Treize étapes essentielles pour répondre aux défis de sécurité du nouveau Règlement général sur la protection des données de l'UE

12 septembre 2017

Sommaire

Une fois en vigueur, le Règlement général sur la protection des données (RGPD) de l'Union européenne exigera de toutes les entreprises multinationales offrant des produits ou des services aux résidents de l'Union européenne d'adhérer à un ensemble strict de mesures sur la confidentialité et la sécurité des données. Ces exigences s'appliqueront également aux partenaires commerciaux de ces entreprises et nécessiteront l'utilisation de technologies émergentes et de concepts susceptibles de représenter une nouveauté pour les professionnels de la sécurité de l'information. Toutefois, ces professionnels peuvent tirer parti de la plupart de leurs capacités existantes, en y ajoutant quelques éléments clés afin de satisfaire à ces nouvelles exigences et permettre la conformité avec le nouveau règlement dans chacun des 28 États membres de l'UE.

Organisation de ce document

Les responsables informatiques d'un certain nombre d'entreprises multinationales ont reconnu le besoin d'amorcer le processus de modification de leur infrastructure informatique afin de satisfaire aux nombreuses exigences du règlement. Ce document a été conçu pour aider les professionnels de la sécurité de l'information à hiérarchiser les changements et les ajouts dans leurs programmes de sécurité. Les personnes familiarisées avec les régimes de protection actuels de l'UE peuvent passer directement à la section Treize étapes essentielles. Celles qui ne le sont pas encore voudront probablement lire le document dans son intégralité afin de mieux appréhender le contexte dans lequel le règlement a été promulgué. Les Annexes offrent un examen approfondi des concepts clés du règlement ainsi qu'une comparaison entre le règlement et le régime actuel, la Directive 95/46/EC de protection des données.

Qu'est-ce que le Règlement général de protection des données ?

Le 4 mai 2016, le texte officiel du Règlement général de protection des données (le « Règlement ») a été publié au Journal officiel de l'Union européenne, couronnant ainsi un processus de 4 ans visant à remplacer le régime de principe de confidentialité et de sécurité des données de l'Union européenne, la Directive 95/46/EC de protection des données personnelles (la « Directive »).[1] La Directive, adoptée par le Parlement européen et le Conseil de l'Union européenne en 1995, et qui s'applique principalement aux organisations localisées dans l'UE, a placé très haut la barre de la protection des données personnelles, mais s'est révélée inadaptée pour résoudre les défis posés par l'évolution de la technologie. Une des limitations fondamentales de la Directive était que celle-ci n'exigeait pas des États membres individuels de l'UE qu'ils intègrent un texte standard à leur législation. Au lieu de cela, elle répertoriait un ensemble de principes de confidentialité des données et amenait ces États à adopter une législation basée sur ces principes, ce qui a conduit à une version unique pour chaque État. Par conséquent, la mise en œuvre était différente selon les États et son application manquait de mordant. À l'inverse, le Règlement lie tous les membres de l'UE tel qu'il a été promulgué et, fort de 88 pages, a été prévu pour remédier à la perturbation dans la confidentialité des données provoquée par l'évolution rapide de l'informatique et des modèles commerciaux au cours des 20 dernières années. En mai 2018, le Règlement sera applicable par les autorités chargées de la protection des données (appelées « autorités de contrôle » dans le Règlement) des États membres. Tandis que des entreprises multinationales sont d'ores et déjà susceptibles de répondre à certaines des exigences de cette loi, la plupart d'entre elles vont découvrir qu'elles n'auront pas trop de ces deux années afin d'être prêtes pour sa mise en application.

En quoi le Règlement est-il important pour les professionnels de la sécurité de l'information ?

a. **Les sanctions pour infraction sont beaucoup plus sévères.** Les sanctions pour infraction des règlementations en vigueur sur la confidentialité de la vie privée dans l'UE varient d'un État membre à l'autre, les sanctions financières potentielles pouvant s'élever de 150 000 à 900 000 €. Dans un certain nombre de cas impliquant des infractions à la confidentialité de la vie privée, les autorités de contrôle possédaient peu de marge de manœuvre contre les grandes multinationales aux ressources financières importantes, qui pouvaient voir de telles amendes comme un simple prix à payer pour mener leurs activités. Cependant, d'après l'article 83(5) du Règlement, ces autorités peuvent infliger des amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % du revenu annuel de la société incriminée — le plus élevé de ces deux montants étant retenu. Dans la perspective d'un tel pouvoir de régulation, les organes législatifs en France débattent actuellement d'une augmentation du montant maximal des amendes pouvant être imposées par l'autorité de surveillance française, la CNIL, afin qu'il corresponde à celui en vigueur à l'heure actuelle dans le Règlement, plutôt que d'attendre mai 2018.

b. **La définition de « données personnelles » a été élargie.** Aux États-Unis, la définition des données personnelles identifiables (DPI) varie selon les juridictions et, au niveau fédéral, selon les agences. L'Insititut national des standards et de la technologie [National Institute for Standards and Technology (NIST)], par exemple, est relativement normatif dans sa définition des DPI :

