SOPHOS
Security made simple.

Nouvelle législation européenne sur la protection des données

Quelles sont les exigences en matière de protection des données et comment s'y conformer

Jusqu'à peu, la pièce maîtresse de la législation de l'UE en matière de protection des données à caractère personnel, à savoir la directive 95/46/CE datait de 1995. Les choses ont bien changé depuis cette période. Par exemple, les appareils mobiles sont omniprésents et il n'est pas rare qu'une seule personne en possède deux ou trois. Les données professionnelles sensibles sortent aujourd'hui du périmètre de sécurité traditionnel mis en place par l'entreprise. Les employés s'envoient des documents par e-mail, utilisent leurs smartphones et tablettes personnelles pour accéder à leurs données professionnelles et stockent leurs données dans le Cloud. Les violations des données personnelles sont monnaie courante aujourd'hui et font courir aux clients le risque de se voir voler leur identité et de subir de lourdes pertes financières. Les entreprises, quant à elles, doivent faire face au risque de perdre la confiance de leurs clients et investisseurs.

Ce livre blanc discute des conséquences qu'aura pour les entreprises le nouveau Règlement **Général sur la Protection des Données** (RGPD) de l'Union européenne, adopté en avril 2016 et qui entrera pleinement en application en mai 2018.

Livre blanc Sophos Mai 2016

Comme la majorité des états aux États-Unis, de nombreux pays de l'Union européenne (UE) ont promulgué leur propre loi de protection des données afin de s'adapter à cette nouvelle situation d'érosion du périmètre de sécurité du réseau. Semblablement à ce qui se passe aux États-Unis, les règlements européens sur la protection des données varient d'un pays à l'autre de l'UE. Il n'y avait pas eu de réforme importante de la réglementation sur la protection des données dans l'UE pendant une longue période. Les développements technologiques depuis 1995 et la prolifération des données sur tous les nouveaux supports rendaient nécessaires la modernisation et l'harmonisation des législations sur la protection des données au sein de l'UE.

En janvier 2012, la Commission européenne a initié un projet de réforme sur la protection des données, qui a abouti à l'adoption en avril 2016 par les institutions de l'Union Européenne d'un nouveau Règlement Général sur la Protection des Données. Ce règlement établit un cadre juridique plus solide et plus cohérent dans toute l'Union et vient remplacer la mosaïque existante de lois votées par les pays membres. L'objectif est de renforcer les libertés et droits fondamentaux des citoyens de l'UE, notamment leur vie privée, de restaurer un climat de confiance dans l'environnement en ligne et de mieux protéger les données des consommateurs, en demandant aux entreprises d'adopter les nouveaux processus et contrôles en matière de protection des données. Ce nouveau Règlement général sur la protection des données contient 99 articles[1] qui, comme pour tout texte de loi, peuvent prêter à confusion. L'objectif de ce livre blanc n'est pas d'aider le lecteur à comprendre tout le texte de loi. Nous lui proposons plutôt de se pencher sur la nécessité de protéger les données, pour ne pas tomber sous le coup des lourdes amendes qui pourront être infligées à partir de mai 2018. Vous trouverez plus de renseignements sur la réforme en consultant les liens répertoriés à l'annexe du présent document.

L'Union européenne (UE) est un partenariat économique et politique unique entre 28 nations européennes qui, ensemble, englobent la vaste majorité du continent. Bien que chaque pays possède sa propre culture et ses propres lois, les pays de l'UE sont également soumis à une intégration économique, politique et législative dans de nombreux domaines. Cette intégration a pour but d'éviter de nouveaux conflits entre les États membres et d'accroître le commerce et la libre circulation des biens et des personnes dans l'Union.

Éléments de base de la réforme

Le nouveau Règlement général sur la protection des données a établi un record de 3999 amendements votés au Parlement pour un même texte de loi. Suite à ce processus de révision, le Parlement Européen a apporté son soutien indéfectible à la réforme de la protection des données au cours d'un vote quasi unanime de 621 voix en sa faveur, 10 voix contre et 22 abstentions au mois de mars 2014. Après un nouveau cycle de discussions et d'amendements mené avec le Conseil de L'Union européenne, le règlement (UE) 2016/679 a finalement été adopté en avril 2016.

Ce règlement abroge l'ancienne directive 95/46/CE de 1995 et sera pleinement applicable à partir du 25 mai 2018. Comme il s'agit d'un règlement et non d'une directive, le texte s'applique en l'état pour tous les pays membres de l'Union européenne, sans nécessiter de transcriptions dans les cadres législatifs nationaux. Nous disposons donc du texte définitif.

