018. Il appartient à chaque entreprise de prendre les mesures nécessaires pour améliorer ou remplacer tous les systèmes existants qui ne sont pas entièrement conformes au RGPD afin de ne pas se voir imposer d'amendes après l'entrée en vigueur de celui-ci.

Pourquoi la **sécurité physique** est-elle importante ?

*Bien que les entreprises accordent un degré de priorité élevé aux risques numériques, ce serait une erreur de supposer que les **risques concernant la sécurité physique** ont disparu.*



POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Ayant examiné les exigences du RGPD à l'égard des entreprises, il est maintenant important de se pencher sur la question de la sécurisation du matériel physique au sein d'une organisation et d'expliquer pourquoi elle revêt une grande importance quand les entreprises se préparent à se conformer aux dispositions du RGPD.

Après les menaces en ligne et la divulgation involontaire de données, les **appareils mobiles** et la **perte physique** constituent la plus importante source de violations de données[2] :

Tous les jours, en moyenne, plus de **5 millions d'enregistrements de données sont perdus ou volés**[3], et plus **d'un tiers des entreprises n'ont aucune politique de sécurité physique en place** pour protéger les ordinateurs portables, les appareils mobiles et les autres biens électroniques.[4]

Compte tenu du montant des amendes potentielles prévu par le RGPD, de la plus grande mobilité du personnel et de la popularité croissante du partage de bureau, la sécurisation des ordinateurs portables et des appareils mobiles est une précaution élémentaire, au bureau et en dehors. Le verrouillage d'un appareil représente un moyen de protection contre le vol à la fois simple, rapide et très efficace.

Kensington offre une gamme de **solutions de sécurité** pour un vaste éventail d'ordinateurs portables, y compris les appareils sans encoche de sécurité. Les sacoches de la gamme SecureTrek™ peuvent être solidement attachées à un point fixe dans des lieux publics tels que les aéroports, les hôtels et les salons professionnels.

La **sécurité physique** encore impliquée dans de nombreuses violations de sécurité

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Sur les 697 incidents de violation de données enregistrés entre avril et juin 2017 par l'autorité de contrôle en matière de protection des données au Royaume-Uni (Information Commissioner's Office ou ICO), 6 % étaient dus au vol d'un appareil non crypté. De plus, le stockage des données dans un endroit non sécurisé et le vol de l'unique copie de données chiffrées représentaient 3,5 % des infractions.[5]

Dans le **secteur financier, 25 %** des violations sont causées par le vol ou la perte d'appareils, raison la plus fréquente des fuites de données. Ces appareils constituent des cibles particulièrement attrayantes en raison du volume de données sensibles qui y sont conservées et traitées.[6]

Dans le **secteur de la santé**, le vol ou la perte d'appareils représente la cause la plus importante des incidents de sécurité, soit **32 %** des plus de 100 000 incidents enregistrés dans 82 pays.[7]

Les capacités et exigences informatiques actuelles doivent également être évaluées et modifiées en conséquence avant mai 2018. Il appartient à chaque entreprise de prendre les mesures nécessaires pour améliorer ou remplacer tous les systèmes existants qui ne sont pas entièrement conformes au RGPD afin de ne pas se voir imposer d'amendes après son entrée en vigueur.

Le respect du RGPD exige une véritable implication des utilisateurs

Comme la sécurité physique reste indispensable à la protection de l'information, comment les entreprises peuvent-elles la renforcer ?

Kensington est le leader mondial de la sécurité physique du matériel informatique et a inventé le câble de sécurité pour ordinateur portable. Au cours des 35 dernières années, Kensington a recueilli de précieuses informations sur les besoins, les attentes et les challenges des organisations cherchant à se protéger et souhaitant aujourd'hui respecter le RGPD.

Ces enseignements nous ont confirmé qu'il existe quatre freins et obstacles principaux à une sécurité physique efficace dans les organisations :

1. *« Nous travaillons dans un environnement sûr »*
2. *« Nous cryptons nos données et les stockons sur le cloud »*
3. *« Les câbles de sécurité ont uniquement un effet dissuasif »*
4. *« Il est impossible de verrouiller cet appareil »*

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Surmonter les obstacles à la conformité au RGPD

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

« Nous travaillons dans un environnement sûr »

Les caméras de surveillance, les badges des employés et le personnel de sécurité peuvent parfois donner un faux sentiment de sécurité et réduire la perception des risques. 58 % des ordinateurs portables sont volés au bureau et 85 % des responsables informatiques suspectent qu'il s'agit de vols internes.[8] Les données sont menacées dès la saisie de l'appareil, d'autant que seuls 3 % des ordinateurs[9] sont retrouvés. Les câbles de sécurité permettent d'empêcher les vols opportunistes, et ainsi d'éviter les investissements en temps et en argent pour retrouver le coupable, remplacer l'ordinateur et payer les amendes prévues par le RGPD.