> Tout renseignement concernant un individu conservé par une agence, y compris (1) tout renseignement pouvant être utilisé pour distinguer ou tracer l'identité d'un individu, tel que son nom, son numéro de sécurité sociale, sa date et son lieu de naissance, le nom de jeune fille de sa mère, ou son dossier biométrique; et (2) tout autre renseignement lié ou pouvant être lié à un individu, tel que des informations médicales, de formation, financières et professionnelles.[2]

Le Règlement définit les données personnelles d'une manière similaire, mais élargie en incluant « l'identité » d'une personne dans d'autres contextes :

> « données personnelles » correspond à tout renseignement relatif à une personne physique identifiée ou identifiable (« sujet des données ») ; une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par rapport à un élément identifiant tel qu'un nom, un numéro d'identification, des **données de localisation**, **un identifiant en ligne,** ou à un ou plusieurs facteurs propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de ladite personne physique[.] [Point souligné][3]

Ces ajouts à la définition de données personnelles sont importants pour les professionnels de la sécurité de l'information, car ils impliquent des données qui peuvent ne pas sembler, à première vue, de nature personnelle. Les adresses IP, Identifiants de l'utilisateur pour une application, données du système mondial de localisation [Global Positioning System (GPS)], cookies, adresses de commande d'accès aux médias [media access control (MAC)], identificateurs de ressources mobiles uniques [Unique mobile device identifiers (UDID)], et Identités internationales d'équipement mobile [International Mobile Equipment ID (IMEI)] en sont quelques exemples. Ainsi, les entreprises et les tierces parties qui « traitent » ces données devront le faire sur une base juridique répertoriée dans le Règlement. Par exemple, utiliser un logiciel pour naviguer dans un réseau afin d'en faire l'inventaire logiciel à des fins d'obtention de licence est considéré comme un traitement de données personnelles (Identifiants utilisateurs d'applications) et implique de respecter le Règlement.

c. L'Envergure de la phrase « mesures de [sécurité] organisationnelle et technique ». Le Règlement exige des « contrôleurs » (les entités qui ont le dernier mot sur la manière dont sont utilisées les données) pour « mettre en œuvre des mesures techniques et organisationnelles appropriées »[4] afin de protéger les données personnelles. En fait, le Règlement a recours à cette phrase 21 fois. Ce faisant, le Règlement cite à titre d'exemple la vague « capacité d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience continue des systèmes » et plus spécifiquement le « cryptage » et « capacité à restaurer la disponibilité et l'accès aux données en temps voulus en cas d'incident technique ou physique. »

   En substance, le Règlement demande aux contrôleurs d'employer des cadres de sécurité de l'information, qui permettent aux professionnels de créer des processus cohérents et reproductibles et d'instaurer des contrôles généralement acceptés par la communauté de la sécurité de l'information. La grosse surprise de ce Règlement pour ces professionnels se situe au niveau de la recommandation (pour ne pas dire l'exigence claire) de l'usage de la « pseudonymisation », peut-être plus connue sous le nom de « tokenisation » ou «aliasing ». Le Règlement cite la pseudonymisation 15 fois, et ce qui est frappant ici c'est que cela représente un contrôle plutôt nouveau pour la vaste majorité des professionnels, et aussi certainement pour ceux qui ne travaillent pas dans le secteur des paiements par carte, où la tokenisation dispose de devises. Cette exigence nécessitera une somme importante de travail (principalement de la part des prestataires de services tiers) afin de remanier les processus et l'architecture informatique. D'autres exigences, telles que la protection des données dès la conception et par défaut (décrite ci-dessous) ne feront que s'y ajouter.

d. **La portée juridictionnelle s'est élargie.** La portée juridictionnelle (appelée le « champ territorial » du Règlement est, en réalité, internationale. Les entreprises établies en dehors de l'UE et qui y offrent des biens ou des services aux sujets des données (c.-à-d. les individus) sont couvertes par le Règlement. Cependant, celles qui sont impliquées dans le « suivi du[] comportement » de ces sujets des données sont également couvertes. Ce concept de suivi est étroitement lié au concept de « profilage », qui comprend le traitement des données personnelles à des fins de « prédiction et d'analyse d'aspects relatifs aux performances professionnelles, à la situation économique, à la santé, aux goûts personnels, aux centres d'intérêt, à la fiabilité, au comportement, à la localisation ou aux déplacements de cette personne physique »[.][5] En d'autres termes, l'analyse des données personnelles dans le but de prévoir des préférences de consommation ou de suggérer des produits ou services, communément utilisée par les prestataires de commerce en ligne. Cette portée juridictionnelle inclut potentiellement toute organisation procédant à un recueil d'analyses à l'aide des données personnelles de sujets de données de l'UE, y compris à des fins de sécurité de l'information.