Ce règlement ne peut donner lieu qu'à des sanctions administratives, qui peuvent cependant être très conséquentes, allant jusqu'à 4 % du chiffre d'affaires annuel mondial d'une entreprise.

La réforme contient également un volet pénal, qui pourra agraver les sanctions. Elle fait l'objet de la directive (UE) 2016/680. Comme toute directive, nous devrons attendre sa transcription dans les cadres législatifs des différents pays membres de l'Union européenne avant de disposer des textes applicables, et nous n'en discuterons donc pas

ici.

Le nouveau Règlement (UE) 2016/679

Au premier abord, le nouveau règlement peut paraître intimidant avec ses 99 articles et sa centaine de pages. Il ne faut cependant pas hésiter à le consulter car l'essentiel de ce qui concerne les entreprises tient dans quelques articles clairement exprimés.

Pour une première lecture, on peut laisser de côté le préambule de 173 paragraphes, qui précise et restitue l'esprit des débats pendant les quatre années de discussion législatives sur le texte, de même que les deux premiers chapitres de dispositions générales et principes.

Le chapitre III (Droits de la personne concernée) constitue le cœur du règlement, avec douze articles sur une petite dizaine de pages:

Article 12: Transparence des informations et des communications
Article 13: Informations à fournir si les données sont collectèées auprès de la personne
Article 14: Informations à fournir si les données ne sont pas collectées auprès de la personne
Article 15: Droit d'accès de la personne concernée
Article 16: Droit de rectification
Article 17: Droit à l'effacement (« droit à l'oubli »)
Article 18: Droit à la limitation du traitement
Article 19: Obligation de notification pour la rectification ou l'effacement de données
Article 20: Droit à la portabilité des données
Article 21: Droit d'opposition
Article 22: Décision individuelle automatisée, y compris le profilage
Article 23: Limitations

Les chapitres IV (Responsable du traitement et sous-traitant) et V (Transfert vers des pays tiers) rassemblent sur 27 articles toutes les responsabilités qui incombent aux entreprises, et le chapitre VII (Voies de recours, responsabilité et sanctions) détaille en 8 articles tout ce qui concerne les sanctions administratives potentielles.

Les autres chapitres concernent essentiellement les autotités de contrôle.

Confidentialité des données personnelles

Nous avons extrait de ce texte les principaux articles qui concernent la nécessité de préserver la confidentialité des données personnelles.

L'**Article 32**[5] aborde la sécurité du traitement des données :

1. *Compte tenu de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris*

Terminologie des propositions sur la protection des données

Les **données personnelles** correspondent à toutes les information qui, directement ou indirectement, permettent d'identifier un individu. Il peut s'agir de données privées, professionnelles ou publiques. Il peut s'agir d'un nom, d'une photo, d'une adresse électronique, de coordonnées bancaires, de messages publiés sur des réseaux sociaux, d'informations médicales ou de l'adresse IP de son ordinateur.

Responsables du traitement des données
Décident des conditions, des fins et de la manière dont les données à caractère personnel sont traitées. Il peut s'agir d'individus, de sociétés ou d'autorités publiques. Par exemple, des docteurs, des pharmaciens ou des politiciens qui possèdent des données sur leurs patients, leurs clients et leurs électeurs.

Sous-traitants
Traitent les informations personnelles sous l'autorité du responsable du traitement des données mais ne prennent aucune décision sur les conditions, fins et sur la manière dont le traitement est effectué. Par exemple, les sociétés de gestion de paie et les sociétés d'études de marché peuvent traiter des informations personnelles pour le compte de tiers (d'autres sociétés ou autorités publiques qui auraient le rôle de responsables du traitement des données dans ces cas de figure). Toutefois, s'ils décident des conditions et des fins ou agissent au-delà du cadre des instructions reçues par les responsables du traitement des données, ils endossent le rôle de responsables du traitement des données pour cette activité de traitement spécifique.

Personne concernée
Données personnelles utilisées pour identifier une personne. Cette personne est la « personne concernée. »[4]

entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

(...)

En termes simples, l'article demande aux entreprises de mettre en œuvre les mesures de sécurité qui s'imposent pour protéger efficacement leurs données personnelles.

