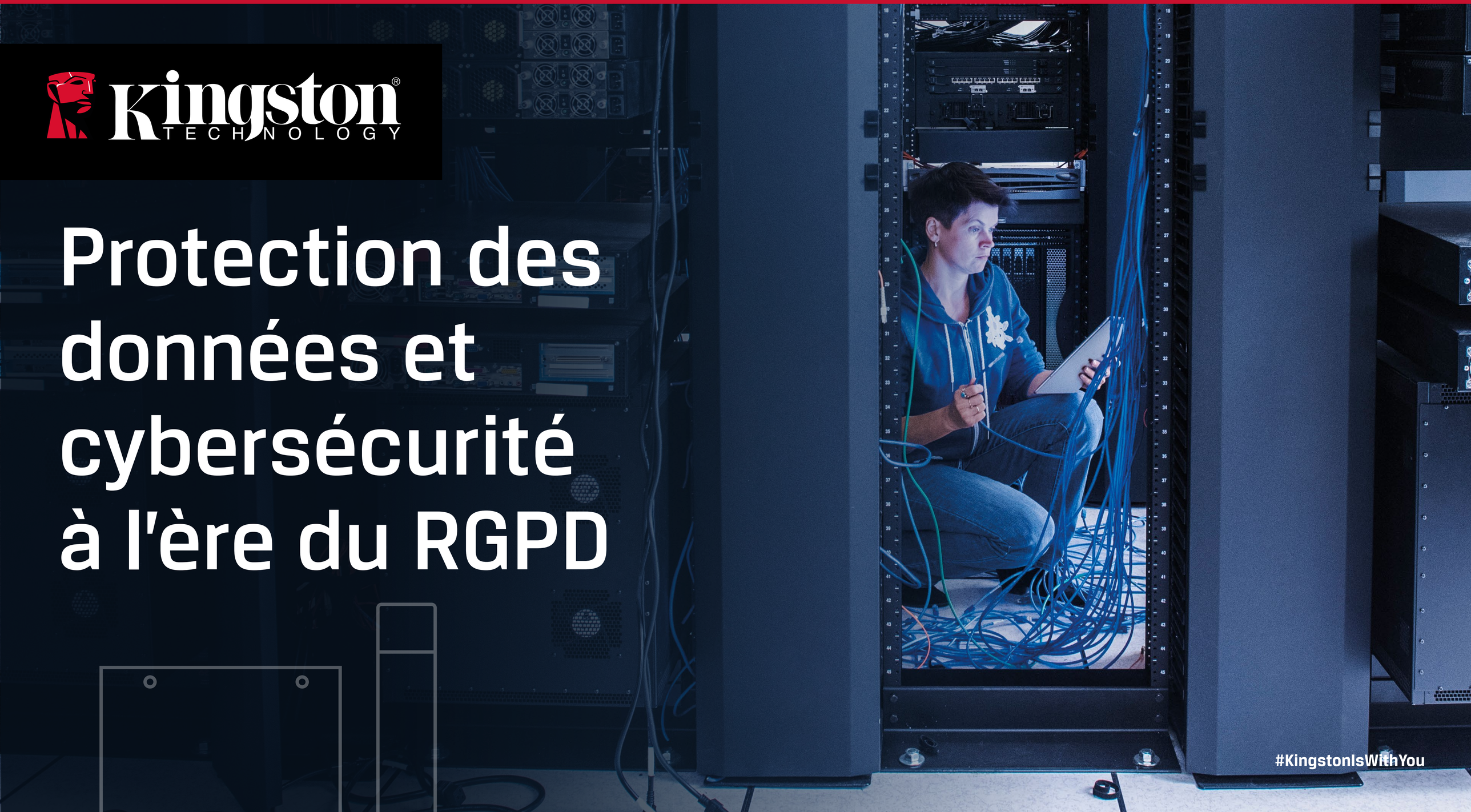
Protection des données et cybersécurité à l'ère du RGPD



#KingstonIsWithYou

Protection des données et cybersécurité à l'ère du RGPD

Avant-propos

Des milliers d'entreprises et d'organisation ont déployé de gros efforts et ont recruté à grande échelle pour relever les défis de l'entrée en vigueur du RGPD. Dont votre entreprise, peut-être. Toutefois, de par la nature changeante des cybermenaces, vous ne pouvez pas vous permettre de vous arrêter pour reprendre votre souffle. La conformité avec le RGPD ne se limite pas à répondre correctement à un questionnaire à choix multiple. Il s'agit d'un cadre d'évaluation de vos efforts continus en matière de protection des données et de cybersécurité. Vous ne pouvez pas baisser la garde.

