Garanties de sécurité physique et de protection du GDPR

Le Règlement général sur la protection des données (GDPR) de l'Union européenne exige des organisations dans le monde de repenser la manière dont elles accèdent, utilisent et conservent les données à caractère personnel. Ce livre blanc décrit les scénarios à risque pour les données susceptibles d'entraîner des sanctions administratives et des pénalités financières conformément à la nouvelle réglementation. Il expose également des pratiques exemplaires en matière de sécurité physique et de vie privée car elles représentent un aspect important mais souvent négligé de la protection des données. Ensemble, les garanties administratives, de cybersécurité et de protection physique peuvent aider à protéger les données à caractère personnel sensibles et démontrer l'engagement de l'organisation dans ce domaine.

Ce qu'il faut retenir :

- Savoir ce que le GDPR dit de la sécurité physique et des mesures de protection des données à caractère personnel.
- Découvrir ce que les experts du secteur considèrent comme un niveau raisonnable de protection des données et de la vie privée.

Vivre dans un monde dirigé par les données
Aujourd'hui, dans le cadre normal des affaires, la plupart des organisations collectent et utilisent des données à caractère personnel, aussi bien au sujet des employés que des clients, des prospects ou de tiers. Ces données sont généralement stockées sous forme électronique pour être accessibles à l'organisation[1] et à des parties extérieures. De plus, la principale fonction de certaines organisations consiste à collecter et analyser des volumes de données à caractère personnel.

Si la quantité et le type de données recueillies par chaque organisme varie, on sait maintenant qu'il n'a jamais été aussi facile de les trouver. Les gens laissent derrière eux de multiples traces de données en créant des profils sur les réseaux sociaux, en participant aux communautés en ligne, en effectuant des recherches sur Internet, en répondant aux sondages et en profitant d'offres promotionnelles et de services « gratuits » comme le stockage de photos et la musique en streaming.

La technologie permet de constituer de riches profils sur les personnes grâce à des avancées au niveau de l'intelligence artificielle, des e-tags, des balises Web, des cookies et d'autres outils de suivi.

Aujourd'hui, les efforts en matière de technologie et d'extraction de données ont permis aux organisations d'accumuler des trésors de données personnelles. Ces référentiels peuvent révéler l'âge, le statut matrimonial, la date de naissance, la formation, les hobbies, la religion, le parcours professionnel, les convictions politiques, les préférences d'achats, les nouvelles sources préférées, les revenus, le casier judiciaire, et bien d'autres informations.

Alors qu'une grande partie de ces informations est centralisée dans les bases de données d'entreprises, des poches de données sont souvent dispersées au sein de la chaîne d'approvisionnement dans des systèmes disparates qui n'ont souvent pas de mécanisme permettant de transmettre aux futurs bénéficiaires la manière et les raisons pour lesquelles ces renseignements ont été recueillis. Cela laisse les données à caractère personnel exposées à des utilisations bien éloignées du but initial pour lequel elles ont été obtenues.

Tous les jours, de nombreuses personnes au sein d'une organisation peuvent accéder à ces données stockées pour, par exemple, payer un employé, réaliser une étude de marché, lancer une campagne marketing par courriel ou suivre l'engagement des clients. Chaque point d'accès à ces ensembles de données représente la possibilité pour ces données à caractère personnel d'être mal utilisées ou de tomber entre de mauvaises mains.

Faits en bref

Qu'est-ce que le GDPR ?
Le Règlement général sur la protection des données (GDPR) vise à protéger la vie privée des personnes au sein de l'Union européenne (UE).

Quand entre-t-il en vigueur ?
Le 25 mai 2018

Qui concerne-t-il ?
Toutes les entreprises, quelle que soit leur localisation, qui contrôlent ou traitent des données à caractère personnel de personnes concernées au sein de l'Union européenne.

Qu'est-ce qui constitue des données à caractère personnel ?
Toute information concernant une personne physique ou une personne concernée. Ce peut être aussi bien un nom, une photo, une adresse e-mail, des coordonnées bancaires, des publications sur les réseaux sociaux, des informations médicales ou l'adresse IP d'un ordinateur.