Treize étapes essentielles

1. **Utiliser un cadre de sécurité de l'information.** L'article 32 du Règlement oblige les contrôleurs et les processeurs à « mettre en pratique des mesures techniques et organisationnelles appropriées afin d'assurer un niveau de sécurité correspondant au risque ». Les cadres de sécurité de l'information représentent une collection de pratiques exemplaires accumulées par les professionnels sur l'ensemble des secteurs au fil du temps et, en tant que tels, offrent un point de départ idéal pour le développement de mesures appropriées. Les cadres tels que le cadre de cybersécurité NIST (2014)[6] et l'ISO/IEC 27001[7]/27002[8] proposent des normes industrielles reconnues pour la protection des données. Alors que l'UE ne recommande pas de cadre particulier, le respect par une entreprise des normes établies dans l'un de ces cadres attestera, sans doute, de la conformité avec l'Article 32 en cas de violation.

2. **Identifier les données personnelles, y compris les données « spéciales ».** Étant donné la définition large des données personnelles du Règlement, à peu près tous les types de surveillance des systèmes informatiques, des périphériques connectés au réseau ou des appareils mobiles impliqueront des données personnelles. Les soi-disant données « spéciales » présentent un autre défi : le Règlement les définit très largement et inclut des données génétiques ou biométriques, ainsi que des informations personnelles de santé. Les données biométriques étant considérées comme des données « spéciales », impliquées dans des contrôles d'accès logiques et aux installations physiques, les professionnels trouveront probablement que leurs propres systèmes de sécurité de l'information contiennent des données spéciales. Ils seront peut-être surpris d'apprendre que les données spéciales comprennent également :

   - les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale ; et
   - les données concernant la vie ou l'orientation sexuelle des personnes

   La « découverte de données » est l'une des approches recommandées dans ce cas. Elle comprend l'utilisation à la fois du scan actif de système et de la surveillance passive de réseau dans le but de localiser des données sensibles non cryptées dans les écosystèmes d'information d'entreprise. À partir de là, les membres de l'équipe de découverte peuvent déterminer s'ils doivent retirer ces données ou appliquer des contrôles.

3. **Inclure des actifs inconnus et le Shadow IT dans votre champ de recherche.** Deux phénomènes - les actifs inconnus et le Shadow IT - ont le potentiel pour provoquer des examens intensifs des autorités de contrôle en cas de violation ou d'abus de données personnelles. Le stockage sans autorisation, par des employés ou des fournisseurs tiers, de données personnelles d'autrui sur des appareils mobiles ou via des prestataires de services cloud provoque une exposition considérable pour des acteurs malveillants. Ces actifs ou services ne bénéficiant pas du programme de sécurité de l'information de l'entreprise peuvent comporter des failles non corrigées, ou simplement se révéler inadaptés au stockage de telles données. Une fois l'entreprise mise en cause, les autorités de contrôles voudront savoir pourquoi un programme de lutte contre de tels phénomènes n'a pas été mis en place. De plus, les autorités règlementaires américaines pourraient être impliquées, comme cela avait été le cas avec Google Street View.[9]

4. **Déterminer si vos opérations de traitement sont considérées comme étant « à haut risque ».** Le Préambule 89 du Règlement suggère que les opérations de traitement des données personnelles à « haut risque » peuvent être celles « qui, en particulier, impliquent le recours aux nouvelles technologies, ou sont d'un genre nouveau et pour lesquelles aucune analyse d'impact relative à la protection des données n'a été réalisée auparavant par le contrôleur, ou qui deviennent nécessaires au vu du temps qui s'est écoulé depuis le traitement initial ». En d'autres termes, les occasions de traitement à haut risque apparaissent sur l'ensemble de l'entreprise. De fait, il peut être souhaitable de pré-supposer que les traitements en cours ou prévus sont bel et bien à haut risque, et d'avancer à partir de ce constat.

5. **Mener une analyse d'impact relative à la protection des données (data protection impact assessment, DPIA).** Les lois fédérales américaines exigent que toutes les agences fédérales réalisent une analyse d'impact relative à la vie privée (privacy impact assessment, PIA) avant le lancement de toute nouvelle collecte de données personnelles et avant le développement ou l'obtention de moyens informatiques visant à les collecter, conserver ou diffuser.[10] Le Canada possède ses propres exigences en matière de PIA[11] et au Royaume-Uni, bien qu'elles ne soient pas obligatoires, les PIA sont courantes.[12] Le Règlement est analogue à cela, l'Article 35 sur l'analyse d'impact relative à la protection des données (ou DPIA) exigeant de manière similaire qu'une analyse soit réalisée « [l]orsqu'un type de traitement en particulier utilisant les nouvelles technologies » est susceptible d'entraîner un risque élevé pour les personnes. Les leaders de la sécurité de l'information utilisant le Cadre de cybersécurité NIST

peuvent appliquer les catégories dans la fonction Identifier afin de soutenir le processus DPIA. De même, les leaders de la sécurité de l'information utilisant la norme ISO/IEC 27002 peuvent appliquer ses fonctions Classification de l'information et Sécurité dans le développement et les processus d'assistance afin de soutenir le processus de DPIA.