Ce bref eBook est un recueil des connaissances de quelques-uns des spécialistes les plus expérimentés en matière de cybersécurité au Royaume-Uni appliquées à l'impact de l'entrée en vigueur du RGPD sur la protection des données. Nous vous expliquons également comment aider les employés à comprendre la nécessité de la conformité et nous voyons comment les services informatiques et les fournisseurs de technologies peuvent améliorer la protection de l'infrastructure informatique et former les utilisateurs finaux aux défis émergents pour la sécurité.

Protection des données et cybersécurité à l'ère du RGPD

Contributeurs

Ce bref ebook a été rédigé par cinq experts de la protection des données et de la cybersécurité.

Rob Allen
@Rob_A_kingston

Rob occupe les fonctions de Directeur Marketing et Services techniques. Il travaille chez Kingston Technology depuis 1996. À ce titre, Rob est chargé de la supervision des relations publiques, des réseaux sociaux, du marketing y compris le digital marketing pour tous les produits et marques Kingston.

Tara Taubman-Bassirian
@clarinette02

Tara a plus d'une corde à son arc : avocate, défenseur, médiatrice, chercheuse, consultante, conférencière et auteur. Dotée d'une riche expérience dans des domaines tels que la confidentialité, la propriété intellectuelle et la protection des données, elle s'est forgée une réputation à travers le monde, principalement au Royaume-Uni, en France et aux États-Unis.

Rafael Bloom
@rafibloom73

Rafael est directeur de Salvatore ltd. Il aide les société à gérer les défis et les opportunités au niveau de la stratégie, des ventes et des procédures qui résultent de l'évolution des technologies et des réglementations.

Miriam Brown
@Kingston_MBrown

Responsable du marketing stratégique B2B. Elle travaille chez Kingston Technology depuis 1997. Dans le cadre de ses fonctions, Miriam est chargée de définir la stratégie marketing, le contenu et les campagnes pour l'ensemble des produits B2B de Kingston.

Sally Eaves
@sallyeaves

La professeure Sally Eaves est présentée comme le porte-lambeau des technologies éthiques. Elle apporte la richesse de son expérience accumulées dans des fonctions telles que P.D.G. et Directrice technique, professeure en technologies émergentes et Conseillère stratégique internationale. Sa carrière de conférencière, d'auteur, de chercheuse et d'influenceuse qui partage des opinions authentiques et originales sur le leadership lui a valu de nombreux prix.

Protection des données et cybersécurité à l'ère du RGPD

Table des matières

Section 1 – En quoi la protection des données a-t-elle changé depuis l'entrée en vigueur du RGPD ?

Les entreprises ont parcouru un long chemin. Au cours des deux dernières années, les équipes juridiques se sont agrandies, le nombre de délégué à la protection des données a explosé[1] et la demande pour les services de conseillers externes en confidentialité a augmenté. Les exercices d'évaluation d'impact sur la protection des données sont devenus le lot commun de milliers d'organisations.

Mais il reste encore un long chemin à parcourir.

Un des plus grands défis liés au RGPD est l'attention permanente qu'il requiert. Dans la majorité des organisations, tout membre du personnel peut, à tout moment, violer les règles. La difficulté est encore plus grande dans les secteurs où la main-d'œuvre est répartie ou jouit d'un grand degré d'autonomie comme dans le secteur des soins de santé, de l'éducation ou du droit. Prenons l'exemple du droit. Nombreux sont les avocats qui n'hésitent pas à partager les détails sensibles d'une affaire par simple pièce jointe. Des professionnels de la santé peuvent échanger les données d'un patient ou les résultats d'un IRM via des adresses emails non sécurisées. Dans les organisations soumises à un stress élevé, une simple augmentation de la pression sur l'exécution des tâches peut suffire à faire passer la conformité au second plan. La productivité, semble-t-il, a priorité sur le protocole.

Il est temps de changer tout cela.

Prenons également le sujet de la prise de conscience dans le secteur des associations caritatives. Trop souvent, les associations caritatives considèrent qu'elles ne sont pas concernées par le RGPD. Et même lorsqu'elles sont parfaitement conscientes du fait que toute organisation privée, publique ou du tiers secteur doit être en conformité avec le RGPD, elles ne sont pas toujours prêtes à consacrer une partie des ressources destinées à leur cause à la protection des données. On peut les comprendre.

Depuis 2016 la demande en délégués à la protection des données a explosé et a augmenté de plus de 700 %.