Quelles sont les conséquences ?
Une amende de 20 millions d'euros ou pouvant aller jusqu'à 4 % du chiffre d'affaires global annuel (le montant le plus élevé étant retenu). Il s'agit de l'amende maximale pouvant être imposée pour les infractions les plus graves.

Où puis-je obtenir de plus amples renseignements ?

- Aperçu du règlement
- Lire le règlement
- Solutions de sécurité physique

65 %
des personnes interrogées déclarent que les cas de violations de données leur ont fait perdre confiance dans l'organisation exposée.[5]

Pour comprendre les risques de sécurité physique auxquels font face les organisations, étudiez ces scénarios :

Un employé passe en revue des données sensibles sur son téléphone alors qu'il est à l'aéroport et ne remarque pas qu'une personne à proximité regarde son écran.

- Un employé perd son ordinateur portable et les informations présentes sur le disque ne sont pas cryptées.
- Un employé s'éloigne de son bureau pour se faire un café et laisse les coordonnées d'un client affichées sur son écran, ou sur le bureau, alors qu'une personne n'y ayant pas accès passe par-là.
- Un employé mécontent prend des photos de documents laissés sur une imprimante, affichés sur un écran ou encore des identifiants de connexion scotchés à un moniteur d'ordinateur.
- Des ordinateurs portables ou fixes sont remis à des associations sans effacer entièrement leurs disques durs.
- Le cabinet d'un médecin ferme et les dossiers des patients sont jetés à la poubelle sans les déchiqueter.

Ce sont ces types de scénarios qui sont de plus en plus inquiétants, tandis que les violations de données sont très répandues dans le monde numérique d'aujourd'hui. Forrester indique qu'en 2016, les pirates informatiques ont violé un milliard de dossiers en seulement 12 mois. En milieu d'année 2017, 918 cas de violations de données ayant compromis 1,9 milliard de données dans le monde ont été signalés. Cela représente une augmentation de 164 % par rapport au premier semestre 2016.[2]

En 2016, les pirates informatiques sont compromis
1 milliard de dossiers[2]

Chaque fois que des données sont violées, l'inquiétude monte quant à savoir si leur confidentialité a pu être préservée. D'après une étude récente, les gens estiment que leur vie privée est menacée par les problèmes de sécurité et de confidentialité. En effet, 91 % de la population craint de perdre le contrôle sur la façon dont leurs données à caractère personnel sont collectées et utilisées par les entreprises. Environ le même pourcentage pense qu'il serait très difficile de supprimer des informations inexactes publiées en ligne les concernant.[3] Les piratages de grande envergure ne sont pas la seule préoccupation. Il est vrai que les petites entreprises peuvent avoir moins d'informations sur un individu mais elles n'en sont pas moins importantes pour ces personnes en cas de vol ou d'utilisation abusive.

Ces craintes continuent de monter même si des directives et des règlements stricts sur la vie privée et la protection des données sont en vigueur depuis plus d'une décennie. Le Health Insurance Portability and Accountability Act (HIPAA), le Fair Credit Reporting Act et la Directive de l'Union européenne sur la protection des données n'en sont que quelques exemples.

La Directive sur la protection des données énonce les principes comme l'exigence que les données soient sécurisées, traitées à des fins limitées et conservées uniquement pour la durée nécessaire. Cependant, s'agissant d'une « directive » et non d'une loi, la mise en œuvre et l'application dans chaque pays d'Europe ne sont pas les mêmes.

Comprendre le GDPR
Le GDPR est le règlement le plus complet et le plus efficace dans le monde pour protéger les données à caractère personnel. Il a été créé à partir de la conviction partagée que chacun possède un droit fondamental à la protection de sa vie privée. Il vise à protéger la vie privée des personnes au sein de l'UE en appliquant une nouvelle réglementation sur la manière dont les entreprises protègent, traitent et utilisent les données à caractère personnel.

