RGPD :

Guide d'action pour les DSI

Édition 2017 – Révisée & mise à jour

Nigel Hawthorn

skyhigh

RGPD : Guide d'action pour les DSI.

Skyhigh Networks, Londres et Californie

Juin 2017

Préface par Alain Bensoussan, avocat à la Cour d'appel de Paris, Lexing Alain Bensoussan Avocats

Traduit de l'anglais par Marilyne Barzun, Lexing Alain Bensoussan Avocats

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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)

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

Imprimé et relié au Royaume-Uni.

Sommaire

Préface d'Alain Bensoussan

A moins d'un an de l'entrée en vigueur du règlement général sur la protection des données fixée le 25 mai 2018, il est urgent pour les entreprises privées et les organismes publics d'anticiper le nouveau cadre juridique de la protection des données personnelles.

En corollaire de la suppression des formalités déclaratives préalables auprès de la Cnil des traitements de données personnelles ne présentant pas de risque particulier pour les droits et libertés des personnes physiques, les responsables de traitement et les sous-traitants devront être en mesure de démontrer que les traitements qu'ils mettent en œuvre sont conformes au règlement (principe d'accountability). Compte tenu du nouveau régime de responsabilité et de réparation, ainsi que de l'aggravation du montant des sanctions administratives pécuniaires que pourra prononcer la Cnil (20 millions d'euros ou 4% du chiffre d'affaires mondial consolidé), chaque entreprise ou organisme doit définir son plan d'action de mise en conformité au règlement.

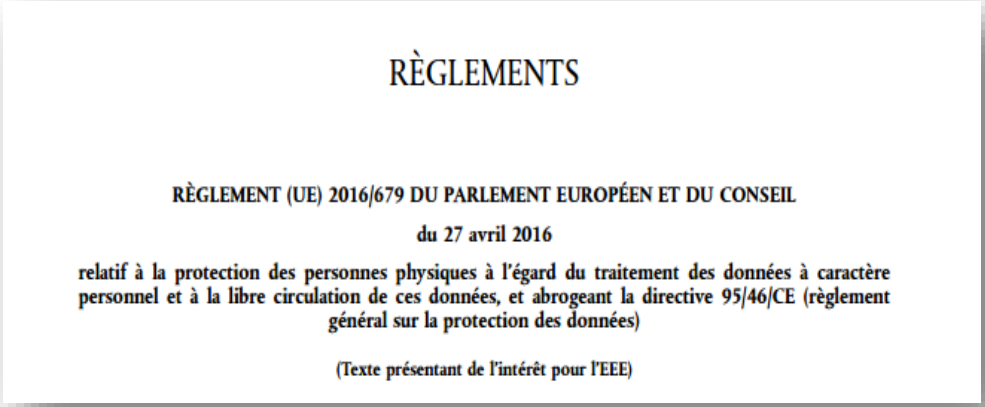
La direction des systèmes d'information aura un rôle essentiel dans le pilotage de cette mise en conformité puisqu'elle dispose des compétences techniques et des outils propres à assurer le respect des dispositions du règlement relatives à la sécurité des traitements de données personnelles. Notamment, lors du développement ou de l'acquisition d'applications informatiques, elle devra s'assurer, depuis les premières lignes de spécification générale et jusqu'à la dernière ligne du dossier de maintenance, que ces applications sont sécurisées dès la conception et par défaut.

Le présent guide et sa FAQ ont vocation à accompagner la direction des systèmes d'information en examinant les nouvelles obligations mises à la charge des responsables de traitement et des sous-traitants afin de permettre leur respect effectif au sein de l'entreprise. Par ailleurs, ce guide présente la nouvelle fonction de délégué à la protection des données (DPO) qui aura notamment un rôle central de conseil et de sensibilisation sur les nouvelles obligations.

Sans remplacer les conseils de professionnels du droit, ce guide expose de façon opérationnelle les dispositions du règlement afin d'appréhender les étapes de la route de la mise en conformité à franchir pour être prêt en mai 2018.

Introduction

Le règlement général sur la protection des données (ci-après le « règlement » ou le « RGPD ») entrera en vigueur dans les Etats membres de l'Union européenne (UE) et de l'Espace économique européen (EEE) le 25 mai 2018. Il s'agit d'une modification majeure de la réglementation européenne en matière de protection des données personnelles, qui augmentera notamment de manière significative le montant des amendes infligées en cas de non-respect des obligations mises à la charge des responsables de traitement et des sous-traitants. Le présent guide a pour but de vous expliquer ce nouveau texte et de vous indiquer les étapes à suivre pour assurer la conformité de votre entreprise au RGPD.



RÈGLEMENTS

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

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)

(Texte présentant de l'intérêt pour l'EEE)

Le RGPD peut être considéré comme une loi générale sur la protection des données personnelles, car il concerne toute organisation possédant des données sur les personnes situées dans l'UE/l'EEE.

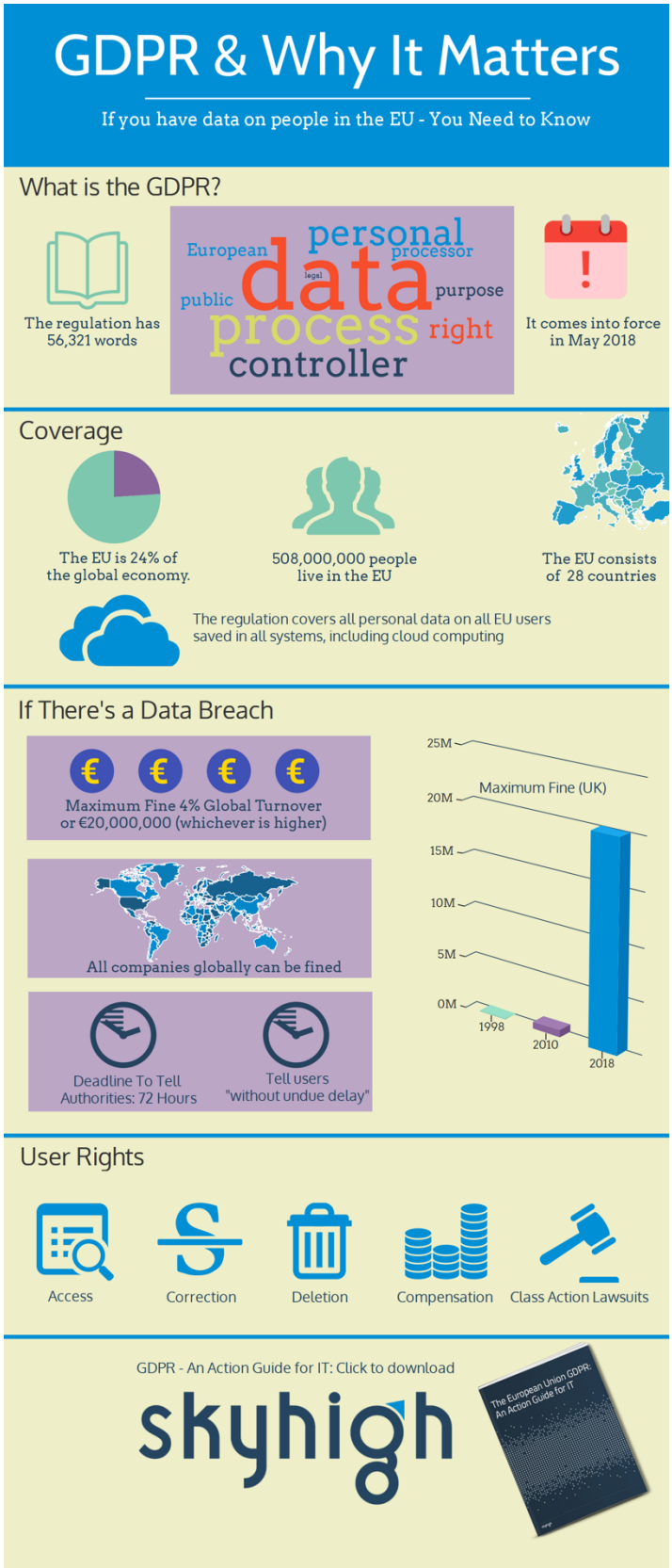
Ce guide s'adresse plus particulièrement aux membres de la direction des systèmes d'information (DSI). Il est conçu comme un guide pratique à l'usage des équipes informatiques afin de les aider à auditer les données et méthodes de traitement des données actuelles appliquées et à mettre en place les politiques, les procédures et les mesures techniques appropriées pour se conformer au RGPD. Nous attirons votre attention sur le fait que ce document ne constitue pas un conseil juridique, et il vous est par conséquent recommandé de vous adresser à des avocats spécialisés en matière de protection des données afin d'obtenir tous les éclairages dont vous pourriez avoir besoin. Il contient des extraits du texte du règlement, qui ne remplacent en aucun cas le texte intégral (qui compte près de 200 pages), et auquel il vous est conseillé de vous reporter. Enfin, il n'a pas vocation à être exhaustif et n'aborde que certains aspects majeurs du règlement ; ce guide ne couvre pas, par exemple, les données relatives aux enfants, les données dites « sensibles » (race, religion et orientation sexuelle, etc.), les données sur les infractions pénales ou les exemptions applicables aux traitements à des fins de recherche scientifique ou historique.