Aussi noble soit cette position, elle n'en reste pas moins naïve. À côté des amendes qu'une organisation pourrait être amenée à payer pour une contravention au RGPD, les dépenses probables en technologies de l'information sont minimes.

Tara Taubman-Bassirian
@clarinette02

RGPD, Protection des données et Conseil en propriété intellectuelle

« Beaucoup d'organisation du tiers secteurs sont d'avis 'que le RGPD ne les concerne pas car elles ne sont que des associations caritatives ' . Même au niveau de la conformité du site Web, j'essaie de leur faire comprendre que le problème ne se situe pas au niveau du type de données qu'elles souhaitent récolter, mais bien au niveau des tiers auxquels elles octroieront un accès aux données des visiteurs. »

1. Varonis : A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [consulté le 26/11/2019]

En quoi la protection des données a-t-elle changé depuis l'entrée en vigueur du RGPD ?

La minimisation des données est une tendance encourageante

De nos jours, la collecte des données est omniprésente. Les Quatre géants que sont Google, Apple, Facebook et Amazon détiennent des volumes de données considérables sur leurs clients. Dans ce contexte, on pourrait s'attendre à ce que les autres entreprises copient ce comportement et recueillent le plus de données possible. Mais voilà, plus le volume de données récoltées est important, plus le risque de non-conformité augmente. Une des tendances les plus positives observées depuis l'entrée en vigueur du RGPD est sans conteste la rébellion contre la collecte excessive de données. Les entreprises intelligentes ont adopté une éthique de minimisation des données et récoltent uniquement les données utiles.

Tara Taubman-Bassirian
@clarinette02

RGPD, Protection des données et Conseil en propriété intellectuelle

« La minimisation des données est probablement une des meilleures conséquences du RGPD. La création d'une base de données signifie la création d'un risque. »

Rob Allen
@Rob_A_kingston

Directeur du marketing et des services techniques, Kingston Technology

« Nous disposons de règles strictes en matière de suppression des données. Certes, les données cruciales à l'activité doivent être correctement stockées. Mais tout le reste ? Nous les effaçons après un an. À quoi bon les conserver ?»

Les avantages vont bien au-delà de la réduction du risque. Prenons le cas du marketing par exemple. Si votre base de données marketing n'est pas bien entretenue, il se peut qu'elle contienne des données obsolètes. Quand votre base de données contient des dizaines de milliers d'enregistrement de personnes et que vous réalisez fréquemment des campagnes marketing par emails, les coûts augmentent. Les statistiques sur les performances de vos campagnes sont également tronquées.

La minimisation des données s'applique également aux données physiques. Réfléchissez à ce que vous aller imprimer (par exemple, la copie numérisée d'un passeport d'un client) ; soyez attentif à ce que vous écrivez (par exemple, les mots de passe de compte). Et si une copie physique est vraiment indispensable, stockez-la en sécurité. Certes, des montagnes de documents sur votre bureau impressionneront les visiteurs. Mais en matière de sécurité, c'est loin d'être impressionnant.

Rafael Bloom
@rafibloom73

Directeur chez Salvatore Ltd

« Nous sommes témoins d'un changement total au niveau de la manière d'envisager l'interface entre la technologie et l'activité de l'entreprise. Les leaders d'entreprise doivent vraiment atteindre ce niveau de maturité numérique.

Impact de l'exposition : des hauts dirigeants au client

Le concept de protection des données en tant que réglementation ne date pas d'hier. Mais ce sont les lourdes amendes imposées à des sociétés telles que Google[1], British Airways et la chaîne d'hôtels Marriott[2] et la couverture médiatique de ces décisions qui ont rappelé le RGPD au bon souvenir des hauts dirigeants. Il y a eu ensuite un effet cascade.

1. Varonis : A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [consulté le 26/11/2019]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [consulté le 26/11/2019]

En quoi la protection des données a-t-elle changé depuis l'entrée en vigueur du RGPD ?

Suite...