Le GDPR constitue peut-être l'avancée la plus importante de ces 20 dernières années en matière de sécurité des données et de réglementation de la vie privée, à la fois en raison de ses exigences en matière de responsabilité pour la tenue des registres et de ses éventuels répercussions financières. Avec deux niveaux d'amendes, les organisations peuvent être pénalisées à hauteur de 2 % du chiffre d'affaires ou de 10 millions d'euros en cas de violations, comme pour :

- le non signalement d'une violation de données à une autorité de contrôle et aux personnes concernées ;
- la non-désignation d'un délégué à la protection des données si l'organisation en exige un.

Les organisations peuvent faire l'objet d'une amende à hauteur de 4 % du chiffre d'affaires ou de 20 millions d'euros en cas de violations, comme pour :

- le non-respect des droits de la personne concernée ;
- le non-respect d'une ordonnance d'une autorité de contrôle ;
- le non-respect des exigences relatives aux transferts internationaux de données.[4]

Ces amendes sont en sus de la perte de réputation, de valeur de la marque et de confiance en celle-ci, lesquelles peuvent être tout aussi dévastatrices pour les résultats d'une entreprise. En effet, il a été rapporté que les incidents de violation des données entraînaient une perte de confiance dans l'organisation pour 65 % des personnes concernées.[5]

Le respect du GDPR n'est pas un sujet secondaire car il tient les organisations responsables de la façon dont elles collectent, utilisent, conservent et effacent les données à caractère personnel tout en les maintenant en sécurité. Même celles qui ont mis en place des programmes de protection des renseignements personnels et de sécurité doivent réévaluer leurs processus. Plus précisément, le GDPR exige que les organisations mettent en œuvre des mesures techniques et organisationnelles appropriées pour prévenir la perte ou l'accès non autorisé aux données à caractère personnel.

Le GDPR est le règlement le plus complet et le plus efficace dans le monde pour protéger les données à caractère personnel.[1]

Cela suscite beaucoup de questions comme :

Q. Qu'est-ce qui constitue des données à caractère personnel ?
R. Toute information concernant une personne physique identifiée ou identifiable.[6] Il peut s'agir d'identifiants (comme un nom ou un numéro d'identification) ou de données révélant l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, les infractions pénales mais aussi la prédiction d'éléments concernant le rendement au travail, la situation économique, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, etc.[7]

Q. Qu'est-ce que la pseudonymisation et pourquoi dois-je m'y intéresser ?
R. Mentionné à 15 reprises dans le GDPR, le terme « pseudonymisation » est une procédure par laquelle les champs d'identification d'un registre de données sont remplacés par un ou plusieurs identifiants ou pseudonymes. Le GDPR recommande l'application de la pseudonymisation aux données à caractère personnel pour réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données.[8]

Q. Les organisations sont-elles en mesure d'obtenir le consentement des personnes pour recueillir des données à caractère personnel ?
R. Oui mais le consentement doit être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.[9] Les organisations doivent tenir un registre des consentements reçus et faire en sorte que les demandes de consentement soient présentées sous une forme qui les distingue clairement des autres demandes, et formulées en des termes clairs et simples.[10] L'article 13 énonce toutes les informations à fournir auprès de la personne concernée lorsque des données à caractère personnel sont collectées comme la finalité de la collecte des informations, les destinataires ou les catégories de destinataires des données à caractère personnel, et la durée de conservation des données à caractère personnel.

Q. Qu'est-ce qu'une Analyse d'impact relative à la protection des données (DPIA) ?
A. Une DPIA, nécessaire pour les activités à haut risque, aide les organisations à évaluer l'origine, la nature, la particularité et la gravité des risques et à mettre en œuvre les mesures appropriées pour réduire les risques tels que le chiffrement. Dans l'évaluation des risques pour la sécurité des données, il est nécessaire d'envisager les risques présentés par le traitement des données à caractère personnel comme la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée ou l'accès à des données à caractère personnel transmises, stockées ou autrement traitées pouvant entraîner un préjudice physique, matériel ou moral.[11]