Le texte complet du règlement est disponible à l'adresse :

http://eur-lex.europa.eu/eli/reg/2016/679/oj

INFOGRAPHIE : LE RGPD : Présentation et enjeux

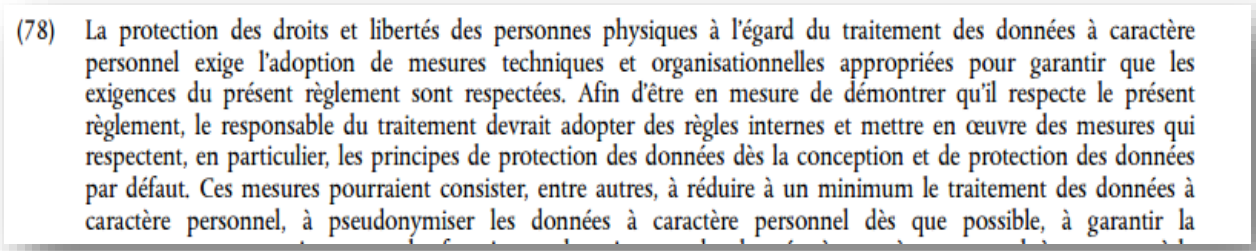
Cette infographie est également disponible en ligne à l'adresse :
https://www.skyhighnetworks.com/eu-gdpr-infographic/



Présentation générale du règlement

Le règlement, dont le processus d'élaboration a débuté en 2012, constitue une mise à jour importante de la directive européenne sur la protection des données datant de 1995. Le RGPD poursuit plusieurs objectifs. Il vise à :

- harmoniser la législation existante dans les vingt-huit Etats membres de l'UE ;
- clarifier les points interprétés jusqu'alors de manière divergente dans les différents pays ;
- élargir son champ d'application afin d'y inclure toute personne physique ou morale qui collecte des données sur les citoyens de l'UE ;
- assurer une application cohérente et homogène des règles de protection des données dans l'ensemble des pays de l'UE.



(78) La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel exige l'adoption de mesures techniques et organisationnelles appropriées pour garantir que les exigences du présent règlement sont respectées. Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la

Toute entreprise qui collecte des données (le « responsable du traitement ») ou qui stocke et traite des données (le « sous-traitant ») relatives à des personnes physiques qui se trouvent sur le territoire de l'UE ou de l'EEE est tenue de respecter ce règlement. A cet effet, elle doit veiller à se doter de politiques et de technologies appropriées lui permettant de garantir sa conformité au RGPD.

POINTS CLÉS DU RÈGLEMENT

Parmi les nombreux domaines couverts par le règlement, voici les dix points clés auxquels il convient de prêter une attention particulière :

- **Augmentation des amendes.** Les amendes peuvent atteindre jusqu'à 4% du chiffre d'affaires mondial consolidé ou 20 millions d'euros, le montant le plus élevé étant retenu.
- **Consentement préalable (dit « opt-in »).** Les utilisateurs doivent donner, de manière claire et univoque, leur accord au responsable du traitement pour qu'il puisse collecter et utiliser les données les concernant, et les responsables de traitement et sous-traitants ne doivent les utiliser que pour des finalités déterminées.
- **Notification des violations de données.** En cas de violation de données, l'autorité de contrôle locale doit être notifiée dans les 72 heures (cf. « Missions et pouvoirs des autorités de contrôle »), et les personnes concernées doivent être informés « dans les meilleurs délais ».
- **Champ d'application territorial.** Toute organisation possédant des données relatives aux citoyens de l'UE, qu'elle soit établie dans l'UE ou non, est tenue de respecter le règlement.
- **Coresponsabilité.** Le responsable du traitement et le sous-traitant peuvent être coresponsables en cas de violation de données.
- **Droit à l'effacement.** Les utilisateurs ont le droit d'exiger l'effacement de leurs données.
- **Suppression de la fragmentation juridique**. Il n'existe plus qu'une seule loi applicable en matière de protection des données pour l'ensemble des pays membres de l'UE.
- **Transfert de données.** Le transfert de données en dehors de l'UE est possible, mais le responsable du traitement assume la responsabilité si les données sont perdues par son fournisseur de cloud en dehors de l'UE.
- **Application cohérente.** Les autorités chargées de surveiller le respect du règlement doivent veiller à garantir son application cohérente dans l'ensemble des pays de l'UE.
- **Recours collectif.** Les utilisateurs peuvent se regrouper en vue d'introduire un recours collectif.

DATES CLÉS

1995	Publication de la directive européenne de protection des données (directive 95/46/CE) qui réglemente la collecte, le traitement et la libre circulation des données des personnes au sein de l'UE.
Depuis 1995	Depuis 1995, chaque pays de l'UE a transposé la directive sur la protection des données dans son droit interne, avec de légères variations. Chaque pays a mis en place sa propre autorité de contrôle chargée de conseiller les entreprises sur les règles applicables, d'enquêter sur les violations ainsi que, le cas échéant, d'infliger des amendes et des sanctions. Par exemple, la France a modifié la loi Informatique et libertés de 1978 qui a instauré la Cnil, tandis qu'au Royaume-Uni l'autorité de contrôle compétente est l'ICO.
Janvier 2012	Publication de propositions en matière de protection de données en vue de l'adoption d'un règlement destiné à remplacer la directive (contrairement aux directives, les règlements sont directement applicables dans tous les Etats membres, sans besoin d'être transposés dans le droit interne de chaque Etat membre).
Juin 2015	Adoption d'une orientation générale concernant le RGPD par le Conseil de l'UE
Décembre 2015	Adoption du RGPD par la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen http://europa.eu/rapid/press-release_IP-15-6321_fr.htm
Avril 2016	Adoption du texte final par le Parlement européen et le Conseil
25 mai 2018	Entrée en vigueur du RGPD

Le compte à rebours a commencé. Il n'y a pas de temps à perdre pour se mettre en conformité !