6. **Réaliser et documenter les mesures d'atténuation des risques.** La capacité des organisations à réduire les risques dans le cadre du traitement des données personnelles et à documenter cette réduction est cruciale dans plusieurs contextes. Le Préambule 83 exige des contrôleurs et des processeurs qu'ils évaluent les risques inhérents au traitement, puis qu'ils mettent en œuvre les mesures d'atténuation de ces risques. Dans le cas où ce traitement est considéré à « haut risque », le Règlement exige des contrôleurs qu'ils consultent les autorités de contrôle lorsqu'ils ne sont pas capables d'atténuer ces risques (Préamb. 84 et 90). En cas de violation de données, le contrôleur devra également: documenter les mesures d'atténuation qu'il a prises à ce sujet (Art. 33(3)(d)), collaborer avec les autorités de contrôle (Art. 36), et démontrer l'efficacité de ses mesures en tenant compte d'une sanction administrative prévue (Art. 83(2)(c)). Les processeurs devront de même documenter l'atténuation des risques dans le cadre de leurs mesures techniques et organisationnelles (Art. 28(1)) ainsi que l'atténuation des dommages en cas de violation (Art. 83(2)(c)).

7. **Revoir votre utilisation du cryptage et votre plan de pseudonymisation.** Le Règlement cite l'utilisation du cryptage comme étant une exception à l'exigence pour les contrôleurs d'aviser les sujets des données en cas de violation des données personnelles, en partant du principe que les données personnelles en question étaient cryptées de manière efficace (Art. 34(3)(a)). Il cite également le cryptage comme étant une mesure de sécurité « organisationnelle et technique » (Art. 32(1)(a)). Toutefois, la pseudonymisation joue un rôle plus grand et globalement plus important dans l'ensemble du Règlement. Elle est notamment citée dans le contexte du traitement des données dans des buts non consentis au préalable par le sujet des données (Art. 6(4)(e)) comme mesure de sécurité « organisationnelle et technique » (Art. 32(1)(a)), dans le cadre d'un Code de conduite du secteur (Art. 40(2)(d))et dans le cas d'un traitement des données personnelles « à des fins d'archivage dans l'intérêt du public, de recherche scientifiques, historiques ou statistiques » [.] (Art. 89(1)). Bien que la raison d'être d'un rôle si important que la pseudonymisation dans le Règlement reste floue, les professionnels doivent commencer à étudier comment l'incorporer dans leur programme et leur budget global de sécurité.

8. **Ajouter « résilience » à votre triade CIA.** L'Article 32 du Règlement exige des contrôleurs et des processeurs qu'ils mettent en œuvre des mesures de sécurité incluant « la capacité d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et services de traitement »[.] Alors que ces trois premiers composants sont bien connus des professionnels sous le nom de « triade CIA », le quatrième, la résilience, est relativement nouveau. La Règlement ne définit pas ce terme (qui n'apparaît en fait qu'une fois). Cependant, une analyse scientifique a établi que

   > [l]a redondance semble être un élément clé, c'est-à-dire que la faille de tout composant discret ne doit pas causer de faille systémique. De plus, les différentes manières dont l'information est stockée, accessible, modifiée et transférée devront toutes être soigneusement élaborées de manière à ce qu'une faille ou une manipulation unique ne provoque pas de conséquences en aval, qui soient préjudiciables au système dans son ensemble ou qui permettent une exploitation/modification des informations.[13]

   Le concept de résilience est abordé explicitement par le Cadre de cybersécurité du NIST, qui indique que « Le cadre permet aux organisations — quels que soient leur taille, leur degré de risque ou leur niveau de sophistication en matière de cybersécurité — d'appliquer les principes et les pratiques exemplaires de gestion des risques afin d'améliorer la sécurité et la résilience des infrastructures critiques ».[14]

9. **Revoir votre Plan de continuité d'activité et de reprise après sinistre.** L'Article 32(1)(c) exige, comme mesure de sécurité, « la capacité à rétablir la disponibilité et l'accès aux données personnelles en temps opportun en cas d'incident technique ou physique »[.] Les professionnels doivent revoir à la fois leur Plan de continuité d'activité et de reprise après sinistre et les accords de niveau de services fournisseurs, afin de déterminer si des changements sont nécessaires à la lumière du Règlement. Les organisations utilisant le cadre de cybersécurité du NIST peuvent appliquer ces conseils dans la fonction Récupération. De même, les organisations ayant recours à la norme ISO/IEC 27002 peuvent appliquer ses Aspects de Sécurité de l'Information dans le cadre de la gestion de la Continuité d'Activité.

10. **Revoir votre Plan de réponse aux incidents.** En cas de violation des données, un contrôleur doit être capable d'en faire état auprès des autorités de contrôle concernées « sans retard excessif » et si possible, sous 72 heures après avoir eu connaissance de la violation en question (Art. 33(1)). En cas d'événement à « haut risque », le contrôleur doit en aviser les

sujets des données « [s]ans retard excessif » (Art. 34(1)). Un processeur doit être capable d'aviser le contrôleur « sans retard excessif » (Art. 33(2)). Les notifications de la part du contrôleur doivent contenir les éléments suivants :

- La nature et les détails de la violation ;
- Les coordonnées du délégué à la protection des données ;
- Les conséquences probables de la violation ; et
- Les mesures qui ont été prises (ou qui sont prévues) afin de remédier à la violation, y compris les efforts faits pour atténuer ses effets négatifs.

