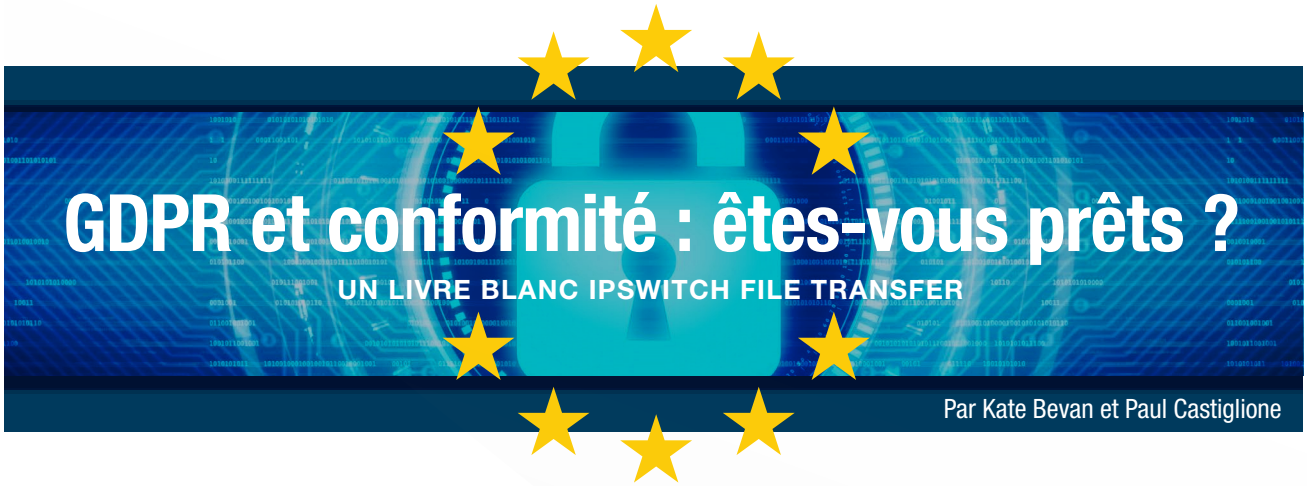
IPSWITCH
FILE TRANSFER



GDPR et conformité : êtes-vous prêts ?

UN LIVRE BLANC IPSWITCH FILE TRANSFER

Par Kate Bevan et Paul Castiglione

Contenu

« Votre priorité doit être l'adoption d'une approche ciblée sur l'identification des données sensibles. »

DAVID JUITT
membre de l'équipe Ipswitch responsable de la gouvernance, de la conformité et de la sécurité

La législation sur la protection des données au sein de la Communauté européenne est obsolète et mal adaptée à sa finalité. En outre, chaque État membre dispose de son propre régime de lois ce qui, à l'heure actuelle, entraîne des complications cauchemardesques en termes de mise en conformité pour les entreprises.

Lorsque les lois actuelles sur la protection des données ont été rédigées, la sécurité représentait un tout autre enjeu. En effet, les données des entreprises étaient conservées sur des serveurs internes et n'en quittaient que rarement leur périmètre. Les politiques de sécurité étaient donc ciblées sur la protection de ce périmètre.

Aujourd'hui la donne a radicalement changé : les volumes de données recueillis sont plus importants que jamais, et plutôt que d'être conservées au sein de limites physiques, les données sont stockées dans le cloud. Des documents, des formulaires et des bases de données sont distribués sur les serveurs et au-delà de leurs frontières.

De nouvelles technologies ne cessent de faire leur apparition : jusqu'à récemment, la consommation de masse était le défi n° 1 des responsables informatiques ; en effet, les utilisateurs choisissaient leurs propres téléphones mobiles et ordinateurs portables, ce qui obligeait les équipes informatiques à gérer une multitude de terminaux sécurisés et à faire face aux risques associés. Aujourd'hui les technologies portables / ordinateurs vestimentaires connaissent un essor rapide, ce qui implique la nécessité de protéger de nouvelles masses de données. Parallèlement, le développement de l'Internet des Objets s'accompagne d'une foule de périphériques qui communiquent avec des serveurs en back-end, générant toujours plus de données.

