3M | Les experts de la confidentialité des écrans.

FAQ sur la préparation au GDPR

Enza Iannopollo, Forrester Research

Enza est analyste au sein de l'équipe Sécurité et risque, et une Professionnelle certifiée de la confidentialité de l'information (CIPP/E). Chez Forrester, elle couvre la protection des données, la confidentialité, l'analytique et l'internet des objets en mettant l'accent sur l'impact de la réglementation et des technologies qui les sous-entendent.

Le GDPR est l'une des évolutions les plus importantes de ces 20 dernières années en matière de réglementation relative à la protection des données. Il définit la manière dont les organisations doivent gérer les données à caractère personnel de leurs clients, employés et partenaires commerciaux sur une base continue. 3M s'est récemment entretenu avec Enza Iannopollo de Forrester Research pour discuter des mesures de sécurité, des politiques et des programmes de protection de la vie privée que de nombreuses organisations mettent en place pour se conformer à des règlements comme le GDPR. Enza nous a fourni des renseignements sur la préparation du lieu de travail et a souligné la nécessité de dispositifs de protection physique contre les menaces pour la confidentialité des données.

Voici ce qu'elle avait à nous dire :

Quels sont les enjeux ?

Les organisations peuvent être condamnées à une amende pouvant atteindre 4 % du chiffre d'affaires global annuel ou

20 millions d'euros.

Q. Les salariés sont-ils prêts à se conformer au GDPR ?

R. Nos chiffres montrent que seulement une entreprise sur trois dans le monde est prête à respecter le Règlement général sur la protection des données (GDPR). Le GDPR entrant en vigueur le 25 mai 2018, de nombreuses organisations doivent évoluer rapidement pour terminer leurs préparatifs.

Nous constatons que les entreprises ont des difficultés à répondre à l'exigence de mise en œuvre et de documentation des programmes de formation et de sensibilisation à la protection de la vie privée destinés aux employés. Les autorités de réglementation européenne ont indiqué que ces programmes sont essentiels pour le respect du GDPR. Dans le même temps, nous avons constaté que les organisations qui respectaient cette exigence avaient pu améliorer leur culture de protection de la vie privée et qu'elles avaient mis en place des pratiques exemplaires allant parfois au-delà des exigences réglementaires.

Q. Les entreprises de certaines régions sont-elles mieux préparées que d'autres ?

R. 34 % des entreprises américaines indiquent être prêtes contre 26 % en Europe.[1] Les entreprises qui ne sont pas conformes au GDPR, qu'elles en soient conscientes ou non, prennent un risque important. Les entreprises qui pensent être prêtes mais qui ne le sont pas prennent un risque encore plus grand.

Il est intéressant de noter qu'il y a plus d'entreprises aux États-Unis qui pensent être prêtes qu'en Europe. Cela est lié à l'effet extra-territorial du GDPR. Le règlement s'applique à toutes les entreprises, quelle que soit leur localisation, qui traitent ou détiennent des données à caractère personnel appartenant à des résidents de l'Union européenne. Cela signifie que non seulement les entreprises européennes mais aussi de nombreuses entreprises ayant leur siège aux États-Unis seront tenues de se conformer à ces règles strictes de protection de la vie privée.

Nous soupçonnons qu'une lecture superficielle des règles, associée à des attentes trompeuses et infondées quant à une application peu stricte du GDPR, peut remettre en question la perception qu'ont les entreprises de leur préparation.

Q. Quelles sont les garanties en matière de sécurité physique et de protection de la vie privée fixées par le GDPR ?

R. Le GDPR est un règlement fondé sur des principes. Cela signifie que les organismes de réglementation ne fournissent pas aux organisations un ensemble d'actions définitives à suivre. Au lieu de cela, les organisations doivent se pencher sur les exigences du GDPR en le regardant comme une sorte « d'état souhaité » à l'égard de leurs pratiques de traitement des données. Cela signifie également que les organisations doivent identifier et évaluer les risques spécifiques qu'elles ont besoin d'atténuer pour se conformer aux exigences du GDPR.