QUAND VA-T-IL ENTRER EN APPLICATION ?

Même si le RGPD n'est pas applicable immédiatement, certains pays ont choisi de l'anticiper et d'introduire d'ores et déjà des lois équivalentes au RGPD dans leur propre législation. À titre d'exemple, la France a adopté le 7 octobre 2016 la loi dite pour une République numérique qui contient des mesures anticipant le RGPD ; elle prévoit notamment une augmentation du montant de l'amende encourue à trois millions d'euros. Une fois le règlement entré en vigueur, la loi prévoit que ce seront les sanctions européennes qui s'appliqueront.

Pays de l'UE et de l'EEE

Le RGPD est applicable dans tous les pays de l'UE. L'UE est composée des 28 pays suivants, regroupant une population totale de plus de 500 millions de personnes : Allemagne, Autriche, Belgique, Bulgarie, Croatie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République Tchèque, Roumanie, Slovaquie, Slovénie, Suède, Royaume-Uni.

En outre, des pays qui ne sont pas dans l'UE, mais qui sont membres de l'EEE, adopteront également des lois similaires au RGPD : il s'agit de l'Islande, du Liechtenstein et de la Norvège.

Pays hors UE

Certains pays hors de l'UE qui sont dotés de lois similaires à la directive de 1995, se sont engagés à adopter des lois équivalentes au RGPD. Ces lois et le présent guide pourront utilement être consultés afin de connaitre le régime applicable aux données des citoyens hors UE en ce qui concerne leurs données. Par ailleurs, l'UE a reconnu certains pays tiers comme assurant un niveau « adéquat » de protection des données, en 2017 figurent parmi ces pays : l'Andorre, l'Argentine, le Canada (organisations commerciales), les Îles Féroé, Guernesey, Israël, l'Ile de Man, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay. Les lois sur la protection des données changent assez fréquemment. Des informations actualisées sur les lois de la plupart des pays du monde sont disponibles sur le site Web de DLA Piper.

QUI EST CONCERNÉ ?

Le règlement concerne toute organisation (privée ou publique) dans le monde entier dès lors qu'elle collecte, stocke ou traite des données relatives à des personnes qui se trouvent sur le territoire de l'UE. Le RGPD étend ainsi le champ d'application de la directive de 1995 qui visait uniquement les responsables de traitement et les organisations établis dans l'UE. En outre, le sous-traitant est désormais coresponsable avec le responsable du traitement, ce qui signifie que si votre entreprise collecte des données sur des personnes, et confie ensuite le traitement de ces données à une autre entité, votre entreprise sera tenue coresponsable avec cette entité de tout ce qui arrive à ces données.

QUEL IMPACT POUR LE RESPONSABLE DU TRAITEMENT HORS UE ?

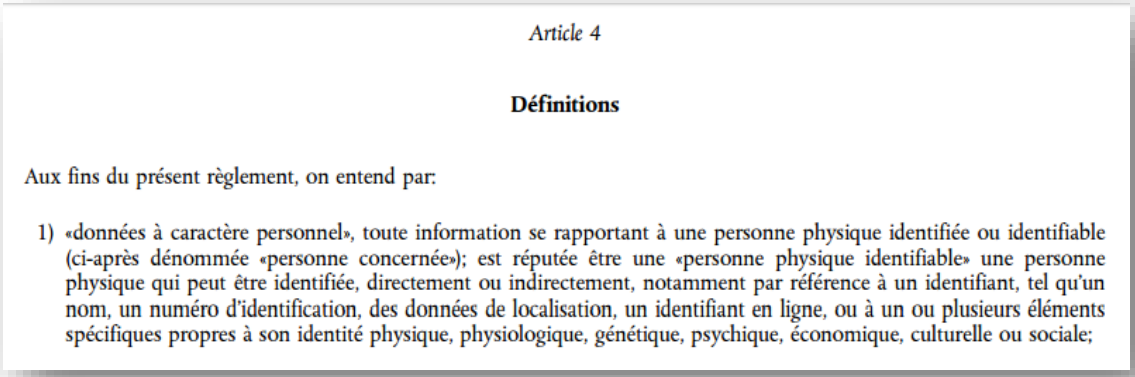
Si, par le passé, certains responsables de traitement établis en dehors de l'UE avaient pu soutenir qu'ils n'étaient pas soumis à la directive de 1995 sur la protection des données, cette argument ne sera dorénavant plus recevable : le règlement précise clairement qu'il s'applique au traitement des données à caractère personnel relatives à des personnes qui se trouvent sur le territoire de l'UE par toute organisation, quel que soit son lieu d'établissement.

Autrement dit, une autorité de protection des données d'un des pays de l'UE a compétence pour sanctionner des entreprises dont le siège est établi en dehors de l'UE. C'est ainsi que dans l'affaire Weltimmo, la Cour de justice de l'Union européenne a jugé qu'une société dont le siège était situé en Slovaquie pouvait se voir infliger une amende par l'autorité de protection des données de Hongrie. En l'espèce, constatant que cette société slovaque employait au moins un salarié en Hongrie et offrait un service aux clients hongrois via son site web, le juge communautaire a considéré qu'elle pouvait être sanctionnée pour violation de la loi hongroise sur la protection des données.

(80) Lorsqu'un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union traite des données à caractère personnel de personnes concernées qui se trouvent dans l'Union et que ses activités de traitement sont liées à l'offre de biens ou de services à ces personnes dans l'Union, qu'un paiement leur soit demandé ou non, ou au suivi de leur comportement, dans la mesure où celui-ci a lieu au sein de l'Union, il convient que le responsable du traitement ou le sous-traitant désigne un représentant, à moins que le traitement soit occasionnel, n'implique pas un traitement, à grande échelle, de catégories particulières de données à caractère personnel ou le traitement

QU'EST-CE QU'UNE DONNÉE A CARACTÈRE PERSONNEL ?

Le RGPD a été rédigé de façon à ne pas préciser de manière exhaustive les éléments pouvant constituer des données à caractère personnel, afin de s'assurer que le règlement ne devienne pas obsolète au fur et à mesure de l'apparition de nouvelles techniques d'identification des personnes. D'une manière générale, toute donnée qui identifie une personne est considérée comme une donnée à caractère personnel.



Article 4

Définitions

Aux fins du présent règlement, on entend par:

1) «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

Concrètement, un nom, une adresse, une date de naissance, une adresse électronique personnelle ou professionnelle, un numéro de téléphone sont des données à caractère personnel. Sont également considérées comme des données à caractère personnel les identifiants en ligne fournis par les appareils et applications informatiques comme les adresses IP, les cookies, ainsi que d'autres identifiants, tels que les étiquettes RFID, si ces éléments peuvent être utilisés, seuls ou avec d'autres données, afin d'identifier une personne.