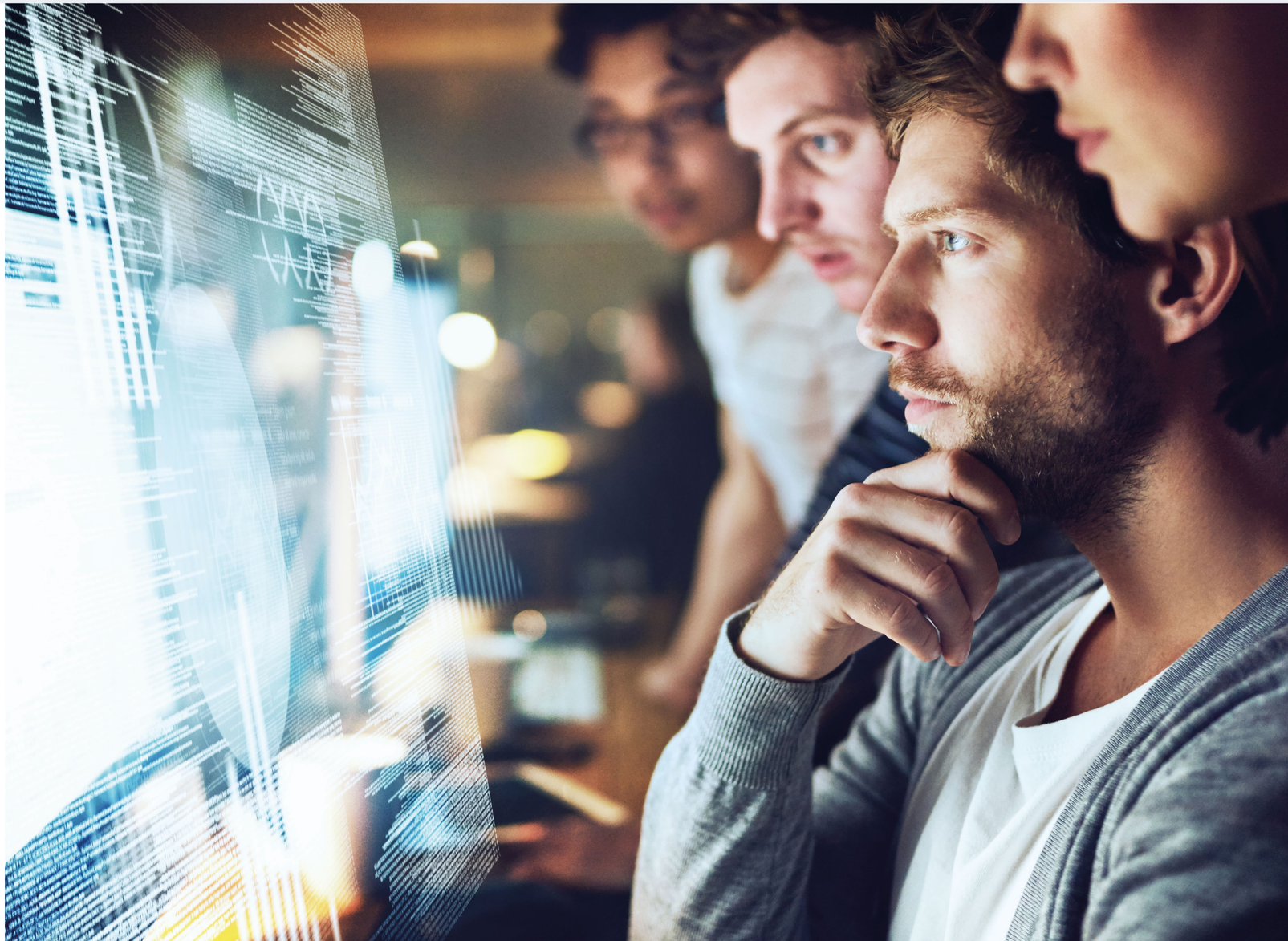
La coopération entre les entreprises a également joué un rôle important dans l'adoption de solides mesures de protection des données. De nos jours, les grandes entreprises sont très attentives à l'intégrité de la sécurité des données chez leurs fournisseurs car elles ne souhaitent pas devenir responsable par association d'une violation de données.

La plus grande attention commerciale portée au RGPD entraîne une autre conséquence : les consommateurs connaissent mieux leurs droits numériques. Et ils savent que si une société perd le contrôle des données (attention, il ne doit pas s'agir nécessairement d'une violation), ils ont le droit à une compensation. Les entreprises ne doivent pas relâcher leur attention.

Sally Eaves
@sallyeaves

P.D.G et administrateur,
Sally Eaves Consultancy

« La protection des données est devenue incontournable pour les entreprises qui peuvent gagner ou perdre la confiance des consommateurs ».



Comment les organisations assurent-elles la formation de leurs employés ?

Formation du personnel : une expression qui peut provoquer des grimaces chez vos employés.

Une raison de plus pour que votre formation soit intéressante. Un personnel formé est plus susceptible de respecter les bonnes pratiques en matière de protection des données. Et en cas de divulgation de données, l'ICO fera preuve d'une plus grande compréhension si vous pouvez démontrer que vous aviez réalisé les efforts requis pour former votre personnel à la sécurité des données.