Q. Dois-je désigner un délégué à la protection des données ?
A. La désignation d'un délégué à la protection des données est obligatoire chaque fois que les données sont traitées par une autorité publique (à l'exception des tribunaux dans l'exercice de leurs fonctions) ou pour une entreprise dont le cœur de métier est de procéder à des opérations de traitement nécessitant un suivi régulier et systématique des personnes concernées. Un délégué à la protection des données est également obligatoire pour toutes les entreprises qui traitent des données sensibles telles que la santé et les convictions religieuses ou politiques à grande échelle. Plus particulièrement, le délégué à la protection des données :

- doit être nommé sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données ;
- doit être un membre du personnel du responsable du traitement ou du sous-traitant ;
- doit fournir ses coordonnées à l'autorité de contrôle concernée ;
- doit être doté des ressources nécessaires pour accomplir ses tâches et conserver ses connaissances spécialisées ;
- doit être placé directement sous l'autorité du niveau le plus haut de la direction ;
- ne doit pas accomplir d'autres tâches susceptibles d'entraîner un conflit d'intérêts.[12]

Exigences de sécurité physique et de protection de la vie privée
Que doivent faire les organisations pour prévenir les violations de données ? L'article 24 du GDPR énonce la responsabilité d'une organisation de mettre en œuvre des « mesures techniques et organisationnelles appropriées » pour assurer et démontrer un traitement approprié des données à caractère personnel. L'article 32 va au-delà pour expliquer que « Lors de l'évaluation du niveau de sécurité approprié, il est tenu de rendre compte en particulier des risques que présente le traitement, résultant notamment de la destruction accidentelle ou illicite, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ».

L'accent mis sur la prévention de tout accès non autorisé constitue un aspect important de ce règlement. C'est à ce niveau que la sécurité physique est essentielle. Plus précisément, elle peut garantir de protéger les données des menaces humaines internes et externes dont le but est d'exploiter les lacunes au niveau des enceintes de votre organisation et par l'intermédiaire de votre personnel. Il s'agit notamment de limiter les données qui peuvent être observées, volées ou accessibles. Passez en revue les éléments suivants et évaluez si votre effectif dispose des mesures techniques et organisationnelles appropriées pour être conforme.

Déployez la protection des données dès la conception et la protection des données par défaut :
Pour protéger les données par défaut, les organisations doivent de manière proactive identifier et recueillir uniquement les données à caractère personnel nécessaires à leur usage prévu, conserver les données uniquement pour la durée nécessaire (principe de minimisation) et doivent faire en sorte que les données à caractère personnel ne soient pas mises à disposition d'un nombre indéterminé de personnes. Il s'agira probablement de veiller à ce que les risques pour la vie privée soient identifiés à l'avance et que les systèmes soient conçus pour atténuer ces risques, en faisant appel le cas échéant à la pseudonymisation et à l'anonymisation, en instaurant de la transparence dans les fonctions de traitement et en identifiant les personnes ou rôles spécifiques ayant besoin d'accéder aux données. Posez-vous les bonnes questions : Prenez-vous en considération les risques pour la vie privée des personnes avant de concevoir vos systèmes d'information, vos pratiques commerciales et la conception physique de vos installations ? Avez-vous rencontré votre personnel informatique pour examiner les systèmes actuels et les pratiques de traitement, pour savoir si des mesures supplémentaires sont nécessaires pour renseigner la manière dont les données à caractère personnel seront protégées pendant toute la durée de vie des informations ?