« Votre priorité doit être l'adoption d'une approche ciblée sur l'identification des données sensibles. » déclare David Juitt, membre de l'équipe Ipswitch responsable de la gouvernance, de la conformité et de la sécurité.

Suivre de près des technologies en constante évolution est un défi ; garder la maîtrise des problèmes de réglementation et de conformité en est un autre pour les professionnels de l'informatique.

Une évolution fondamentale se dessine : la création d'un nouveau cadre de protection des données qui s'appliquera à l'ensemble de l'Union européenne. L'objectif est de mettre en place une réglementation harmonisée en adéquation avec un paysage informatique, des données et une politique de conformité en mutation rapide.

Pourtant, même si les nouvelles règles qui sont proposées seront probablement appliquées d'ici deux ans à peine, les professionnels restent désarmés face au changement qui s'annonce, ce qui rend la situation préoccupante.

Selon deux tiers des professionnels de l'informatique, suivre de près les règles sur la protection des données constitue un fardeau pour les entreprises ; plus inquiétant encore, presque un cinquième des professionnels ne se doutent absolument pas qu'ils seront concernés par les futurs changements.

En quoi consiste exactement le projet de règlement général relatif à la protection des données ? Quelles seront les principales transformations ? Quels sont les principaux obstacles ? Et comment les entreprises doivent-elles se préparer à la mise en place de la nouvelle réglementation ?

Qu'est-ce que le GDPR ?

Le règlement général relatif à la protection des données de l'union européenne (le GDPR en est l'acronyme anglais) est destiné à remplacer l'ensemble disparate des autorités de protection des données de chacun des 28 États membres par un régime qui s'appliquera à l'ensemble de ces pays.

Ce règlement s'appliquera également aux entreprises non européennes qui traitent les données de citoyens européens au sein de l'Union. Concrètement, cela veut dire que les plus grands groupes dans le secteur du cloud et des réseaux sociaux tels que Google, Facebook, Twitter, Microsoft ou Apple devront se conformer à cette réglementation.

IPSWITCH
FILE TRANSFER

Le premier projet de règlement a été publié par la Commission européenne en 2012. Depuis cette date, les propositions ont été examinées dans le cadre du processus législatif et ont été finalement adoptées par le Conseil des ministres au mois de juin. Désormais, la prochaine étape des négociations peut donc être consacrée à la résolution de certaines des divergences qui sont apparues entre le Parlement européen et le Conseil des ministres. Il y a lieu d'espérer qu'un accord final sera conclu d'ici la fin de cette année.

Un tel accord inaugurerait ainsi la période de deux ans précédant l'entrée en vigueur du GDPR, ce qui signifie que le règlement devrait, en théorie, s'appliquer aux 28 États membres fin 2017.

Quelles sont les principales dispositions du GDPR ?

Consentement

Toute entreprise devra obtenir le consentement univoque des clients, de son personnel et des fournisseurs concernant l'utilisation de leurs données, ce qui constitue un changement radical par rapport à la situation actuelle.

Ce consentement s'applique à la fois aux données recueillies après la mise en œuvre du nouveau règlement et aussi, ce qui est capital, aux données déjà en sa possession.

DIFFICULTÉ : L'ensemble des données existantes devront être soumises à un audit afin de s'assurer qu'elles sont conformes à la nouvelle norme. Ainsi, toute personne dont votre organisation détient des données devra être contactée pour validation de son consentement. En outre, le Commissariat à l'information devra pouvoir accéder à ces consentements sur simple demande. En d'autres termes, cette disposition nécessitera d'immenses efforts en matière d'audit et de mise en conformité.

Communications

Le projet actuel de réglementation exige que toute organisation ayant subi une violation de sa sécurité en informe l'autorité de protection des données ainsi que toute personne impactée par une violation dans les 72 heures suivant l'incident.

DIFFICULTÉ : L'exemple de la violation dont a été victime la société Ashley Madison donne à réfléchir sur l'impact potentiel de cette exigence : Au mois de juillet, des pirates ont déclaré avoir volé la base de données des clients d'un site Web qui facilite les relations extra-conjugales. En août, les pirates ont diffusé sur Internet cette base qui contenait des informations sur quelques 30 millions d'utilisateurs. Même si Ashley Madison est une société américaine, nombreux de ses utilisateurs sont des citoyens de l'Union européenne et, à ce titre, Ashley Madison aurait été tenue, aux termes du GDPR, de notifier cette violation à l'autorité de protection des données et les utilisateurs dans les 72 heures qui ont suivi sa découverte.