Le chiffrement est une des rares technologies à être mentionné explicitement comme mesure technique appropriée. Ni le texte d'origine de la Commission européenne, ni le texte amendé par le Parlement européen, ne citaient explicitement de technologie appropriée. Il est dont particulièrement remarquable et significatif que le Conseil de l'Union européenne ait souhaité renforcer le texte en ajoutant cette mention particulière sur le chiffrement.

En cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, l'**Article 33**[6] indique que l'entreprise doit adresser une notification à l'autorité de contrôle si possible dns les 72 heures au plus tard après en avoir pris connaissance.

En revanche, l'entreprise sera tenue ou non de communiquer à la personne concernée la violation de ses données. Sur ce point, l'**Article 34**[7] mentionne :

1. *Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.*
2. *(...)*
3. *La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:*

a) le responsable du traitement a mis en oeuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

(...)

Si, au moment de la perte de données personnelles, les mesures de protection techniques rendaient les données incompréhensibles (et donc inutilisables par toute personne qui n'est pas autorisée) *et* que l'entreprise prouve, à la satisfaction de l'autorité de contrôle, qu'elle a mis en œuvre de telles mesures de protection techniques, elle ne sera donc pas tenue de

communiquer à la personne concernée la violation ou le vol de ses données personnelles.

Une fois encore, le chiffrement est cité explicitement comme mesure technique appropriée.

Si une entreprise omet d'adopter des règles internes ou de mettre en œuvre les mesures requises pour assurer et prouver le respect des obligations énoncées, ne se conforme pas aux obligations énoncées au présent règlement ou si elle omet de notifier la violation de données à caractère personnel en temps utile ou de façon complète à l'autorité de contrôle, l'**Article 83**[8] stipule que l'autorité de contrôle peut lui infliger au moins l'une des sanctions administratives suivantes :

> 4. *Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:*
>
> *a) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43;*
>
> *(...)*

En bref : si vous n'adoptez pas la bonne technologie de protection des données personnelles, vous vous exposez au risque d'avoir à payer une lourde amende à l'autorité de contrôle. Vous encourez également le risque de voir votre réputation ternie et de perdre la confiance de vos clients. À l'inverse, les entreprises qui chiffrent leurs données assurent aussi bien leur propre protection que celle de leurs clients.

Qui est visé par cette nouvelle réforme ?

Le nouveau Règlement général sur la protection des données de l'UE est d'intérêt général. En effet, il aura des répercussions sur toutes les entreprises ayant des relations commerciales avec des citoyens européens quel que soit l'endroit où se trouve l'entreprise.

Il se rapproche des lois américaines sur la protection des données. Par exemple, une société établie en France ayant des clients américains en Californie doit impérativement respecter la loi californienne sur la protection des données. Si cette société a également des clients dans l'état du Massachusetts, elle doit également respecter la loi sur la protection des données du Massachusetts, et ainsi de suite.

Les principaux avantages du nouveau Règlement général sur la protection des données de l'Union européenne sont :

- Un marché européen, une loi : les entreprises européennes et non européennes n'auront plus à rechercher et à connaître les détails de 28 règles et règlements différents.

- Procédure unifiée : la même procédure sera suivie en cas de violations et/ou d'enfreintes.
- Les mêmes règles s'appliqueront à toutes les entreprises : quel que soit l'endroit où se trouvent les entreprises, la même série de lois sera applicable à toute activité commerciale effectuée au sein de l'Union européenne.

Comment respecter la nouvelle législation

Pour la majorité des entreprises qui devront respecter le nouveau Règlement sur la protection des données, le meilleur moyen de se préparer est de mettre en œuvre une stratégie et un processus solides de protection des données qui **incluera le chiffrement** afin d'être encore plus efficace.

Si le règlement n'impose pas la mise en place de mesures techniques spécifiques, il cite explicitement le chiffrement comme mesure technique appropriée. A cet égard, il est utile d'observer la manière dont les entreprises se mettent en conformité avec d'autres règlements ayant pour objectif de protéger les données personnelles. La norme PCI DSS (Payment Card Industry Data Security Standard), la loi HIPAA (Health Insurance Portability and Accountability Act) et la loi Sarbanes-Oxley (SOX) sont des exemples, parmi tant d'autres, de règlements exigeant des mesures de contrôle de la protection des données semblables à celles indiquées dans le nouveau Règlement général sur la protection des données de l'UE. Parce qu'il permet de rendre les données incompréhensibles, le chiffrement est largement reconnu comme étant le moyen le plus adéquat de satisfaire à ces exigences. En effet, en cas de perte ou de vol des données chiffrées, celles-ci ne pourront tout simplement pas être exploitées. Personne ne pourra accéder aux données. Ceci est au cœur même des lois et règlements sur la protection des données.