En effet, même si des données ne semblent pas, de prime abord, identifier une personne spécifique, elles peuvent néanmoins, en les combinant avec une ou plusieurs autres données, permettre son identification. Ces données seront alors considérées comme des données à caractère personnel couvertes par le RGPD. Aujourd'hui, à l'ère du Big data, où les « data cruncher » permettent aux entreprises de recueillir des données provenant de sources multiples, il est prudent de considérer tout identifiant unique comme une donnée à caractère personnel.

QU'EST-CE QU'UNE DONNÉE SENSIBLE ?

Les données sensibles sont soumises à un régime spécial, non détaillé dans le présent guide. Ces données désignent notamment les données qui révèlent l'origine ethnique, l'appartenance syndicale, les convictions religieuses ou philosophiques, ou qui concerne la santé et la vie sexuelle.

L'UTILISATEUR EST AUX COMMANDES

Une personne concernée a le droit d'obtenir l'accès aux données la concernant, la rectification des données qui sont inexactes ou leur effacement, et, si ces données n'ont pas été collectées auprès d'elle, toute information quant à leur source, ainsi que la durée de leur conservation (ou à défaut la politique de conservation appliquée). Une personne concernée a également le droit d'introduire une réclamation auprès d'une autorité de contrôle si elle considère qu'un responsable du traitement ne respecte pas le règlement, et l'autorité doit alors procéder à une enquête.

Les personnes concernées ont de surcroît un droit à la portabilité des données : elles ont le droit de transmettre les données les concernant à un autre responsable du traitement et à cette fin les recevoir dans un format lisible par machine.

Enfin, le règlement offre un nouveau droit d'action aux personnes concernées : si une autorité de contrôle ne traite pas une réclamation qui lui a été adressée par une personne concernée, cette dernière peut former un recours à l'encontre de cette autorité afin de la forcer à le faire. Lorsqu'une personne concernée formule une demande d'exercice des droits qui lui sont conférés, et énumérés ci-dessous, auprès d'un responsable du traitement, le responsable du traitement est tenu d'y répondre « dans les meilleurs délais » et au plus tard dans un délai d'un mois.

DROIT D'ACCÈS

Les personnes concernées ont le droit de demander au responsable du traitement quelles données à caractère personnel les concernant il a collecté, et le responsable du traitement a l'obligation de leur répondre. De cette manière, la personne concernée est en mesure de confirmer si ces données sont correctes et de choisir, le cas échéant, de les confier à un autre responsable du traitement. Imaginez par exemple un client qui, après plusieurs années, décide de changer de banque : il lui sera bien utile que sa banque actuelle transmette l'ensemble des informations recueillies au fil des ans relativement à toutes les transactions le concernant à son nouvel établissement bancaire.

(63) Une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité. Cela inclut le droit des personnes concernées d'accéder aux données

DROIT DE RECTIFICATION ET DROIT A L'EFFACEMENT

La personne concernée a le droit d'obtenir du responsable du traitement la rectification des données à caractère personnel la concernant qu'elle considère inexactes.

(65) Les personnes concernées devraient avoir le droit de faire rectifier des données à caractère personnel les concernant, et disposer d'un «droit à l'oubli» lorsque la conservation de ces données constitue une violation du présent règlement ou du droit de l'Union ou du droit d'un État membre auquel le responsable du traitement est soumis. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données à caractère personnel soient effacées et ne soient plus traitées, lorsque ces données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de

En outre, elle a le droit d'obtenir du responsable du traitement qu'il efface ses données et arrête leur traitement.

Les responsables du traitement sont donc tenus de disposer d'un processus qui leur permette de modifier et de supprimer les données qu'ils traitent. L'opération de suppression peut être complexe, surtout lorsque les sources de données sont multiples.

DONNÉES COLLECTÉES A DES FINS DE PROSPECTION COMMERCIALE

Le RGPD contient une clause traitant spécifiquement de la collecte de données à des fins de prospection commerciale.

Lorsque les données à caractère personnel sont destinées à être collectées pour cette finalité, la personne concernée a le droit de s'opposer non seulement à la collecte de ces données, mais également à leur profilage par des agences de marketing direct.

(70) Lorsque des données à caractère personnel sont traitées à des fins de prospection, la personne concernée devrait avoir le droit, à tout moment et sans frais, de s'opposer à ce traitement, y compris le profilage dans la mesure où il est lié à une telle prospection, qu'il s'agisse d'un traitement initial ou ultérieur. Ce droit devrait être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information.

Conscient que les agences de marketing direct utilisent des techniques de profilage de plus en plus sophistiquées afin d'améliorer leur ciblage, le législateur européen choisi de faire expressément référence à la prospection dans le texte du règlement. Il est également important de noter que le droit de s'opposer au traitement à des fins de prospection doit être porté à l'attention de la personne concernée séparément de toute autre information, en veillant à ce qu'elle puisse donner son accord à l'utilisation d'une ou plusieurs de ses données à des fins de prospection commerciale, séparément de leur utilisation pour toute autre finalité.

RÉPARATION

Toute personne ayant subi un dommage du fait d'une violation de données a le droit d'obtenir réparation du préjudice subi. Le RGPD ne limite pas cette réparation aux seuls dommages matériels, et peuvent également être indemnisés d'autres types de dommages, tels que la perte de temps, l'atteinte à la réputation ou la détresse émotionnelle (par exemple, l'affaire Vidal-Hall c/ Google Inc. au Royaume-Uni).

Article 82

Droit à réparation et responsabilité

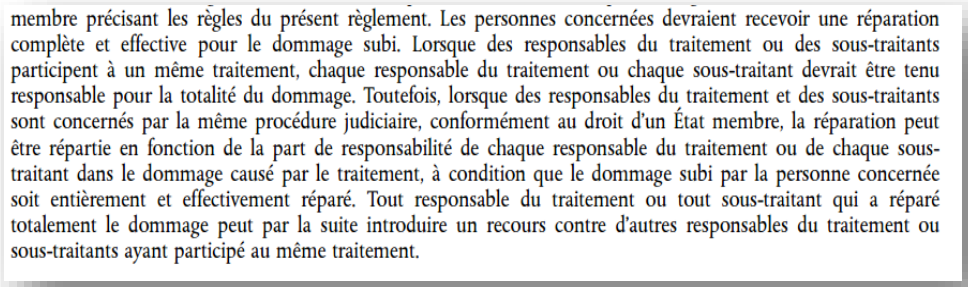
1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Lorsqu'un responsable du traitement a recours à un sous-traitant, ils sont tous deux conjointement responsables de réparer le dommage subi par la victime de la violation de données. Par ailleurs, si l'un d'entre eux répare totalement le dommage subi, il est en droit d'engager une action judicaire à l'encontre de l'autre pour lui réclamer la part de la réparation correspondant à sa part de responsabilité dans le dommage. Ces nouvelles dispositions changent la règle du jeu qui prédominait jusqu'alors, et il sera intéressant d'en suivre les conséquences sur les relations contractuelles entre les fournisseurs de cloud computing et leurs clients.

Les fournisseurs de cloud computing vont probablement chercher à intégrer une clause visant à faire assumer par leur client l'intégralité de la responsabilité en cas de pertes de données et des éventuelles amendes prononcées, ou encore exiger de connaitre les mesures de sécurité prises par le client.