Lors de l'identification des risques, les entreprises doivent tenir compte de ceux liés au traitement des données, en particulier, dans le cas d'une perte accidentelle ou illicite, d'une divulgation ou d'un accès non autorisé aux données transmises, stockées ou traitées autrement. Peu importe qu'une divulgation non autorisée de données se produise parce qu'un pirate informatique lance une cyberattaque élaborée sur le site Web d'une entreprise ou qu'un intrus prenne une photo de données très sensibles affichées sur l'écran de l'ordinateur portable d'un employé. Les deux situations représentent des risques aussi sérieux l'un que l'autre et nécessitent des stratégies d'atténuation appropriées.

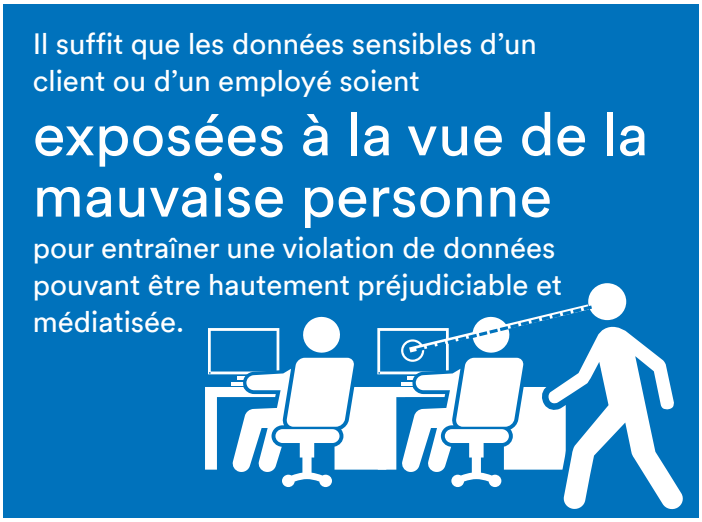
Q. Le piratage visuel constitue-t-il un risque ?

R. Absolument. Rappelez-vous : les clés d'entrée pour de nombreuses organisations se présentent sous la forme d'un nom d'utilisateur et d'un mot de passe. Il suffit d'un rapide coup d'œil sur un écran non protégé pour qu'une personne non autorisée obtienne les clés et l'accès. Sans compter que le risque augmente avec le développement croissant de l'ingénierie sociale.

Il y a un an, un journaliste a été piraté alors qu'il travaillait dans un avion.[2] Le pirate a été en mesure de décrire les détails d'un article que le journaliste écrivait, des emails personnels qu'il avait envoyés et des réunions de travail à venir. Il a indiqué qu'il avait récupéré toutes les informations en piratant le Wi-Fi de l'avion. ou, peut-être avait-il tout simplement regardé l'écran de l'ordinateur du journaliste. Bien qu'indigné, ce dernier a compris le message : alors qu'il travaillait sur un article sensible, à savoir l'analyse des répercussions considérables pour la protection de la vie privée et du fait qu'Apple refusait la demande du FBI de décrypter le téléphone d'un terroriste, il avait oublié de protéger la confidentialité et la propriété intellectuelle de son propre appareil. De même que ce journaliste, de nombreuses organisations font la même erreur en sous-estimant le risque de cyberpiratage et de piratage visuel.

Q. Quels sont les avantages de l'application de protections physiques à faible technologie ?

A. Compte tenu des reportages incessants sur les violations de données à grande échelle, il est facile d'oublier que les entreprises numériques doivent, aujourd'hui encore, relever des défis de sécurité physique. La mise en œuvre de dispositifs de protection physique comme des caméras de vidéosurveillance, des verrous sur les câbles d'ordinateurs portables et des filtres de confidentialité pour les moniteurs, les ordinateurs portables, les tablettes et les smartphones, revêt de multiples avantages. Les filtres de confidentialité apportent par exemple une stratégie saine d'atténuation des risques de violation de la vie privée et des données. Il suffit que les données sensibles d'un client ou d'un employé soient exposées à la vue de la mauvaise personne pour entraîner une violation de données pouvant être hautement préjudiciable et médiatisée.



Ils sont également en mesure d'assurer le respect de règlements autres que le GDPR. Une assistante médicale a, par exemple, été licenciée d'un hôpital à l'Université de l'Iowa il y a quelques années pour avoir violé les règles de confidentialité des données des patients. Elle a été accusée d'avoir piraté visuellement un collègue qui examinait le dossier médical d'un patient, ce qui constitue une violation de la loi HIPAA.[3]

Les mesures de sécurité physique comme les filtres de confidentialité peuvent servir de rappel visuel aux employés en leur indiquant que les meilleures pratiques en matière de sécurité et de confidentialité sont des priorités pour l'organisation. Et comme toujours avec la confidentialité visuelle, il ne s'agit pas seulement de répondre aux exigences de conformité mais aussi de protéger les biens les plus précieux d'une entreprise.