Rafael Bloom
@rafibloom73

Directeur,
Salvatore

« Pour moi, les données sont un élément de chaîne d'approvisionnement. L'origine et tout le cycle de vie doivent être régis par une gouvernance adéquate. C'est très bien de réunir l'équipe dans une pièce pendant une demi-heure pour lui expliquer ce qu'elle doit faire… qu'il ne faut pas déchiqueter, que le mot de passe doit être robuste. Vous réduisez ainsi le risque pour l'entreprise. Mais mis à part le petit impact initial que vous avez à peu près imposé à vos collaborateurs, peut-on vraiment parler d'une différence matérielle ? Non. »

Toutefois, en avril 2019, Margo James, ministre britannique de la politique numérique, a laissé entendre que trois organisations sur dix au Royaume-Unis avaient formé leurs employés aux actions à adopter face aux cybermenaces[1]. Il est temps de prendre la formation au sérieux.

Priorité au changement de culture

La formation doit poursuivre un véritable changement des comportements et de la culture. Son but ne doit pas se limiter à réussir l'évaluation. Tout le monde est capable de trouver une offre de formation en ligne avec des questions simples sur la protection des données auxquelles tout le monde pourra répondre sans faute. La question est de savoir si ce genre de formation va vraiment contribuer à la protection de votre organisation.

Pour générer le comportement adéquat en matière de protection des données, il faut compter sur deux ingrédients. Tout d'abord, une formation intelligente et intéressante axée sur les défis uniques de votre organisation. Deuxièmement, se rendre compte que le RGPD est essentiellement une question de culture du lieu de travail qui a un impact sur le quotidien des employés. Il s'agit de traiter les données comme il se doit, à travers toute l'organisation. Prenons le service des ressources humaines par exemple. Pensez un instant à tous les détails personnels des candidats qui se trouvent sur les serveurs de messagerie. La protection des données est la responsabilité de tous.

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [consulté le 26/11/2019]

Comment les organisations assurent-elles la formation de leurs employés ?

Derrière les données se trouve un individu

Dans la première partie, nous avons vu que les consommateurs prennent de plus en plus conscience de leurs droits en matière de données. Un bon moyen de présenter la formation à la protection des données consiste à aider les membres de votre personnel à comprendre qu'il y aura toujours un individu derrière les données. Demandez-leur de réfléchir à toutes les organisations auxquelles ils ont communiqué des données et ils comprendront que la protection des données est avant tout une question de confidentialité.

Prévoir un plan d'urgence

Sally Eaves
@sallyeaves

« La formation continue des employés sur la sécurité et la protection des données est devenue incontournable pour les entreprises. Autrement dit, cette formation ne doit pas prendre la forme d'une session ponctuelle, une fois par an, mais bien être conçue comme une expérience proactive, interactive et intéressante qui viendra s'intégrer au quotidien des employés. Il faut impliquer les employés dans les discussions relatives à ce qu'il faut atténuer, gérer et défendre »

Miriam Brown
@Kingston_MBrown

« Je pense que la formation devient plus intéressante quand vous dites aux participants : et s'il s'agissait de vos données ? Si mon banquier va traiter des données sensibles à domicile sur son ordinateur portable, je préférerais qu'il utilise un disque chiffré. »

Rob Allen
@Rob_A_kingston

« Traiter les données comme s'il s'agissait des vôtres. »

Section 3 – Les services informatiques peuvent-ils garantir une meilleure sécurité des dispositifs ?

Le télétravail est devenu la nouvelle norme

Il est probable que vos collaborateurs accèdent à leur environnement de travail depuis différents dispositifs, dont des dispositifs personnels qu'il est si facile d'oublier dans le train ou le taxi. Votre défi consiste à trouver la façon d'aider votre personnel à travailler efficacement sans vous exposer à des risques pour la sécurité et des violations de données. Une personne suffit pour réduire à néant vos efforts de protection des données.

Sally Eaves
@sallyeaves

P.D.G et administrateur, Sally Eaves Consultancy

« Il faut protéger les données pendant le transfert, lors de l'utilisation et au repos. Il est essentiel que votre plan de protection, de récupération et de suppression des données englobe tous ces contextes. Il convient d'attirer l'attention sur les zones à risque souvent sous-estimées comme les clés USB non chiffrées, l'envoi de pièces jointes non chiffrées par email ou les fonctions d'un navigateur Web qui exposent les données sensibles de l'utilisateur. Vu la quantité de dispositifs connectés et l'évolution des habitudes de travail, il faut absolument veiller à ce que la sécurité des données sur un téléphone portable soit à la hauteur de la sécurité des données sur un serveur de l'entreprise. »

Authentification à deux facteurs

Pour les organisations communes, la solution la mieux adaptée et la plus simple consiste à protéger le périmètre réseau. Pour cela, l'utilisation d'un gestionnaire de mots de passe et l'adoption de l'authentification à deux facteurs peuvent suffire. L'authentification à deux facteurs désigne une méthode dans laquelle l'utilisateur doit fournir un mot de passe sur l'ordinateur portable ainsi qu'un code envoyé au numéro de téléphone portable dès que le mot de passe a été accepté.