RECOURS COLLECTIFS - ACTIONS DE GROUPE

Les responsables de traitement et les sous-traitants doivent porter une attention particulière aux recours collectifs, ou actions de groupe, (également connues sous le terme de « class actions ») susceptibles d'être intentés par les personnes concernées devant les tribunaux européens, et dont le nombre risque d'augmenter. Si le règlement ne contient aucune clause concernant ces recours collectifs, plusieurs recours de ce type ont néanmoins déjà été portés devant la justice européenne (par exemple, Google c/ Vidal-Hall c/Google Inc. au Royaume-Uni ; Max Schrems c/Facebook Inc. en Autriche).



membre précisant les règles du présent règlement. Les personnes concernées devraient recevoir une réparation complète et effective pour le dommage subi. Lorsque des responsables du traitement ou des sous-traitants participent à un même traitement, chaque responsable du traitement ou chaque sous-traitant devrait être tenu responsable pour la totalité du dommage. Toutefois, lorsque des responsables du traitement et des sous-traitants sont concernés par la même procédure judiciaire, conformément au droit d'un État membre, la réparation peut être répartie en fonction de la part de responsabilité de chaque responsable du traitement ou de chaque sous-traitant dans le dommage causé par le traitement, à condition que le dommage subi par la personne concernée soit entièrement et effectivement réparé. Tout responsable du traitement ou tout sous-traitant qui a réparé totalement le dommage peut par la suite introduire un recours contre d'autres responsables du traitement ou sous-traitants ayant participé au même traitement.

Il sera intéressant de suivre comment évoluera la jurisprudence sur cette question. Qu'en serait-il par exemple de cette situation : une PME européenne, ne comptant que quelques salariés, décide de lancer un service de cloud computing en s'appuyant sur les services d'un fournisseur multinational de services de stockage dans le cloud. La PME collecte un million de coordonnées relatives à ses utilisateurs et les enregistre en ligne dans le cloud. A la suite d'une faille de sécurité, les noms et mots de passe des utilisateurs sont diffusés publiquement. L'un des utilisateurs victime entame un recours collectif à l'encontre de la PME et du fournisseur du cloud. Imaginons ensuite que la PME soit déclarée en cessation de paiement, le recours collectif pourrait-il néanmoins continuer et, dans l'affirmative, le fournisseur de cloud devra-t-il alors assumer l'entière responsabilité pour les condamnations éventuellement prononcées ?

RENFORCER LA CONFIANCE DES UTILISATEURS

Le règlement contient un paragraphe encourageant la mise en place d'organismes et de mécanismes de certification permettant aux responsables de traitement de démontrer le respect de leurs obligations en matière de protection des données.

(100) Afin de favoriser la transparence et le respect du présent règlement, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.

Ces organismes et mécanismes de certification vont probablement se mettre en place prochainement. Ils devraient offrir des garanties en termes de protection des données suffisamment fortes pour donner aux personnes concernées la confiance de partager leurs données avec les organisations bénéficiant de cette certification.

MISSIONS ET POUVOIRS DES AUTORITÉS DE CONTRÔLE

Chaque pays dispose de son propre régulateur de données (désigné sous le terme d' « autorité de contrôle » par le règlement). Il s'agit par exemple de l'ICO au Royaume-Uni et de la Cnil en France. L'Allemagne, qui est un Etat fédéral, possède plusieurs autorités de contrôle, une dans chaque Etat fédéré. Les délégués à la protection des données (cf. section « Délégué à la protection des données ») doivent s'enregistrer auprès de leur régulateur local.

Les autorités de contrôle ont pour mission d'appliquer le règlement, d'informer et de conseiller les entreprises et, le cas échéant, d'imposer des amendes.

de l'Etat membre dans lequel le responsable du traitement a son établissement principal devrait rester l'autorité de contrôle chef de file compétente, mais l'autorité de contrôle du sous-traitant devrait être considérée comme étant une autorité de contrôle concernée et cette autorité de contrôle devrait participer à la procédure de coopération prévue par le présent règlement. En tout état de cause, les autorités de contrôle du ou des États membres dans lesquels le sous-traitant a un ou plusieurs établissements ne devraient pas être considérées comme étant des autorités de contrôle concernées lorsque le projet de décision ne concerne que le responsable du traitement.

Si chaque pays européen dispose déjà de ces autorités prévues par la directive de 1995, leurs dispositions ont été interprétées différemment selon les pays. En effet, certains pays ont choisi d'appliquer la directive à la lettre et de manière stricte, en donnant à leur autorité le pouvoir d'infliger des amendes relativement importantes et de rendre publiques les sanctions prononcées, tandis que dans d'autres pays les régulateurs endossent davantage le rôle d'accompagnateur, privilégiant la diffusion d'informations au public et de conseils aux responsables de traitement. C'est pour cette raison, notamment, que la sensibilisation et les préoccupations en matière de protection des données peuvent varier considérablement d'un pays européen à l'autre.

Article 83

Conditions générales pour imposer des amendes administratives

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

De nombreux articles du règlement (articles 51 à 67) sont consacrés aux autorités de contrôle et à leur relation avec le Comité européen de la protection des données. Ces articles définissent l'indépendance, les règles de fonctionnement, les missions et les pouvoirs des autorités de contrôle, le but étant de favoriser la coopération entre les pays et d'assurer l'application cohérente du règlement. Ces articles devraient inciter les pays qui avaient jusqu'à présent adopté une approche flexible dans la transposition modérée de la directive à appliquer le règlement de manière plus rigoureuse. On s'attend par conséquent dans ces pays à assister à une augmentation du nombre des amendes prononcées et de l'exécution de décisions de justice.

Il convient de noter que les Etats membres ont la possibilité de déterminer des sanctions pénales en cas de violations du règlement.

(149) Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du présent règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces

AMENDES INFLIGÉES PAR LES AUTORITÉS DE CONTRÔLE

La directive de 1995 sur la protection des données laisse aux Etats membres l'entière décision quant aux sanctions à appliquer en cas de violations de ses dispositions. Il s'en est suivi des disparités assez importantes sur les amendes prononcées dans chaque pays. En outre, le montant des amendes infligées a évolué au fil du temps. Par exemple, l'amende maximale pouvant être prononcée par la Cnil est passé de 200.000 francs à 150.000 euros, et désormais 3 millions d'euros. En pratique, le montant moyen de l'amende effectivement prononcée en cas de violation de données a progressivement augmenté, atteignant en janvier 2014 le chiffre record de 150.000 euros. Aux termes du règlement, les amendes imposées doivent être « effectives, proportionnées et dissuasives ». Les amendes énoncées par le législateur européen sont à cet égard particulièrement sévères.

En cas de violation des principaux articles du règlement, une entreprise encourt en effet l'amende maximale prévue par le RGPD, à savoir soit 20 millions d'euros ou 4% de son chiffre d'affaires mondial consolidé, le montant le plus élevé étant retenu.

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:

Dans ses considérants, le règlement rappelle que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental (...) toute personne a droit à la protection des données à caractère personnel la concernant ».

Le montant des amendes prévues ne laisse aucun doute quant au fait que la protection des données est prise très au sérieux par l'UE, et que toute personne responsable de la perte ou de l'utilisation abusive de données relatives à des personnes qui se trouvent sur le territoire de l'Union s'expose à de très lourdes sanctions.