Q. Comment les entreprises peuvent-elles exploiter la protection de la vie privée afin de proposer une meilleure expérience client ?

R. Les entreprises qui appliquent des programmes efficaces en matière de suivi du GDPR et de protection de la vie privée bénéficient d'un certain nombre d'avantages commerciaux au-delà de la conformité. Notamment celui d'offrir une expérience client supérieure. La façon dont votre

organisation protège les données de vos clients peut avoir un impact direct sur la construction, ou la destruction, du sentiment de confiance sous-jacent que vos clients vous portent.

Nous savons par exemple que les clients passent à la concurrence suite à une violation de leur vie privée.[4] De plus, notre recherche sur les attitudes des clients par rapport à la protection de leur vie privée souligne que 30 % des personnes refusent d'effectuer une transaction en ligne s'ils lisent quelque chose qu'ils n'aiment pas dans l'avis de confidentialité de l'entreprise.[5]

Si vous vous engagez à protéger les données de vos clients et que vos employés reconnaissent et affichent cet engagement dans leurs interactions avec les clients, vous êtes en mesure de vous démarquer de la concurrence.

Q. Y a-t-il des entreprises qui se démarquent par leur engagement envers la protection de la vie privée et la sécurité ?

R. La protection de la vie privée est passée de sujet propre aux services juridiques au statut de valeur fondamentale pour de nombreuses organisations. Aujourd'hui, les directeurs informatiques et marketing font partie des cadres qui estiment que la protection des données contre les attaques et l'utilisation abusive figurent parmi leurs priorités. Notre étude a révélé que 23 % des entreprises du classement Fortune 100 ont adopté la protection de la vie privée dans le cadre de leurs efforts de responsabilité sociale des entreprises (RSE).[6] Près de 70 % ont inclus la sécurité dans leurs rapports de RSE.

23 % des entreprises du classement Fortune 100

ont adopté la protection de la vie privée dans le cadre de leurs efforts de responsabilité sociale des entreprises (RSE).

Nous avons également remarqué que les entreprises engagées dans la protection de la vie privée et la sécurité gagnent à être ouvertes et transparentes sur la façon dont elles traitent les données à caractère personnel. Il peut s'agir d'un moyen extrêmement utile d'apporter une assurance aux clients, aux employés ainsi qu'aux partenaires commerciaux. Toutefois, exercer ses activités conformément à cet engagement n'est pas simple. Bien souvent, les organisations doivent changer leur mode de fonctionnement pour concrétiser ces engagements et établir une culture d'entreprise qui reconnaisse la protection de la vie privée et la sécurité comme des valeurs fondamentales.

Q. Y a-t-il d'autres règlements comme le GDPR en préparation ?

R. Il n'y a aucun doute quant au fait que le GDPR annonce une tendance. Nous avons récemment terminé une nouvelle étude qui analyse les règles et pratiques de 54 pays en matière de protection de la vie privée.[7] Il apparaît clairement que des régions telles que l'Asie-Pacifique envisagent le GDPR comme une évolution possible pour leurs propres règles de confidentialité. Des éléments du GDPR, comme la résidence des données, sont également intégrés dans les règles de protection des données en Amérique latine et en Russie. Enfin, le Parlement européen travaille actuellement à la mise à jour des exigences de la directive ePrivacy. Les détails doivent encore être définis mais le projet est d'aligner les exigences de l'ePrivacy sur le GDPR.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, « Apple vs FBI shown in different light as journalist hacked mid-flight », 25 janvier 2016
[3]Veriphyr, « Medical Assistant Fired for « Shoulder Surfing » and Breaching Patient Data Privacy », 2011
[4]Ponemon Institute, « The Impact of Data Breaches on Reputation and Share Value », mai 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey (étude) (partie 2), 2016
[6]Forrester Report « The Future of Data Security and Privacy: Growth And Competitive Differentiation », 2017
[7]Forrester « Interactive Data Privacy Heat Map », 2017

FORRESTER®