Sanctions

Bonne nouvelle pour les entreprises sur ce point : la première proposition, qui consistait à instaurer des sanctions pouvant aller jusqu'à 5 % du chiffre d'affaires global, ou atteindre un montant de 100 millions d'euros, a été retoquée. Aujourd'hui, la proposition consiste en des sanctions atteignant au maximum 1 ou 2 millions d'euros du chiffre d'affaires global, selon la gravité de la faille de sécurité.

DIFFICULTÉ : Sous le régime actuel du Royaume-Uni par exemple, les amendes ne peuvent pas dépasser 500 000 livres sterling, ce qui peut sembler peu pour les entreprises affichant des chiffres d'affaires de plusieurs millions ou même milliards de livres ou d'euros. Le groupe anglais Carphone Warehouse, qui en août dernier a été victime d'un vol d'informations concernant 90 000 cartes de crédit, ne se verra peut-être pas infliger des sanctions de ce niveau. En revanche, l'amende de 200 000 livres qui a frappé en 2014 le Service britannique d'informations pour les femmes enceintes après le vol d'informations concernant des milliers d'utilisateurs par un pirate informatique a eu des conséquences financières très lourdes.

En France, les vols d'informations les plus conséquents de 2015 sont bel et bien les 2 suivants: en Janvier, 1.9 million de détails des comptes clients d'un site partenaire de la chaine TF1 furent dérobés par le groupe de hacker Linker Squad – puis en Avril, les 11 chaines et sites web de la chaine TV5 Monde furent attaqués et revendiqués par des hackers se disant membres de l'Etat Islamique.

Une des principales conclusions du Commissaire adjoint et du Directeur de la protection des données britanniques était que le Service britannique d'informations pour les femmes enceintes ne connaissait pas la nature des informations qu'il détenait, et qu'il ne savait pas non plus que ces données étaient mal protégées.

Les entreprises affectées par le GDPR devront prendre des mesures en amont de sa mise en œuvre pour s'assurer qu'elles appréhendent bien les informations qu'elles détiennent, ce qui nécessite un énorme travail d'audit et de mise en conformité.

69 % des sondés déclarent avoir besoin d'investir dans les nouvelles technologies ou les nouveaux services.

Droit à l'oubli

Les entreprises manipulant des données de citoyens de l'Union européenne devront supprimer sans tarder les données de citoyens qui en font la demande, ainsi que les données traitées de manière illégale ou si la loi le leur impose. Certaines réserves à ce principe existent néanmoins : la liberté d'expression et d'information, l'intérêt public ou l'archivage à des fins scientifiques et historiques peuvent l'emporter sur le droit à l'oubli.

DIFFICULTÉ : Avec de tels volumes de données conservés dans le cloud et circulant à travers l'entreprise, ainsi que sur les réseaux des partenaires et des clients, il devient beaucoup plus difficile pour les organisations de mettre en place des systèmes qui leur permettront d'identifier et de supprimer des informations personnellement identifiables sur demande. Les entreprises devront appliquer des processus permettant de répondre aux demandes liées au droit à l'oubli en temps opportun.

Les entreprises sont-elles prêtes pour la mise en place de ce règlement ?

La réponse est : pas vraiment. Selon un sondage Ipswitch portant sur plus de 300 professionnels de l'informatique basés au Royaume-Uni, en France et en Allemagne, 56 % des personnes interrogées étaient incapables de définir précisément ce que recouvrait le sigle GDPR, et 52 % ont répondu ne pas être prêts. Par ailleurs, 64 % des personnes interrogées ont reconnu ne pas connaître la date d'entrée en vigueur de ce règlement, alors que 35 % déclaraient ne pas savoir si leurs règles et processus informatiques existants étaient conformes aux nouvelles réglementations. Seules 12 % des personnes interrogées ont répondu qu'elles étaient prêtes pour le changement.

Au Royaume-Uni, la situation est encore plus préoccupante : seulement 5 % des professionnels de l'informatique déclarent être prêts pour la mise en place du GDPR.