En un mot : préparez-vous au nouveau Règlement général sur la protection des données en commençant à prospecter les technologies de chiffrement.

Sophos SafeGuard vous aide à répondre au défi de la protection des données

L'adoption d'une technologie de chiffrement est en grande partie attribuable au besoin de respecter les obligations légales et réglementaires en vigueur. Toutefois, les entreprises adoptant le chiffrement sont souvent préoccupées par la technologie. Le chiffrement est généralement perçu comme une technologie très gourmande en matière de ressources informatiques qui entrave la productivité.

Les anciennes technologies de chiffrement ralentissent le temps de démarrage des ordinateurs provoquant la frustration des utilisateurs. D'autres ne sont tout simplement pas compatibles avec le matériel le plus récent ou bloquent les machines entraînant une plus grande mobilisation des ressources informatiques déjà surchargées de travail.

Sophos SafeGuard Encryption offre un chiffrement sans aucun compromis. Les nouveaux systèmes d'exploitations Windows et Mac intègrent des moteurs de chiffrement. SafeGuard utilise ces moteurs de chiffrement dès que possible afin de réduire l'impact sur l'utilisateur. Ce dernier bénéficie donc de la protection et de performances optimales.

Nous avons simplifié le chiffrement en protégeant toutes les machines sur toutes les plates-formes sans que cela affecte les utilisateurs et leur façon de travailler. SafeGuard suit les données pour les protéger où qu'elles

se trouvent. Que ce soit dans le Cloud, sur des périphériques amovibles, dans les fichiers réseau ou sur les appareils mobiles, SafeGuard va là où vont vos données.

La simplicité de notre solution de chiffrement signifie également que le service informatique peut la déployer et la gérer facilement. Les fonctions d'audit et de rapports participent aux efforts de mise en conformité. En effet, elles permettent au service informatique de prouver qu'un fichier, qu'un ordinateur ou qu'une clé USB était chiffré au moment de sa perte, de son vol ou de sa violation. Toutes ces fonctions ont pour objectif d'amener plus de sérénité aux entreprises risquant de lourdes amendes en cas de non-respect des lois sur la protection des données.

Sophos est le seul éditeur du marché à offrir à vos utilisateurs une puissante solution de chiffrement utilisable sur leurs ordinateurs, mobiles, dossiers partagés, supports amovibles et dans le Cloud que ce soit sur Windows ou Mac. Cette grande polyvalence est assurée par un seul agent et une seule console d'administration. Notre solution de chiffrement certifiée empêche toute fuite de données et facilite la mise en conformité en toute transparence. De plus, sa grande simplicité d'administration vous fera gagner du temps.

Conclusion

En raison du durcissement des programmes de surveillance gouvernementaux et de la surmédiatisation des violations de données, la demande d'une protection solide des données sensibles et personnelles se fait de plus en plus pressante. Pendant ce temps, on assiste à une perte de confiance des consommateurs envers les entreprises. Le Parlement européen, les autorités de contrôle sur la protection des données et les gouvernements ont tous la volonté de contribuer à protéger et à développer le marché des services en ligne en Europe. Pour atteindre cet objectif, la majorité des entreprises vont devoir mettre en œuvre des processus et mesures techniques qui garantiront la confidentialité des données des consommateurs.

Le chiffrement doit être inclus dans une telle solution car il permettra d'empêcher la lecture de données perdues ou volées à toute personne qui n'est pas autorisée. Sophos SafeGuard Encryption offre aux entreprises la protection dont elles ont besoin sans aucune répercussion sur la productivité de l'utilisateur ou sur les ressources informatiques.

Annexe

1. RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
   Journal officiel de l'Union européenne, 27 avril 2016

2. Q&R: Les nouvelles règles de l'UE sur la protection des sonnées placent les citoyens aux commandes.
   Parlement européen, 13 avril 2016

3. EU Data Protection Reform - What benefits for businesses in Europe?
   Commission européenne, janvier 2016

4. Page du site de la Commission européenne sur la réforme des règles sur la protection des données
   Commission européenne

Équipe commerciale France
Tél. : 01 34 34 80 00
E-mail : info@sophos.fr

2066.11.14DD.wpfr.simple