« Nous cryptons nos données et les stockons sur le cloud »

Le cryptage n'est pas une solution en cas de vol d'un appareil si celui-ci contient des données qui n'ont pas été sauvegardées ailleurs. Même si le disque dur de l'ordinateur volé ne contient aucune donnée, la perte de cet important outil de travail engendra une baisse de productivité contre laquelle il vaut mieux se protéger. Faites le tour de vos locaux. Un coursier pourrait-il facilement s'emparer d'un appareil ? 49 % des PME mettent de 2 à 4 jours à remplacer un ordinateur perdu ou volé.[8]

« Les câbles de sécurité ont uniquement un effet dissuasif »

Les câbles de sécurité sont avant tout destinés à protéger contre les vols opportunistes. Mais ils s'avèrent également efficaces contre d'autres formes de vol. IDC a constaté que, parmi les responsables informatiques victimes de vol d'ordinateur portable, 52 % d'entre eux ont déclaré que le vol aurait pu être évité s'ils avaient utilisé un câble.[8]

Surmonter les obstacles à la conformité au RGPD

« Il est impossible de verrouiller cet appareil »

En raison de l'évolution vers un design plus mince, les ordinateurs ne sont plus toujours munis de l'encoche de sécurité Kensington, la référence du secteur. Or on croit à tort que ces appareils ne peuvent pas être sécurisés physiquement. Même les appareils sans encoche de sécurité peuvent être verrouillés afin d'empêcher les vols opportunistes. Kensington propose une gamme complète de solutions adaptées à un vaste éventail d'appareils :

MicroSaver® 2.0 et ClickSafe® 2.0

Pour les appareils munis de l'encoche de sécurité Kensington, installée sur 90 % des appareils en entreprise.

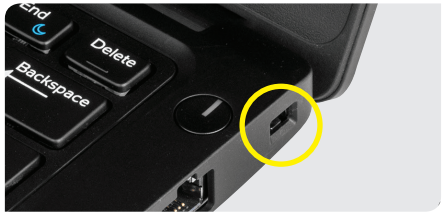
Encoche de sécurité Kensington sur les ordinateurs portables et de bureau

Le MicroSaver® 2.0 se fixe directement dans l'encoche de sécurité

ClickSafe® 2.0 avec point d'ancrage ClickSafe

N17

Pour les appareils munis de l'encoche non standard Wedge, installée sur les modèles Dell Latitude 2017 (et ultérieurs) ainsi que sur d'autres appareils.



Encoche non standard Wedge

Ancrage de l'ordinateur à un objet fixe

NanoSaver®

Pour les appareils munis de l'encoche Nano Security Slot™ de Kensington, installée sur les ordinateurs portables ultraminces.

Encoche de sécurité Nano Security Slot™ de Kensington

Câble de sécurité NanoSaver®

Solutions de sécurité pour Microsoft Surface™

Des solutions spécialement dédiées aux Surface™ Pro, Surface™ Book et Surface™ Studio.

Câble de sécurité pour Surface™ Pro

Kit de sécurité pour Surface™ Studio

Système de sécurité pour Surface™ Book de 13,5"

Station de sécurité 2.0 pour ordinateurs portables

Pour les appareils sans encoche de sécurité comme le Surface™ Laptop et MacBook Pro®.

Station de sécurité pour MacBook Pro®

Trouvez la solution de sécurité idéale pour votre ordinateur portable ou autre appareil sur :
www.kensington.com/lockselector.com

RGPD : les 6 points clés à considérer

1. Nommer un délégué à la protection des données

Ce délégué doit être en mesure de répondre à toutes les responsabilités de l'organisation liées au RGPD, et doit parfaitement comprendre quelles données de l'organisation sont considérées comme « personnelles », où elles sont conservées, qui y a accès, comment détecter les violations éventuelles et à qui les signaler. **Le délégué à la protection des données n'est pas nécessairement un employé ; il est possible de sous-traiter ce rôle.**

2. Évaluer vos systèmes

Examinez l'ensemble des contrats, services d'assistance technique, procédures et outils se rapportant au traitement, à la gestion, au stockage et à l'effacement des données. Vous devez pouvoir identifier toutes les lacunes ou faiblesses exigeant des modifications.