La bonne nouvelle, c'est qu'il reste du temps pour s'y préparer : une période de deux ans doit s'écouler entre la ratification du GDPR et son entrée en vigueur. La meilleure estimation possible pour cette date se situe vers fin 2017.

Que doivent faire les entreprises pour s'assurer qu'elles sont en conformité avec le GDPR ?

En amont de la mise en œuvre du GDPR, les entreprises doivent se concentrer sur deux lignes directrices : la technologie et la formation. Ainsi, 69 % des sondés déclarent avoir besoin d'investir dans les nouvelles technologies ou les nouveaux services.

Les entreprises reconnaissent avoir besoin d'investir dans certaines technologies majeures : le chiffrement, l'analyse et le reporting, la protection du périmètre de sécurité, le partage de fichiers et la gestion des terminaux mobiles. Il est à noter que le chiffrement est mentionné le plus fréquemment (62 % des personnes interrogées).

La formation est l'autre orientation décisive : dans ce domaine, les entreprises ont davantage conscience de la nécessité de se préparer ; 50 % des sondés ont révélé en effet avoir alloué un budget et des ressources à la formation, afin d'aider leurs collaborateurs à comprendre les enjeux du GDPR et à s'y conformer. À l'inverse, environ un tiers des entreprises interrogées n'ont toujours pas alloué de budget ou de ressources et, plus inquiétant, presque un cinquième d'entre elles ne savaient pas si elles disposaient de suffisamment d'argent et de ressources pour la formation.

L'exemple doit venir d'en haut

Préparer l'échéance du GDPR constitue une priorité pour les entreprises de l'Union européenne, et l'immense impact des futurs changements implique que l'impulsion pour les initiatives en matière d'audit et de préparation, de développement de nouveaux processus et de mise en conformité doit venir de la hiérarchie. En effet, cette responsabilité incombe aux équipes dirigeantes et exige un solide sens du leadership, afin que les nouvelles règles et les nouveaux processus puissent être appliqués efficacement.

Toute entreprise qui prépare cette échéance doit toutefois commencer par développer une stratégie clé liée à la gestion des risques.

Le GDPR va impacter de nombreux secteurs au sein de chaque entreprise qui traite des données, de la protection des informations au transfert de fichiers.

Que doivent faire les professionnels de l'informatique ?

Même en parcourant rapidement certaines des principales mesures du GDPR, on se rend vite compte que le spectre des nouvelles règles est très large, et qu'il n'existe pas de feuille de route unique pour les entreprises qui doivent se préparer à la mise en place du GDPR.

Toute entreprise qui prépare cette échéance doit toutefois commencer par développer une stratégie clé liée à la gestion des risques. L'équipe dirigeante doit prescrire un processus de gestion des risques dont l'objectif est d'identifier tous les processus et actifs critiques et d'évaluer l'ensemble des vulnérabilités et menaces potentielles associées. Il fixe les priorités dans le cadre de la prochaine étape de la procédure dédiée à la mise en place du GDPR.

À l'époque de l'entrée en vigueur de la loi actuelle sur la protection des données au Royaume-Uni, le cloud et les transferts transfrontaliers d'actifs numériques et de données existaient à peine ; la politique de sécurité reposait sur la création d'un périmètre sécurisé destiné à protéger les infrastructures informatiques des entreprises sur site.

La technologie a considérablement évolué depuis ; aujourd'hui, un des principaux défis des directeurs techniques et des professionnels de la sécurité informatique consiste à trouver des moyens pour protéger les données conservées dans le cloud, distribuées sur les serveurs et au-delà des frontières de leur entreprise, et régulièrement déplacées d'un site à l'autre. Parmi les actifs particulièrement sensibles circulant régulièrement sur Internet, citons : les données personnelles, les documents stratégiques, les secrets commerciaux, les appels d'offre et les actifs consacrés à la recherche confidentiels ainsi que, bien sûr, les données financières.

Une évaluation des risques doit porter sur les méthodes utilisées pour chiffrer et sauvegarder les données, ainsi que sur la protection et le chiffrement de ces sauvegardes. La vulnérabilité face aux logiciels malveillants, les erreurs humaines potentielles et la dépendance excessive vis-à-vis des membres clés du personnel sont d'autres éléments à prendre en compte lors de l'examen du profil de risque d'une entreprise.