VPN et clés USB/SSD chiffrés

Les P.M.E. se tournent de plus en plus souvent vers les VPN. Cette solution est particulièrement intéressante pour les collaborateurs qui accèdent aux données de l'entreprise via des réseaux Wi-Fi publics. Les entreprises doivent toutefois veiller à ne pas surestimer les capacités de la technologie VPN. Les VPN représentent une partie de la solution et non pas la solution intégrale. Trop souvent, les entreprises déploient un VPN et les télétravailleurs continuent d'utiliser des ordinateurs portables sans chiffrement matériel. Qui ne stocke pas des fichiers sur son ordinateur portable ? Que se passerait-il en cas de perte ou de vol de cet ordinateur ? Les clés USB et les SSD chiffrés coûtent à peine un peu plus cher que les versions standard. L'adoption de clés USB chiffrées et la sélection de SSD chiffré au niveau matériel pour les ordinateurs portables représentent un apport considérable à la résolution des défis que pose le télétravail. Et en cas de perte ou de vol d'un dispositif, vous serez certain que personne ne pourra accéder aux fichiers chiffrés. Vous pouvez même détruire les clés USB à distance.

« J'ai fait la connaissance d'un expert en cybersécurité qui me racontait comment il avait tenté de convaincre le P.D.G. d'une entreprise d'adopter l'authentification à deux facteurs : 'Non... ce n'est pas pour nous... c'est embêtant... c'est une étape en plus. Je ne veux rien savoir.' Peu de temps après, la société en question fut victime d'une fraude pour un montant de 40 000 livres sterling. »

Rafael Bloom
@rafibloom73

Directeur chez Salvatore Ltd

« En fin de compte, la meilleure manière d'améliorer la prise de conscience de la sécurité est de discuter avec les employés afin d'identifier les stratégies qui sont à la fois sûres et productives. »

Rob Allen
@Rob_A_kingston

Directeur du marketing et des services techniques, Kingston Technology

Les services informatiques peuvent-ils garantir une meilleure sécurité des dispositifs ?

Serveurs privés et MSP

De plus en plus de grandes organisations décident d'avoir à nouveau leurs serveurs sur sites. Ainsi, elles peuvent exercer un contrôle intégral sur leur parc de serveurs et les données ne sont plus stockées dans le cloud accessible au public. Il existe également des solutions hybrides dans le cadre desquelles les données non sensibles sont stockées dans le cloud tandis que les données à caractère personnel sont stockées sur site. Pour les P.M.E. et les organisations du tiers secteur, le coût d'un serveur exclusif peut être trop élevé. C'est ici qu'entrent en jeu les prestataires de services gérés (MSP) et les serveurs virtuels privés. Ces solutions permettent de renforcer la sécurité sans faire exploser les coûts d'exploitation.