3. Élaborer une stratégie

Construisez une nouvelle stratégie qui garantira le respect du RGPD. Celle-ci peut donner lieu à de nouveaux investissements technologiques, à une révision des procédures suivies par le personnel et à la création de nouveaux rôles au sein de l'organisation.

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

RGPD : les 6 points clés à considérer

4. Mettre en œuvre une nouvelle politique à l'échelle de l'organisation

L'étape suivante vers la conformité au RGPD consiste à mettre en œuvre votre plan à tous les niveaux hiérarchiques de l'organisation. Investissez dans les nouvelles technologies et les nouveaux systèmes requis sur le lieu de travail et publiez un guide sur la gestion et le traitement des données.

5. Impliquer les employés

Présentez votre nouvelle politique sur la protection des données à tous vos employés. Fournissez-leur les formations, informations et guides nécessaires pour les éduquer et pour les informer des modifications prévues et des responsabilités leur incombant dans le cadre du respect des dispositions du RGPD.

6. Évaluer et améliorer

Après avoir présenté votre plan de conformité au RGPD, le moment est venu de l'évaluer et de l'améliorer avant l'entrée en vigueur de la nouvelle réglementation, en mai 2018. Votre organisation se sera alors adaptée avec efficacité aux nouvelles dispositions légales et les respectera pleinement.

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Solutions

Les câbles de sécurité répondent directement au besoin des organisations de réduire les risques de violations de sécurité, en encourageant leur personnel à respecter leur politique de sécurité physique. D'autres solutions que les antivols peuvent aussi contribuer à la réduction des risques dans les bureaux et en dehors.

Sacoches SecureTrek™
Les sacoches, sacs à roulettes et à dos SecureTrek™ peuvent être attachés à un point fixe dans les endroits à haut risque de vol, comme les aéroports, les hôtels et les salons professionnels.

Filtres de confidentialité
Le « piratage visuel » de données est facile à commettre, se produit rapidement et passe souvent inaperçu.[10] Un filtre de confidentialité réduit ce risque en limitant le champ de vision.

Verrous pour ports USB
Les administrateurs système peuvent empêcher la connexion d'appareils USB à l'aide d'un verrou afin de réduire les risques d'exportation non autorisée de données ou d'attaque de logiciels malveillants.

Coffres de sécurité
Un moyen simple et rapide de recharger, synchroniser et sécuriser simultanément plusieurs tablettes et ordinateurs portables ultraminces.

Clé à empreintes digitales VeriMark™
Elle assure un accès simple, rapide et sécurisé grâce à l'identification biométrique Windows Hello™ et est compatible avec les services exigeant une authentification à double facteur, pour protéger contre les accès non autorisés et renforcer la sécurité sur Internet.

POURQUOI LA SÉCURITÉ PHYSIQUE EST-ELLE INDISPENSABLE À LA **CONFORMITÉ AVEC LE RGPD ?**

Sources :

1. Kensington IT Security & Laptop Theft Survey, août 2016
2. 2016 Data Breaches - Privacy Rights Clearinghouse
3. Breach Level Index, septembre 2017
4. Kensington IT Security & Laptop Theft Survey, août 2016
5. Information Commissioner's Office - https://ico.org.uk/action-weve-taken/data-security-incident-trends
6. Financial Services Breach Report, Bitglass, 2016
7. Verizon Data Breach Investigations Report 2016
8. IDC Executive Brief 2010 - Laptop Theft: The Internal and External Threat
9. IDC White Paper 2007 - The Threat of Theft and Loss of Laptops for the SME
10. Ponemon Institute Visual Hacking Experiment, 2015

Kensington®

kensington.com

POUR DE PLUS AMPLES INFORMATIONS, VEUILLEZ CONTACTER :

Olivier Peschard
Key Account Manager
olivier.peschard@kensington.com
+33 (0)6.83.81.39.54

Patrick Clinchard
Key Account Manager
patrick.clinchard@kensington.com
+33 (0)6.83.81.39.30

The Professionals' Choice™