RGPD vs DIRECTIVE

Le RGPD étant une mise à jour de la directive de 1995 sur la protection des données, il est intéressant de comparer ces deux textes. Les principales évolutions constatées sont décrites ci-dessous.

Les données appartiennent à l'utilisateur, et non pas à l'entreprise (responsable du traitement, sous-traitant)

Il faut d'emblée préciser que les données appartiennent à la personne concernée, et non au responsable du traitement. Ce principe entraine plusieurs conséquences.

Les personnes concernées ont le droit de demander au responsable du traitement de leur restituer les données les concernant, sous forme électronique, afin qu'elles puissent les transmettre à un autre responsable du traitement (un exemple concret pour bien comprendre : imaginez que vous décidez de changer de banque, vous avez le droit de demander à votre banque actuelle de transférer toutes les données concernant vos transactions à votre nouvelle banque).

Les personnes concernées ont également le droit d'obtenir du responsable du traitement la mise à jour des données les concernant si celles-ci sont incorrectes, ou leur effacement (ce qui peut poser problème lorsque le responsable du traitement est par ailleurs tenu par la loi de conserver ces données pendant une certaine période, même si ce type de situations pourra certainement être résolu).

En outre, elles ont le droit d'obtenir du responsable du traitement, de manière claire, précise et univoque, la confirmation que des données à caractère personnel les concernant soient ou non traitées, ainsi que sur les finalités et les modalités de ce traitement.

Enfin, les personnes concernées ont le droit de s'opposer au transfert de leurs données en dehors de l'UE, de l'EEE ou des pays « adéquats », et ce séparément au recueil de leur consentement lors de la collecte initiale de leurs données.

Les équipes marketing doivent réexaminer et actualiser leurs politiques de collecte et de traitement des données

Les utilisateurs doivent être informés au préalable que le sous-traitant souhaite collecter leurs données, et donner leur accord pour cette collecte. Ces informations relatives à la collecte ne doivent pas être cachées ou noyées au sein d'un autre texte. Il est par ailleurs interdit d'utiliser des cases précochées, qui obligeraient l'utilisateur à les désactiver afin de s'opposer à la collecte de ses données. Enfin, les mots utilisés pour obtenir le consentement doivent être clairs et dénués d'ambiguïté.

Le cas échéant, les responsables de traitement devront insérer plusieurs cases à cocher, en fonction de l'utilisation prévue des données. Par exemple une première case pour collecter les données, une deuxième pour les utiliser à des fins spécifiques, une troisième pour autoriser le transfert des données en dehors de l'UE et enfin une quatrième destinée à autoriser la réception de communications marketing.

En outre, il doit être aussi simple de retirer que de donner son consentement.

Les responsables de traitement devraient également diffuser publiquement leur politique de protection des données.

Les services d'une entreprise ne peuvent pas être restreints en fonction des données autorisées à être collectées. Ainsi une personne qui choisit de ne pas partager ses données à caractère personnel doit quand même avoir accès aux services de votre entreprise pour le fonctionnement desquels la collecte des données n'est pas indispensable – concrètement, cela pourrait signifier permettre aux internautes de télécharger des éléments sans partager leurs coordonnées avec le responsable du traitement.

Par ailleurs, les données ne doivent être conservées que pour la durée du service, et doivent ensuite être supprimées.

En cas de violation, les sanctions sont plus lourdes

En cas de non-respect du règlement, les amendes peuvent s'élever jusqu'à 4% du chiffre d'affaires mondial consolidé ou 20 millions d'euros, le montant le plus élevé étant retenu.

Tous les acteurs de la chaîne de données (responsables de traitement et sous-traitants) sont conjointement responsables de la protection des données. Le responsable du traitement est donc tenu de connaître tous les sous-traitants, tous les systèmes et tous les services cloud utilisés au sein de son entreprise et de veiller à ce que chacun comprenne ses obligations et ses responsabilités : dans le cas où un sous-traitant perdrait des données, le responsable du traitement sera conjointement responsable avec le sous-traitant.

Le RGPD décrit de manière détaillée le rôle des autorités de protection des données dans le but d'harmoniser l'application du texte dans tous les Etats membres de l'UE, ce qui n'est actuellement pas le cas.

Les personnes concernées ont le droit de former un recours contre une autorité de protection des données si elles considèrent que cette autorité n'applique pas correctement le RGPD – cette mesure est destinée à s'assurer que les autorités enquêtent bien sur les violations du règlement.

En cas de violation de données à caractère personnel, le responsable du traitement doit notifier la violation en question à l'autorité de contrôle compétente 72 heures au plus tard après en avoir pris connaissance (et, lorsque la notification n'a pas lieu dans les 72 heures, elle doit être accompagnée des motifs du retard). Posez-vous la question : vos systèmes sont-ils suffisamment performants pour vous permettre de respecter ce délai, 24 heures sur 24, 7 jours sur 7 ?

En outre, les personnes concernées doivent être informées de la violation de données à caractère personnel « dans les meilleurs délais ». Disposez-vous d'un plan de communication pour assurer cette information ?

Enfin, les personnes concernées peuvent intenter des recours collectifs devant les juridictions nationales.

Des dispositions plus claires et plus précises

Le RGPD indique clairement que lorsque la combinaison de plusieurs données permet d'identifier une personne, chacune de ces données sera considérée comme une donnée à caractère personnel au sens du RGPD.

Autre apport du texte : une multinationale peut choisir de n'avoir comme interlocuteur qu'une seule autorité de protection des données, et non vingt-huit !

Le RGPD insiste sur le fait que les documents diffusés doivent être clairs, que des politiques et procédures appropriées en matière de protection des données doivent être mises en œuvre, et que les salariés doivent bénéficier de formations : tous ces éléments seront en effet pris en compte par l'autorité de contrôle au moment où elle aura à se prononcer sur d'éventuelles sanctions.

Les technologies peuvent être une aide précieuse pour assurer la conformité au règlement – le RGPD énonce expressément que le chiffrement, sous diverses formes, permet de réduire l'obligation d'informer les personnes concernées.

Pour prouver la conformité au règlement, il conviendra de documenter les diverses actions et mesures prises (politiques et procédures et mise en application, formation dispensée aux collaborateurs) – le RGPD indique clairement que, lorsqu'elle conduit une enquête sur une réclamation introduite auprès d'elle, l'autorité de contrôle examine les politiques, les procédures et les technologies utilisées pour assurer la sécurité des données, afin de fixer les amendes en conséquence. Les autorités de certains pays suivent d'ailleurs déjà cette approche.

Champ d'application territorial et commercial

Le champ d'application est international – toute personne physique ou morale ayant des données sur les personnes qui se trouvent sur le territoire des pays membres de l'UE/l'EEE est concernée.

Coresponsabilité – Le responsable du traitement et l'ensemble de ses sous-traitants, fournisseurs de services cloud, etc., sont conjointement responsables. Cette coresponsabilité peut avoir une conséquence imprévue, en ce sens que les sous-traitants, dans l'optique de réduire leurs risques, pourront exiger de connaître les procédures appliquées par le responsable du traitement avant d'accepter les missions qu'il souhaite lui confier.