L'évaluation des risques couvre tous les domaines de l'activité et doit tenir compte également des technologies et des stratégies visant à minimiser les risques identifiés. La gestion du transfert de fichiers, qui permet de gérer le processus dans son intégralité au sein et au-delà des limites de l'entreprise, est une technologie clé en termes de limitation des risques et de garantie de la conformité.

Conclusion

Les violations de la sécurité sont courantes et préjudiciables : depuis un an ou deux, des incidents retentissants ont affecté des groupes aussi divers que eBay, Sony Picture, Carphone Warehouse et Ashley Madison. Des incidents de ce type, marqués notamment par le vol de données personnelles et de documents internes sensibles, devraient occuper les esprits non seulement des professionnels de l'informatique, mais aussi des directeurs de l'information, des directeurs des technologies et de tous les membres des équipes dirigeantes. Il y a des enseignements à tirer des erreurs que font les autres.

> « L'utilisation de la solution de transfert de fichiers Ipswitch MOVEit nous a permis d'atteindre un niveau de confiance qui jusqu'à présent nous faisait défaut. »
>
> ANDREW GLENCROSS
> *spécialiste chevronné de la sécurité informatique chez NHS Wales*

« Lorsque je vois dans l'actualité les noms d'entreprise victimes de piratage, je me garde de pratiquer l'autosatisfaction. Certes, ce n'était pas nous cette fois-ci, mais nous pourrions être concernés la prochaine fois. Ces atteintes majeures à la sécurité m'incitent à réexaminer nos propres processus et à renforcer l'évaluation des risques auxquels nous sommes confrontés. » commente David Juitt, membre de l'équipe Ipswitch responsable de la gouvernance, de la conformité et de la sécurité.

Même si le langage et les processus de l'Union européenne et de sa législature peuvent sembler durs et opaques, le temps presse donc pour les entreprises de tous les États membres. Au cours des deux prochaines années, il est essentiel que les organisations apprennent vraiment à connaître leurs environnements de données, à mettre en lumière les points qui méritent attention et à identifier les fournisseurs de technologies et de services qui leur permettront d'être prêts le jour J.

En quoi consiste la gestion du transfert de fichiers ?

Pour chaque entreprise, le transfert de fichiers et de données est un processus clé. Il s'agit d'une technologie « middleware » qui rationalise les transferts et les processus de gestion, renforce l'infrastructure informatique, gère et optimise la mise en conformité, améliore la réactivité et aide les entreprises à répondre rapidement aux défis et opportunités qui se présentent. La gestion du transfert de fichiers est un outil essentiel pour limiter les risques. Que les environnements soient administrés de manière empirique, sans politique de sécurité, avec des transferts de fichiers effectués manuellement qui risquent d'être interceptés, mal distribués ou de ne pas aboutir, ou qu'ils soient déjà dotés de règles et de procédures, la gestion du transfert de fichiers permet d'alléger la tâche des employés ainsi que d'améliorer la sécurité et la conformité au sein de l'entreprise.

Une solution complète de transfert de fichiers géré ne sécurise pas seulement les actifs de l'entreprise ; elle apporte également une plus-value en fournissant des outils qui aident les utilisateurs à gérer les pièces jointes et à travailler dans les répertoires locaux. Ce type de solution rationalise également les processus en automatisant les workflows, en gérant la performance et la sécurité, et en fournissant des outils de reporting et d'analyse, de sorte que l'entreprise garde toujours la maîtrise des données et des documents qui circulent au sein et en dehors de ses limites.

Andrew Glencross, spécialiste chevronné de la sécurité informatique chez NHS Wales et responsable de la sécurité des opérations en lien avec les applications et l'infrastructure nationales couvrant tous les sites du groupe, apporte son témoignage : « L'utilisation de la solution de transfert de fichiers Ipswitch MOVEit nous a permis d'atteindre un niveau de confiance qui jusqu'à présent nous faisait défaut. Désormais, nous pouvons affirmer que nous disposons d'une solution fiable qui répond aux besoins denos équipes en interne et garantit la conformité au sein du service et au-delà. »