Utilisez des garanties physiques :
Si les mesures de contrôle pour la cybersécurité telles que le cryptage des données et les mots de passe sont essentielles, les contrôles administratifs et physiques « de faible technologie » sont tout aussi importants. Pour savoir où les barrières physiques sont nécessaires, identifiez les points d'accès aux informations sensibles. Les employés utilisent par exemple souvent leurs appareils mobiles pour accéder et partager des données depuis n'importe où. De plus en plus de salariés ont accès à des informations sensibles dans les espaces publics, souvent à la vue des autres. Le risque d'exposition des données au bureau est également plus important. Les bureaux agencés en open space enlèvent les obstacles physiques qui permettaient de protéger les écrans d'ordinateur. Posez-vous les bonnes questions : Avez-vous placé les écrans d'ordinateur loin des fenêtres, des portes et des zones accessibles au public ? Équipez-vous les moniteurs et les écrans d'appareils mobiles de filtres de confidentialité pour protéger les informations des éventuels regards curieux ? Les imprimantes / photocopieuses / télécopieurs se trouvent-ils dans des zones sécurisées ou sont-ils munis de capots verrouillables ? Stockez-vous les exemplaires physiques des données dans une installation dont l'accès est contrôlé ? Les déchiqueteuses sont-elles standard pour toutes les unités sur site, notamment pour les photocopieuses, les imprimantes et les télécopieurs ainsi qu'une condition sine qua non pour tous les employés en télétravail ou ceux qui utilisent des connexions à distance pour accéder aux informations de l'entreprise ?

Programmez la formation des employés :
Les programmes de formation doivent couvrir trois aspects essentiels : meilleures pratiques en matière d'observation, d'accès physique et de prévention des vols. Les employés doivent par exemple restés conscients de leur environnement lorsqu'ils accèdent et utilisent des appareils connectés dans des espaces publics via leur ordinateur portable, tablette et smartphone. Les écrans d'appareils doivent être tenus éloignés des passants et des éventuels regards curieux, surtout lorsque vous saisissez des identifiants de connexion ou des données de compte sensibles. S'agissant de l'accès physique, les organisations doivent former les employés à bien effacer les informations des tableaux blancs et à ramasser les documents confidentiels après les réunions, à mémoriser les mots de passe au lieu de les écrire, à verrouiller les armoires à dossiers et les ordinateurs portables, à utiliser des filtres de confidentialité sur les appareils et à assurer une politique de tenue des bureaux, notamment en se déconnectant des appareils laissés sans surveillance. Posez-vous les bonnes questions : Votre programme de formation intègre-t-il une prise de conscience de la situation de manière à ce que les employés apprennent à être attentifs à leur environnement et puissent identifier et répondre aux comportements suspects ? Les employés comprennent-ils les attentes de notre organisation quant à la « tenue du bureau » ? Rappelez-vous fréquemment aux employés les bonnes pratiques de sécurité qu'ils doivent suivre ?

Élaborer des politiques claires :
Afin de prouver l'engagement de l'organisation à mettre en œuvre des mesures de sécurité et de protection des renseignements personnels appropriées, ses politiques doivent énoncer les choses à faire et à ne pas faire concernant l'affichage et l'utilisation des informations par les employés et les sous-traitants à la fois en interne et à distance. Les contrats de travail doivent contenir des dispositions précises sur la responsabilité vis-à-vis de la protection des informations sensibles et confidentielles.[13] Posez-vous les bonnes questions : Avez-vous communiqué aux utilisateurs votre déclaration concernant les pratiques de protection des données personnelles et de sécurité expliquant comment votre organisation protège, élimine et donne accès aux données à caractère personnel ? Avez-vous une politique en matière d'AVA (Apportez votre propre appareil) pour régir la conduite des employés et avez-vous exigé des contrôles de sécurité dans les cas où ils accèdent à des ressources de l'entreprise depuis leurs appareils personnels ? Exigez-vous dans le cadre de votre politique de sécurité que les employés utilisent des contrôles visuels et des mesures de cybersécurité ?

Fixez des limites de stockage des données :
Définissez des durées de conservation des données personnelles conformément aux lois applicables. Effacez en toute sécurité toutes les données personnelles qui ne sont pas absolument nécessaires pour assurer les activités pour lesquelles elles ont été collectées. Posez-vous les bonnes questions : Quelles mesures de contrôle technique avez-vous mis en place pour effacer les données à temps ? Les processus de destruction de votre entreprise respectent-ils des directives de sécurité renforcées comme celles indiquées par la Publication spéciale 800-88 du NIST, comme la destruction physique des disques durs qui ont atteint la fin de vie ?