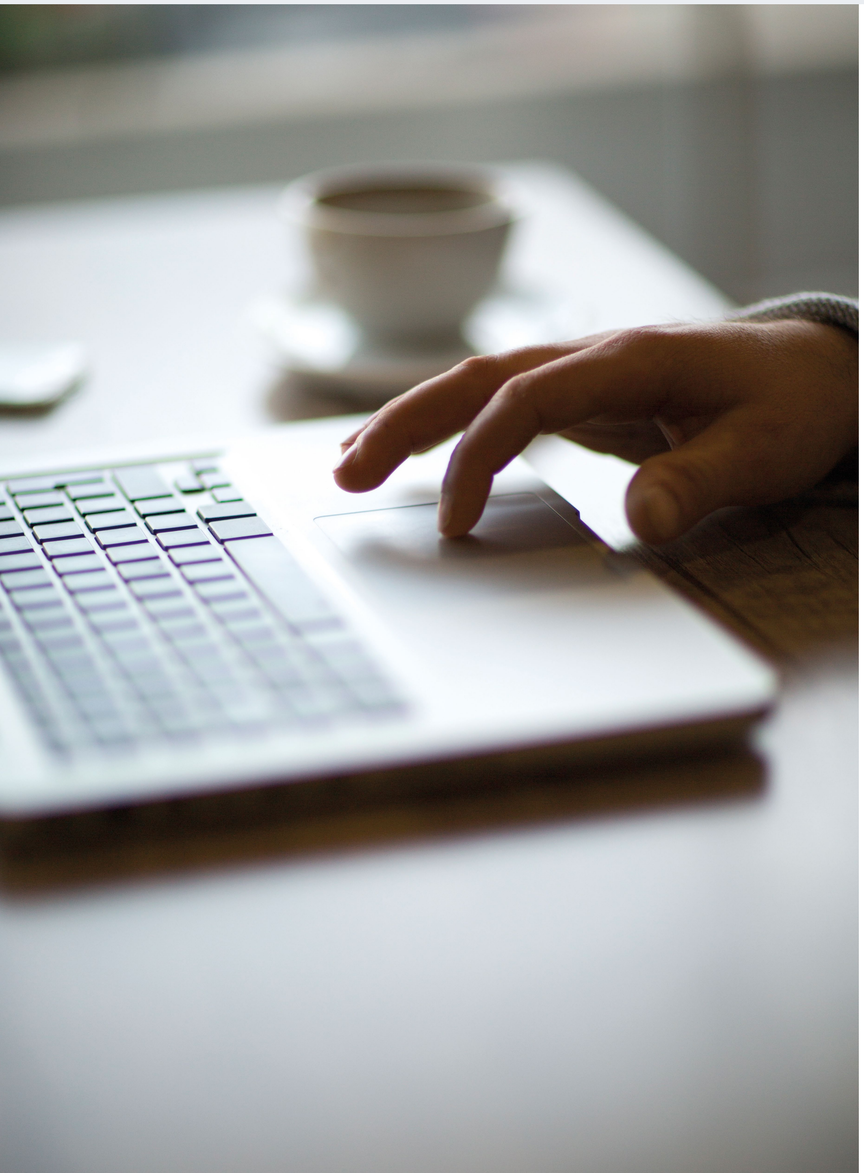
Marquage automatique des données expirées

La nécessité de supprimer les anciennes données est un des axes du RGPD. Ainsi, certains types de données à caractère personnel ne peuvent être conservés plus de sept ans. Et si le système vous rappelait automatiquement que des données sont sur le point d'expirer ? À condition de posséder la base de données adéquate, l'équipe informatique pourrait créer une action pour envoyer un message automatique au délégué à la protection des données à l'approche de la date de fin de conservation.

Travailler avec les bons vendeurs

Le secteur de la sécurité des technologies de l'information regorge de fabricants et de vendeurs. Faites vos recherches. Le secret consiste à disposer d'un système proposé par un fournisseur de solutions de confiance qui possède l'expertise adéquate pour aider les entreprises dans votre secteur. Assurez-vous que le ou les fournisseurs que vous choisissez non seulement possèdent la technologie, mais comprennent également les défis liés à l'acceptation de la sécurité des données.

Section 4 – Comment les fournisseurs de technologies peuvent-ils améliorer les processus et la compréhension ?



TLC pour délégué à la protection des données

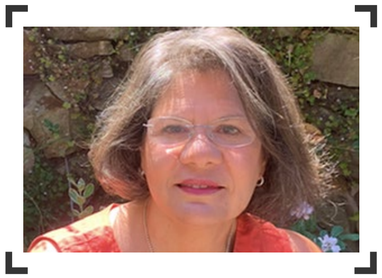
Depuis 2016, la demande en Délégués à la protection des données a explosé avec une augmentation de plus de 700%.[1] On compte actuellement plus de 500 000 délégués à la protection des données en Europe, soit six fois plus que les estimations avancées en 2017.[2] Et malgré tout, le rôle du délégué à la protection des données n'est pas reconnu à sa juste valeur.

Un délégué à la protection des données doit avoir une vue d'ensemble des mesures adoptées par l'entreprise pour garantir la sécurité et la confidentialité des données. C'est un travail à temps plein. Et pourtant, dans certaines organisations, le délégué à la protection des données n'est qu'un titre donné au membre du personnel qui comprend le mieux la technologie. Cette personne est responsable de la politique de confidentialité des données de toute l'entreprise et doit continuer à remplir les fonctions de son travail principal.

Le fait est qu'il faut une gamme de services et d'outils professionnels pour appuyer le travail de cette nouvelle espèce de délégué à la protection des données. Même si vous pouvez compter sur un délégué à la protection des données à temps plein, le domaine de la sécurité des données évolue rapidement et votre entreprise sera toujours confrontée à de nouveaux défis qui requièrent un deuxième avis. Recourir aux services d'un conseiller externe en sécurité des données peut être très utile, mais avant toute chose, votre organisation interne doit être aussi parfaite que possible.