Guide d'action pour le RGPD

La protection des données n'est pas seulement la responsabilité du service informatique, il s'agit d'un sujet qui doit être pris au sérieux au plus haut niveau de l'entreprise. Il doit faire l'objet d'une action coordonnée par l'ensemble des services de l'entreprise, du service juridique au service RH, en passant par les services conformité, comptabilité, et marketing, chacun devant travailler main dans la main avec le service informatique.

Cela étant, le service informatique reste bien entendu un des acteurs majeurs. Il ressort clairement de l'article 32 du RGPD que plusieurs tâches incombent directement aux DSI.

Article 32

Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre 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 œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris 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.

PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT

Ce serait une erreur de considérer que votre entreprise puisse assurer sa conformité au RGPD simplement en ajoutant quelques éléments à ses politiques et procédures actuelles en matière de traitement des données. En effet, avec le RGPD, tous les nouveaux systèmes de collecte et de traitement des données de l'entreprise doivent être conçus de manière à prendre en compte les meilleures pratiques en matière de minimisation et de pseudonymisation des données. Les principes de protection des données dès la conception et par défaut consacrés par le règlement imposent en effet de prendre en compte ces considérations dès le départ. Il convient donc d'intégrer des mesures pour assurer la sécurité et la protection des données, et de ne collecter que les données nécessaires au regard de la finalité poursuivie.

Article 25

Protection des données dès la conception et protection des données par défaut

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre 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, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

POUR LES DONNÉES DÉJÀ COLLECTÉES

Lorsque le règlement entrera en vigueur, il couvrira non seulement toutes les données collectées après son application, mais également toutes celles que l'entreprise a déjà en sa possession. La première action à prendre consiste donc à obtenir une cartographie de vos traitements en dressant un inventaire de toutes les données détenues actuellement par votre entreprise sur des personnes physiques, afin de connaitre les éléments essentiels, tels que le lieu de stockage, les éventuels flux transfrontières existants, le recours à des sous-traitants, l'utilisation des services cloud, les politiques de sécurité, la formation dispensées aux salariés en matière de protection des données et les technologies déployées pour garantir la sécurité des données. Une fois ces éléments recensés, rédigez un rapport sur les données en votre possession.

Aucune des dispositions du RGPD ne précise que les personnes concernées dont vous possédez déjà les données doivent être contactées pour donner un nouveau consentement (en supposant que ce consentement ait bien été donné initialement). Toutefois, des dispositions du RGPD imposant au responsable du traitement de pouvoir démontrer de quelle manière et à quel moment le consentement des personnes concernées a été obtenu, l'entreprise doit nécessairement vérifier l'historique de la collecte des données afin de s'assurer qu'elle est bien conforme aux dispositions du règlement.

(171) La directive 95/46/CE devrait être abrogée par le présent règlement. Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées.

La société doit pouvoir identifier tous les endroits où les données personnelles sont stockées. A cette fin, il sera probablement nécessaire d'interroger chaque salarié qui participe à la collecte des données personnelles et de rechercher tous les systèmes de CRM, de support et de marketing, y compris bien entendu les services cloud. Dans les grandes sociétés, il est courant que de multiples systèmes de collecte soient en place, certains peuvent être mutualisés, certains peuvent être autonomes. La société se doit de connaître et de tracer tous les systèmes existants.

POUR LES NOUVELLES DONNÉES A COLLECTER

Avant de collecter des données, vous devez informer l'utilisateur de la finalité de la collecte, et ne collecter des données qu'à cette fin. Les utilisateurs doivent expressément donner leur accord à cette collecte.

en ce qui concerne ce traitement. En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel. Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique. Il y a lieu de prendre toutes les mesures raisonnables afin de garantir que les données à caractère personnel qui sont inexactes sont rectifiées ou supprimées. Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement.

Ces informations doivent être partagées avec le service marketing, qui est susceptible de recueillir des données, notamment en vue d'identifier de nouveaux prospects. Leurs processus doivent également être audités.

L'utilisateur doit recevoir des informations claires, et donner son consentement par un acte positif clair. Il n'est pas possible d'utiliser des cases précochées afin de recueillir le consentement de l'utilisateur. En outre, les informations sur la collecte des données doivent être claires et concises – elles ne doivent être ni obscures ni noyées au sein de longues conditions générales ou d'autres documents.

Les responsables de traitement doivent utiliser les données exclusivement pour la finalité pour laquelle elles ont été collectées, et informer la personne concernée de la finalité ainsi poursuivie. Une fois collectées, il est interdit d'utiliser les données pour d'autres finalités. Les traitements distincts nécessitent un consentement distinct.

(32) Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé.

Selon le règlement, l'utilisateur doit se voir offrir une véritable liberté de choix qui « ne doit pas être perturbée ». En d'autres termes, vous ne devez pas restreindre l'accès des utilisateurs à un service en ne l'offrant qu'à ceux qui ont consenti à la collecte de leurs données.

(50) Le traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement. Dans ce cas, aucune base

Les données ne doivent être conservées que pendant la durée nécessaire, et l'autorité de contrôle peut demander au responsable du traitement de lui communiquer ses politiques de conservation des données.

Le responsable du traitement doit pouvoir démontrer qu'il a obtenu le consentement de la personne concernée – Et vous, seriez-vous en mesure de répondre à la question : « Où avez-vous obtenu ces données ? ».

Article 7

Conditions applicables au consentement

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

Le règlement va encore plus loin en disposant que les entreprises ne doivent pas subordonner la fourniture d'un de leurs services à une personne concernée au consentement de la collecte de ses données. Cette disposition va sans aucun doute plonger les professionnels du marketing dans la confusion - cela signifie-t-il par exemple qu'un document dont l'accès est conditionné à la fourniture par l'utilisateur de ses coordonnées doit être rendu librement accessible sans que personne ne donne ses coordonnées ?

TRAITEMENT DES DONNÉES

Si le responsable du traitement ne donne pas aux personnes concernées les informations auxquelles elles ont droit et ne leur offre pas le choix de consentir à la collecte des données les concernant, alors le consentement sera réputé ne pas avoir été donné.

4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

De plus, les personnes concernées ont le droit de retirer leur consentement à tout moment. Cela signifie qu'un responsable du traitement doit leur fournir la possibilité de retirer leur consentement, et avoir en place une procédure lui permettant de retirer leurs données de toutes ses sources de données. Ce système peut être compliqué à mettre en œuvre, spécialement si une entreprise possède plusieurs sources de données qui synchronisent automatiquement les données entre elles.

2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.

3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

RÉDUCTION DES RISQUES

Le service informatique, et en particulier l'équipe en charge de la sécurité informatique, doit procéder à un audit des technologies utilisées pour sécuriser les données.

Si l'accent est souvent mis sur la perte de données, le règlement fait également référence à la destruction et à la modification des données. Vous serez donc tout autant exposé à un risque de non-conformité dans le cas où votre système de gestion des données tombe en panne et entraîne, de manière accidentelle, soit la perte, soit la suppression, soit l'altération de vos données.

(83) Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.

Les mesures prises ne doivent pas être uniquement techniques. Votre entreprise devra également mettre en place des politiques de gestion des données, et former ses salariés afin que chacun d'entre eux, susceptible de manipuler des données, connaisse les bonnes pratiques à appliquer et adopte les bons réflexes en matière de protection des données.