La quasi-omniprésence des lois en matière de notifications de violation des données aux États-Unis signifie que les procédures de notification de violation font probablement déjà partie de votre plan de réponse aux incidents. Lors de votre examen, déterminez si vous pouvez répondre à la norme de notification sous 72 heures ainsi que vos capacités à documenter l'atténuation post-violation aux autorités de contrôle.

Les organisations utilisant le cadre de cybersécurité du NIST peuvent appliquer ces conseils dans la fonction Réponse. De même, les organisations ayant recours à la norme ISO/IEC 27002 peuvent appliquer la Gestion des incidents liés à la sécurité de l'information.

11. **Investir en certifications ou attestations de sécurité.** L'Article 42 du Règlement introduit l'idée d'un « établissement de mécanismes de certification en matière de protection des données et de sceaux et de marques liés à la protection des données, le tout à des fins de preuve de conformité avec le présent Règlement dans le cadre d'opérations de traitement par des contrôleurs et processeurs ». Les organismes de certification de l'UE vont à présent commencer à travailler sur un sceau/une marque à l'échelle de l'UE incorporant les exigences du Règlement : le Sceau européen de protection de la vie privée. Cependant, aucun calendrier n'a été publié pour le développement et la parution de ce mécanisme de certification, ni aucune indication de ses exigences. Le processus de certification pourrait ressembler à la certification actuelle ou aux processus d'attestation tels qu'ISO/IEC 27001 ou SOC2 et, en conséquence, les entreprises devraient pouvoir s'appuyer sur les certifications ou attestations qu'elles possèdent déjà. Si votre entreprise envisage un tel investissement, le règlement n'est qu'une raison de plus de sauter le pas.

12. **Soyez prêt au « droit d'être oublié ».** En vertu des lois de l'UE, les sujets des données ont le droit d'accéder aux données personnelles que les contrôleurs possèdent les concernant, et, si leur traitement n'est pas en conformité avec les lois, ils peuvent faire corriger, effacer ou bloquer ces données. Selon l'Article 16 du Règlement, les sujets des données possèdent également le droit de rectification, et, en vertu de l'Article 17, de faire effacer leurs données personnelles uniquement sur la base du fait que les contrôleurs n'ont plus besoin d'y avoir accès. Il s'agit de ce qu'on appelle « le droit d'être oublié ». Cette section du Règlement incarne le résultat du litige entre l'autorité espagnole de protection des données et Google, selon lequel Google s'est vu imposer l'élimination de liens faisant référence aux difficultés financières d'un sujet des données espagnol qui avaient été résolues plusieurs années auparavant.[15] Cette décision était importante, car elle soutenait la proposition selon laquelle les entités hors-UE tout comme les moteurs de recherche sont sujets à la juridiction de l'UE. Étant donné le nombre de fois où les données d'entreprise sont simplement archivées plutôt qu'effacées et le volume considérable de ces données, retirer sur demande des données personnelles non pertinentes va s'avérer être un énorme défi. La connexion aux serveurs et aux appareils, qui peut à elle seule capturer un montant considérable de données personnelles, sera probablement la cible de demandes d'effacement.

13. **Appeler vos avocats.** Le Règlement représente un changement radical dans la manière dont sont régies les données personnelles des sujets des données de l'UE tout au long du cycle de vie des données, et satisfaire aux mandats du Règlement nécessitera d'être aidé par vos avocats, qu'ils soient internes ou externes à votre entreprise. Certaines opérations, telles que le transfert des données personnelles de sujets des données de l'UE vers les États-Unis, sont particulièrement litigieuses et nécessitent une coopération étroite entre les membres de l'équipe de sécurité de l'information et ceux de l'équipe juridique. Si la sécurité des réseaux et de l'information est considérée comme une base « légitime » du Règlement pour le traitement des données à caractère personnel, attendez-vous à ce que les personnes concernées ou leurs représentants du comité d'entreprise justifient des actions de traitement spécifiques.

Le livre blanc a été préparé par Scott M. Giordano sur demande de Tenable Security, Inc., et n'a pas valeur d'avis juridique.

Comment Tenable peut vous aider

Tenable propose des solutions complètes offrant une visibilité et un contexte continus, permettant des actions décisives pour réduire les failles de votre cyber exposition et mieux protéger votre entreprise. Avec SecurityCenter Continuous View® (SecurityCenter CV™), nous pouvons aider votre équipe sécurité à se préparer à la conformité RGPD en abordant les étapes essentielles suivantes :

Utiliser un cadre de sécurité de l'information. SecurityCenter CV vous aide à mettre en œuvre et à automatiser efficacement la surveillance des contrôles techniques des principaux cadres de sécurité, y compris la norme ISO/IEC 27001/27002, le Cadre de cybersécurité NIST et les contrôles CIS. Les organisations, y compris celles qui adoptent des cadres multiples, s'appuient sur SecurityCenter CV et ses outils prêts à l'emploi de rapports, tableaux de bord et d'Assurance Report Cards afin d'automatiser, de démontrer et de communiquer leur conformité de manière efficace.