Clarté, contingence et cohésion

Votre infrastructure informatique sera aussi robuste que son élément le plus faible. C'est la raison pour laquelle à chaque nouvelle acquisition pour votre écosystème informatique, votre fournisseur technique doit vous expliquer clairement les menaces potentielles et vous orienter sur la manière la plus sûre d'utiliser votre nouveau produit.



Tara Taubman-Bassirian
@clarinette02

RGPD, Protection des données et Conseil en propriété intellectuelle

« J'essaie d'expliquer aux personnes qui installent des caméras de vidéosurveillance partout que la sécurité n'est pas nécessairement améliorée car bien souvent, ces caméras sont installées sans mot de passe. Vous pouvez vous connectez à un site web et regardez. En fait, vous dites au voleur potentiel : viens vérifier si je suis là »

1. Varonis : A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [consulté le 26/11/2019]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [consulté le 26/11/2019]

Comment les fournisseurs de technologies peuvent-ils améliorer les processus et la compréhension ?

Il y a le problème de contingence. Que ce passe-t-il quand un produit arrive en fin de vie ou qu'il doit être mis à jour ? Les fournisseurs de technologies doivent donner des conseils de contingences sur leurs produits sans compromettre par accident les données ou sans exposer la sécurité de votre écosystème informatique élargi. Prenons le cas d'un IRM par exemple. Il possède peut-être un SSD chiffré d'une capacité de 4To pour stocker les images des patients. Mais que ce passera-t-il quand l'espace de stockage aura été épuisé ?

Les fournisseurs de technologies et les organisations doivent également favoriser un environnement de cohésion numérique et de cohésion des données, aussi bien au sein de l'organisation que lors des échanges avec des fournisseurs externes et des partenaires. Ce point est crucial pour des organisations comme le NHS qui possèdent plusieurs facettes, plusieurs départements et de multiples implantations.

Miriam Brown
@Kingston_MBrown

Directeur du marketing B2B chez Kingston Technology

« Nous avons vendu beaucoup de produit au NHS, mais nous voyons qu'il existe bel et bien des différences entre chaque trust lorsque nous posons des questions sur les stratégies et les protocoles de sécurité des données adoptés. »

Survol de l'horizon

Les technologies évoluent rapidement. Parfois plus vite que la sécurité. S'agissant des technologies émergentes, comme le paiement via reconnaissance faciale en Chine, il arrive parfois qu'une organisation se dépêche de commercialiser une technologie sans penser aux implications potentielles en matière de sécurité et de protection des données. D'ici un an ou deux, les réseaux 5G seront largement disponibles et le edge computing et les silos de données distribués deviendront une réalité. Les fournisseurs de technologie doivent pouvoir aider les organisations à profiter sans danger des technologies émergentes sans compromettre leur propre intégrité des données ou sécurité informatique.

Sally Eaves
@sallyeaves

P.D.G et administrateur, Sally Eaves Consultancy

« Je pense que nous allons commencer à voir du changement dans le RGPD. Les difficultés liées à la mise en œuvre vont laisser la place à l'optimisation des gains comme l'amélioration des processus informatiques, de la sauvegarde et de la récupération, le renforcement de la sécurité et l'exploitation de ceux-ci en tant qu'éléments différentiateurs par rapport aux autres entreprises du secteur »

Résumé

Le RGPD a été positif pour les entreprises. Il a attiré l'attention des hauts dirigeants et du public sur la confidentialité des données et la sécurité des réseaux. Ceci étant dit, la conformité requiert une attention permanente en matière de sécurité des données, jour après jours, chez l'ensemble du personnel. Vu l'évolution constante des technologies et des cybermenaces, une infrastructure de sécurité adéquate et une formation de qualité, appuyées par de solides conseils en matière de technologie et de confidentialité des données, sont désormais essentielles pour les entreprises. Rappeler à vos collaborateurs qu'il y a toujours un individu derrière les données peut être un excellent moyen d'inculquer une culture de protection des données au sein de vos employés. Et un changement de culture est bien plus efficace qu'un simple questionnaire à choix multiple.

À propos de Kingston

Kingston, avec ses 32 années d'expérience, dispose du savoir pour identifier vos défis en matière de télétravail et vous aider à les relever afin que vos collaborateurs puissent travailler en sécurité n'importe où sans compromettre votre organisation.

#KingstonIsWithYou