Vérifiez les fournisseurs tiers :
Faites appel uniquement aux responsables du traitement et aux sous-traitants qui donnent suffisamment de garanties en termes de connaissances spécialisées, de fiabilité et de ressources pour mettre en œuvre des mesures techniques et organisationnelles, notamment la sécurité du traitement. Posez-vous les bonnes questions : Avez-vous un programme de gestion des fournisseurs qui comporte les obligations contractuelles et définit les activités de surveillance assurées par la direction pour les tierces parties ayant accès aux données à caractère personnel ?

Créez un protocole en cas de violation des données :
Les organisations doivent être prêtes à aviser l'autorité de contrôle sans délai lorsqu'elles constatent qu'une violation de données à caractère personnel s'est produite (au plus tard dans les 72 heures lorsque cela est possible). Ou être en mesure de prouver que la violation des données à caractère personnel n'est pas susceptible d'entraîner un risque pour les droits et les libertés de personnes physiques. En cas de risque élevé, la/les personne(s) concernée(s) doit/vent être avertie(s) de la violation des données, sans retard injustifié.[14] Posez-vous les questions : Quand avez-vous pour la dernière fois passé en revue les politiques et plans de réaction et de notification de violation de votre organisation ? Vos employés savent-ils qui avertir dans l'organisation si leur appareil est menacé ou lorsqu'ils constatent une violation des données ? Avez-vous mis en place un plan de réaction en cas de sinistre et de notification de violation pour déterminer quand et comment informer les autorités d'une violation de données ?

Ayez connaissance des droits des personnes :
Les résidents de l'UE ont maintenant le droit de consulter les données à caractère personnel les concernant détenues par les organisations et de demander à ce que leurs données soient effacées dans certaines circonstances. Le droit à l'effacement exige des organisations qu'elles effacent les liens, copies ou répliques exactes de ces données à caractère personnel. Les organisations doivent fournir aux gens les moyens de formuler leur demande sous forme électronique, surtout si les données à caractère personnel sont traitées par voie électronique.[15] Posez-vous la question : Votre organisation comprend-elle ce qui est considéré comme des « données à caractère personnel » et la manière de répondre aux demandes concernant les données à caractère personnel ?

Conclusion :

Le GDPR est l'avancée la plus importante de ces 20 dernières années en matière de réglementation relative à la protection des données. Il exige que les données à caractère personnel soient gérées d'une manière qui contribue à assurer la sécurité et la confidentialité, une tâche nécessitant des mesures de sécurité techniques et organisationnelles. Et les amendes en cas de non-conformité pourraient être faramineuses. Toutefois, les meilleures pratiques énoncées dans le règlement ne sont que des résolutions normales. Personne ne veut que ses informations soient utilisées à mauvais escient et aucune organisation ne veut faire face aux répercussions d'une violation de données. Les organisations qui ne perçoivent pas la protection de la vie privée comme un fardeau mais comme une responsabilité d'entreprise peuvent s'en servir comme d'un avantage stratégique pour améliorer leur réputation et la valeur de leur marque, attirer de meilleurs employés et au final conserver la confiance du public.

www.3M.fr/filtresecrans

[1]Forrester, Lessons Learned from the World's Biggest Security Breaches and Data Abuses, 9 janvier 2017
[2]2017 Gemalto Breach Level Index, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]GfK Privacy Panel, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014.
[4]Article 83 du GDPR 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, parrainé par Centrify, 2017.
[6]Article 4 du GDPR 2017
[7]Considérant 75 du GDPR 2017
[8]Considérants 26 et 28 du GDPR 2017
[9]Considérant 32 du GDPR 2017
[10]Article 7 du GDPR 2017
[11]Article 35 et Considérants 83 et 84 du GDPR 2017
[12]Articles 37-38 du GDPR 2017
[13]Considérants 74, 77-78 du GDPR 2017
[14]Considérant 81 du GDPR 2017
[15]Considérants 59, 63, 65, 66 du GDPR 2017

Les experts de la confidentialité des écrans. | 3M