Conformité des rapports. SecurityCenter CV permet aux organisations de rassembler plusieurs types de données dans une interface de reporting unique, afin que vous puissiez partager rapidement les bonnes données avec les bonnes personnes, dans un bon contexte. Par exemple, SecurityCenter CV croise les contrôles techniques dans plusieurs cadres de manière à ce que ses outils prêts à l'emploi sous forme de rapports et tableaux de bord, mais aussi d'Assurance Report Cards puissent automatiser et attester de votre conformité de manière efficace auprès d'un large public.

Identifier les données personnelles, y compris les données « spéciales ». SecurityCenter CV est capable de scanner activement les systèmes et d'écouter de manière passive le trafic réseau afin d'identifier les données personnelles chiffrées et les données spéciales au sein de votre entreprise, et ceci lors de leur entrée/sortie de votre entreprise. Vous pouvez alors déterminer la manière de retirer ces données ou d'appliquer les contrôles appropriés pour les sécuriser.

Inclure des actifs inconnus et le Shadow IT dans votre champ de recherche. SecurityCenter CV offre une visibilité totale des actifs connus et inconnus de votre réseau susceptibles de traiter des données personnelles. L'utilisation de Nessus Network Monitor (analyse passive du trafic) et d'outils de surveillance des événements vous permettra de détecter les appareils, les services et les applications en cours de fonctionnement et d'identifier les vulnérabilités associées, vous assurant ainsi une visibilité complète des risques GDPR.

Investir en certifications ou attestations de sécurité. Les certifications et attestations de sécurité exigent généralement des preuves que des contrôles sont en place et qu'ils s'effectuent de manière efficace. Avec SecurityCenter CV, vous pouvez automatiser l'analyse continue des contrôles. Cela vous permet d'évaluer et de produire des rapports sur la conformité en dehors de tout cycle d'audit, ce qui fournit une preuve de conformité permanente, permet de procéder à des ajustements en temps opportun, ou de corriger le tir si nécessaire.

À propos de Tenable Network Security

Tenable, Inc., l'entreprise spécialiste en Cyber Exposition. Plus de 23,000 entreprises de toutes tailles dans le monde entier font confiance à Tenable pour gérer et mesurer leur surface d'attaque moderne et ainsi comprendre et réduire précisément leurs cyber-risques. En tant que créatrice de Nessus, Tenable a depuis l'origine construit sa plateforme sur une compréhension profonde des actifs, des réseaux et des vulnérabilités, étendant ce savoir-faire et cette expertise à Tenable.io pour offrir la première plate-forme au monde capable d'offrir une visibilité en continu de tous les actifs, quelle que soit la plate-forme IT. La clientèle de Tenable comprend plus de 50% des sociétés du Fortune 500, de grandes organisations gouvernementales et des entreprises de taille moyenne des secteurs privé et public.

Annexe A : Concepts clés du Règlement

Données personnelles. Les « données personnelles » ne se limitent pas aux identifiants tels que l'identité nationale ou des numéros similaires, mais incluent des données pouvant finalement être reliées à un individu en croisant d'autres données. Les professionnels américains de la sécurité de l'information sont souvent surpris d'apprendre que les coordonnées commerciales et les adresses électroniques commerciales des résidents de l'UE constituent des données personnelles. La définition inclut les identifiants « en ligne » produits par « les appareils, les applications, les outils et les protocoles », ce qui signifie qu'à peu près tous les logiciels et les appareils électroniques produisent des données personnelles. Les données biométriques, telles que celles obtenues à partir de scanners d'empreintes digitales ou rétiniennes, et les données génétiques sont considérées comme des données personnelles « spéciales » et nécessitent le consentement explicite du sujet des données.

Traitement. Toute action exécutée sur des données personnelles, y compris le stockage, est considérée comme du « traitement », même si elle n'est pas effectuée par des « moyens automatisés », et entre dans le champ d'application du Règlement. En conséquence, les arguments selon lesquels une action précise ne constitue pas un traitement sont probablement voués à l'échec. Permettre que des données soient automatiquement effacées en vertu d'une politique de conservation des documents, par exemple, sera recevable.

Contrôleur et processeur. Un contrôleur de données est une entité qui détermine « les fins et les moyens du traitement de données personnelles », une phrase qui a fait l'objet de nombreux débats. Un processeur est une entité qui « traite les données personnelles au nom du contrôleur ». La distinction entre les deux, cependant, est également souvent sujette à débat. Par exemple, les agences de voyages se considèrent comme étant le co-contrôleur des organisations en contrat avec elles pour fournir des services d'organisation de voyage aux employées, même si ces agences n'ont pas accès aux données de ces employés en dehors de celles présentes dans ledit contrat. En vertu du Règlement, le processeur possède sans conteste tous ou presque tous les droits du contrôleur, et est autant exposé aux sanctions règlementaires.

Mesures techniques et organisationnelles. La phrase « mesures techniques et organisationnelles » n'est pas définie par le Règlement, mais peut être considérée comme l'égale des contrôles administratifs et techniques cités dans les articles NIST Framework for Improving Critical Infrastructure Cybersecurity[16] et ISO/IEC 27002 Code of Practice for Information Security Controls.[17] La principale section sur la sécurité de l'information dans le Règlement (Article 32) indique qu'en analysant le niveau approprié de sécurité, « il faudra prendre en compte... les risques que présente le traitement, en particulier la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non-autorisée ou l'accès à des données personnelles transmises, stockées ou traitées par ailleurs ». L'approche basée sur le risque étant déjà une pratique courante dans le développement et le déploiement des programmes de sécurité de l'information, cette clause représente un certain soulagement pour les professionnels se sentant assiégés et leur budget. L'Article 32 offre également un soulagement (potentiel) supplémentaire : un « mécanisme de certification homologué » peut être utilisé pour valider la conformité. Même s'il est trop tôt pour déterminer si les certifications existantes (telles que ISO/IEC 27001) peuvent être exploitées afin d'obtenir une certification homologuée par l'UE, l'Article 32 offre cette possibilité.

Protection des données par conception et par défaut ; minimisation des données. La « protection des données par conception » est la mise en œuvre par l'UE de la « Confidentialité de la vie privée dès la conception » (Privacy by Design, ou PbD), qui est la philosophie et l'approche consistant à englober la notion de vie privée dans la conception des technologies, des pratiques commerciales et du design physique.[18] Le Règlement (Article 25) exige du contrôleur qu'il incorpore des mesures de protection de la vie privée au moment où le traitement est envisagé et lorsqu'il est lancé. L'Article 25 cite la pseudonymisation comme faisant partie de ces mesures, et va plus loin en mettant en œuvre le principe de « minimisation des données », que le Règlement définit comme une utilisation des données personnelles « adéquate, pertinente et limitée à ce qui est nécessaire en lien avec les fins pour lesquelles elles [les données personnelles] sont traitées[.] ». L'Article 25 exige également que le contrôleur de données mette également en œuvre des mesures qui, par défaut, assurent que « seules les données personnelles nécessaires pour chaque but particulier du traitement soient traitées ». Il précise par ailleurs que ces mesures « devront assurer que par défaut les données personnelles ne soient pas rendues accessibles sans intervention de l'individu auprès d'un nombre indéfini de personnes physiques ». L'Article 25 pose un gros problème aux professionnels pour un certain nombre de raisons, dont la majorité est en lien avec le coût et le risque de révéler certaines faiblesses. Historiquement, les contrôles de sécurité de l'information ont toujours été mis en œuvre après que les processus commerciaux aient commencé à être utilisés. Apporter des changements à ces contrôles et au programme de sécurité qui y est associé sera un processus de plusieurs années, au mieux, et demander à une organisation de procéder à ces changements « uniquement » pour appuyer le Règlement est susceptible de rencontrer un certain scepticisme et d'être rejeté. Chaque fois qu'un programme de sécurité est repensé, la possibilité

d'introduire de nouvelles faiblesses ou d'en rouvrir qui existent déjà est présente et peut très bien mettre en échec tout le processus. Cet article est peut-être le plus problématique pour les professionnels et leurs entreprises et mérite que soit ouverte une discussion sur le recours à des contrôles compensatoires en lieu et place de la Confidentialité de la vie privée dès la conception (Privacy by Design, ou PbD).

Evaluations des impacts liés à la protection des données. L'Article 35 exige que lorsque le traitement de données personnelles est envisagé et est « susceptible d'avoir pour conséquence un risque pour les droits et les libertés de personnes physiques », le contrôleur de données doit réaliser une analyse portant sur l'impact potentiel sur les données personnelles. Cela, bien sûr, pose la question de la définition de « haut risque », de ce que sont « les droits et les libertés des personnes physiques », et du contenu nécessaire de ladite analyse.

Annexe B : Résumé des considérations relatives à la sécurité de l'information en vertu de la Directive 95/46/EC de l'UE sur la protection des données et du Règlement général sur la protection des données

Considération	Article concernant la Directive sur la protection des données	Préambule ou article concernant le Règlement général sur la protection des données
Applicable à :	Contrôleurs de données. Art. 4.	Contrôleurs de données et processeurs de données. Art. 3(1).
Risque de responsabilité engagée pour :	Contrôleurs de données. Art. 23.	Contrôleurs de données et processeurs de données. Art. 82 et 83.
Portée juridictionnelle	Limité principalement aux opérations au sein des États membres de l'UE. • Voir les normes dans l'Art. 4 (a) « mise en place du contrôleur » et l'Art. 4(c) « utilisation des équipements ».	Mondial. • Voir Préamb. 131. S'applique « au traitement réalisé dans le contexte d'une offre de biens ou de services visant les sujets des données sur le territoire de l'État membre... » • Voir également l'Art. 3(2). S'applique à « l'offre de biens ou de services » à, ou la surveillance du comportement des sujets de données de l'UE.
Que peut-on qualifier de « donnée personnelle » ?	Un « numéro d'identification ou [] un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, mentale, économique, culturelle ou sociale...». d'une personne physique. Art. 2(a).	Un « nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou [] un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique »[.] Art. 4(1).
Les mesures de sécurité de l'information représentent-elles un « intérêt légitime » du contrôleur et du processeur ?	Flou. • Voir la Directive 2009/136/EC (directive de l'UE sur les cookies), qui cite « [l]e traitement de données de trafic... dans le but d'assurer la sécurité des informations et des réseaux » comme intérêt légitime.	Oui. Préamb. 49 et 71.
Exigences relatives à la sécurité de l'information	Les contrôleurs de données doivent « mettre en œuvre des mesures techniques et organisationnelles appropriées afin de protéger les données personnelles... » Art. 17(1).	Les contrôleurs de données ou les processeurs « doivent mettre en œuvre des mesures techniques et organisationnelles, afin d'assurer un niveau de sécurité approprié au risque...». Art. 32(1).
Notification de Violation	Aucun. • Mais voir la Directive 2002/58/EC sur la vie privée en ligne, qui exige d'aviser les autorités nationales compétentes chargées de la protection des données (Data protection authority, DPA) en cas de violation (Art. 4(3)).	• Contrôleur aux autorités de contrôle : « [s]ans retard excessif, et, si possible, jamais après 72 heures... ». Art. 33(1). • Processeur au contrôleur : « [s]ans retard excessif... ». Art. 33(2). • Contrôleur au sujet des données : « [s]ans retard excessif... ». lors d'événements à « haut risque » Art. 34(1).

	• Voir également le Règlement No. 611/2013 de la Commission européenne, qui aborde le thème des notifications de violation pour les prestataires de télécommunications, les fournisseurs d'accès Internet (FAI), etc.	
Protection de la vie privée intégrée/ incorporée au cours de la conception ou de la mise en œuvre du système	Non requis.	Obligatoire. « [L]e contrôleur devra…mettre en œuvre des mesures techniques et organisationnelles appropriées… prévues pour appliquer les principes de protection des données…de manière efficace et pour intégrer les protections nécessaires dans le traitement[.] » Art. 25(1).
Analyses d'impact relatives à la protection des données (DPIA)	Non requis.	Obligatoire pour les cas de traitement à « haut risque ». Art. 35(1).
Sanctions financières potentielles	Cela varie pour chaque État membre ; plafond maximum entre 150 000 et 900 000 €.	Jusqu'à 20 millions d'euros ou 4 % du revenu annuel de la société incriminée, le plus élevé de ces deux montants étant retenu. Art. 83(5).

[1] Directive 95/46/EC du Parlement et du Conseil européens du 24 octobre 1995 sur la protection des personnes en ce qui concerne le traitement des données personnelles et leur libre circulation. O.J. (L 281) (23/11), pp. 0031-0050.
[2] Erika McCallister, et al., NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) E-1 (2010), disponible à l'adresse http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.
[3] Règlement (EU) 2016/679 du Parlement et du Conseil européens du 27 avril 2016 sur la protection des personnes physiques en ce qui concerne le traitement des données personnelles et la libre circulation de ces données, qui annule la Directive 95/46/EC (Règlement général sur la protection des données), Art. 4(1). O.J. (L 119) 4.5.2016, p. 33.
[4] Le Règlement utilise l'anglais britannique et le présent livre blanc utilisera l'orthographe en anglais britannique des mots tirés directement du Règlement.
[5] Voir Id. à n3, Art. 4(4).
[6] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, v1.0 (12 février 2014), disponible à l'adresse http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[7] Organisation internationale de normalisation. ISO/IEC 27001 - Management de la sécurité de l'information, disponible à l'adresse http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.
[8] Organisation internationale de normalisation. ISO/IEC 27002:2013. Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour le management de la sécurité de l'information, disponible à l'adresse http://www.iso.org/iso/catalogue_detail?csnumber=54533.
[9] Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data, disponible à l'adresse http://www.ct.gov/ag/cwp/view.asp?Q=520518.
[10] Voir Section 208 de l'E-Government Act de 2002 (Droit public 107-347, 44 U.S.C. Ch. 36).
[11] Voir Directive on Conducting Privacy Impact Assessments, disponible à l'adresse http://www.statcan.gc.ca/sites/default/files/media/dcpia-defrvp-eng_2.pdf.
[12] David Wright, et al., Trilateral Research & Consulting, Privacy impact assessment and risk management, Report for the Information Commissioner's Office, 4 May 2013, at 6, disponible à l'adresse https://ico.org.uk/media/for-organisations/documents/1042196/trilateral-full-report.pdf.
[13] Matt Bishop, et al., Resilience is more than availability. In Proceedings of the 2011 workshop on New security paradigms workshop (NSPW '11)(2011). ACM, New York, NY, USA, 95-104, disponible à l'adresse http://dx.doi.org/10.1145/2073276.2073286.

[14] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, 12 février 2014, p. 1, disponible à l'adresse http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[15] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014), disponible à l'adresse http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.
[16] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, 12 février 2014, disponible à l'adresse http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[17] Voir, de manière générale, ISO/IEC 27002 Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information, Seconde Édition, 01-10-2013, disponible à l'adresse http://www.iso.org/iso/catalogue_detail?csnumber=54533.
[18] Russell R. Densmore, Privacy Program Management Tools for Managing Privacy Within Your Organization (2013), p. 88. Pour une description approfondie de la notion de Confidentialité de la vie privée dès la conception, voir https://www.ipc.on.ca/english/privacy/introduction-to-pbd/.