N'oubliez pas que plus le nombre de données perdues est important, plus le montant des amendes infligées et les coûts des procès qui peuvent s'en suivre seront élevés. Il faut réfléchir aux différentes possibilités offertes par les technologies qui pourraient vous aider à limiter la quantité de données disponible pour chaque utilisateur ou système simultanément, afin de réduire le plus possible le risque de perte de données.

LE CHIFFREMENT – LA SOLUTION MIRACLE ?

Le règlement désigne expressément la technique du chiffrement comme un moyen d'atténuer les risques pesant sur les données. Le chiffrement peut ainsi contribuer à réduire les risques associés aux violations de données. Il serait opportun d'examiner en détail vos fichiers afin d'identifier les données qui pourrait faire l'objet d'un chiffrement et, au contraire, celles pour lesquelles cette mesure ne serait pas nécessaire, car toutes les données n'ont évidemment pas le même niveau de sensibilité.

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 œuvre 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;

UTILISATION DE SOUS-TRAITANTS

Un sous-traitant est une personne morale ou physique (non salariée) distincte du responsable du traitement qui traite des données pour le compte du responsable du traitement. Sont, par exemple, des sous-traitants une entreprise de sous-traitance, un fournisseur de services de stockage hors site, un fournisseur de services cloud, une agence de marketing chargée de mener un projet à court terme impliquant la gestion des données du responsable du traitement. S'agissant plus particulièrement des services cloud, cela inclut notamment des systèmes de collaboration en nuage où les salariés enregistrent des données sur les personnes concernées, ainsi que des applications cloud RH et les systèmes de CRM. L'existence d'une relation contractuelle entre le sous-traitant et le responsable du traitement n'est pas un critère indispensable, de sorte que dès lors qu'un salarié enregistre sur un service cloud des données personnelles concernant des personnes qui se trouvent dans l'UE, le prestataire de ce service cloud sera automatiquement considéré comme le sous-traitant de ces données.

Les responsables du traitement restent toujours responsables de la sécurité des données. Pour autant, ils doivent veiller à ne travailler qu'avec des sous-traitants conscients d'être soumis à des obligations et des responsabilités similaires à celles du responsable du traitement, et qui s'engagent à respecter les dispositions du RGPD.

Un sous-traitant n'est pas autorisé à externaliser le traitement à d'autres sous-traitants sans l'accord du responsable du traitement, et dans ce cas, les responsabilités contenues dans le règlement se répercuteraient en cascade à chaque sous-traitant de la chaîne de traitement.

Article 26

Responsables conjoints du traitement

1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

Le responsable du traitement est donc tenu de connaître chacun des sous-traitants intervenant à la demande de son entreprise ou de ses salariés, et d'évaluer les politiques et les technologies qu'ils utilisent afin de s'assurer qu'elles soient bien conformes au règlement. Le service informatique peut centraliser ces informations et les tenir à jour pour chaque nouveau sous-traitant. De nos jours, une entreprise utilise, en moyenne, plus de 1000 services cloud différents, chacun d'entre eux pouvant potentiellement être qualifiés de sous-traitant. Cette question mérite par conséquent un intérêt particulier.

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

TRANSFÉRER DES DONNÉES À L'EXTÉRIEUR DE L'UNION EUROPÉENNE

La question du transfert de données en dehors de l'UE a toujours fait couler beaucoup d'encre, que ce soit sous l'empire de la directive de 1995 ou, aujourd'hui, du RGPD. Il s'agit d'un sujet complexe, qui ne peut être traité qu'en des termes généraux dans le présent guide.

Tout d'abord, les transferts ne peuvent avoir lieu que s'ils sont « nécessaires ». On parle de transfert des données lorsque ces données quittent le territoire des vingt-huit Etats membres de l'UE, et ce de quelque manière que ce soit. Le transfert peut s'effectuer de diverses manières. Par exemple, les données seront considérées comme transférées même si elles sont échangées au sein de la même entreprise : c'est le cas lorsqu'un salarié d'une multinationale se trouvant dans un établissement situé dans l'UE envoie, par courrier électronique, un fichier client sous format Excel à un de ses collègues travaillant dans un établissement situé aux Etats-Unis. Autres exemples de transfert : les données sont externalisées à un sous-traitant en dehors de l'UE, les données sont enregistrées dans un service de fichiers partagés hébergé en dehors de l'UE, les données sont confiées à un prestataire de services de cloud computing établi en dehors de l'UE, et, pour finir, un cas souvent oublié : une entreprise exploite un site Web établi dans l'UE mais fait appel, pour la gestion des formulaires présents sur son site, à une agence de marketing externe établie, elle, en dehors de l'UE, ainsi dès qu'un internaute remplit le formulaire, ses données font donc l'objet d'un transfert en dehors de UE.

(61) Les informations sur le traitement des données à caractère personnel relatives à la personne concernée devraient lui être fournies au moment où ces données sont collectées auprès d'elle ou, si les données à caractère personnel sont obtenues d'une autre source, dans un délai raisonnable en fonction des circonstances propres à chaque cas. Lorsque des données à caractère personnel peuvent être légitimement communiquées à un autre destinataire, il convient que la personne concernée soit informée du moment auquel ces données à caractère personnel sont communiquées pour la première fois audit destinataire. Lorsqu'il a l'intention de traiter les données à caractère

Lorsqu'un responsable du traitement envisage de transférer des données en dehors de l'UE, il a l'obligation d'en informer la personne concernée. Qu'en est-il pour votre entreprise ? La politique de confidentialité des données publiée sur votre site Web informe-elle les visiteurs qu'un tel transfert est susceptible d'avoir lieu ? Permet-elle aux internautes de s'opposer à ce transfert ?

Les transferts en dehors de l'UE ne sont autorisés que si le pays destinataire assure un niveau de protection adéquat aux données transférées. A ce jour, ont été reconnus comme « adéquats » par la Commission européenne : l'Andorre, l'Argentine, le Canada (organisations commerciales), les Iles Féroé, Guernesey, Israël, Ile de Man, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay. En cas de transfert vers ces pays, il n'est pas nécessaire de conclure un contrat de transfert.

(103) La Commission peut décider, avec effet dans l'ensemble de l'Union, qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection des données, assurant ainsi une sécurité juridique et une uniformité dans l'ensemble l'Union en ce qui concerne le pays tiers ou l'organisation internationale qui est réputé offrir un tel niveau de protection. Dans ce cas, les transferts de données à caractère personnel vers ce pays tiers ou cette organisation internationale peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation. La Commission peut également décider, après en avoir informé le pays tiers ou l'organisation internationale et lui avoir fourni une justification complète, de révoquer une telle décision.

A défaut, tout transfert de données vers un pays en dehors de l'UE requiert la conclusion d'un contrat destiné à encadrer le transfert stipulant que le destinataire non européen s'engage à fournir certaines garanties quant à la protection des données. Afin d'aider les entreprises à élaborer ces contrats, la Commission européenne a publié des clauses contractuelles types que les entreprises peuvent utiliser, en fonction des circonstances du transfert envisagé. Les responsables de traitement doivent donc vérifier qu'ils ont bien conclu des contrats avec chacun de leurs fournisseurs de services cloud ou prestataires externes pour tout transfert de données en dehors de l'UE.

personne concernée. Le responsable du traitement et le sous-traitant peuvent choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence, puis par la Commission.

La responsabilité pour la protection des données se répercute en cascade sur toutes les personnes morales et physiques qui utilisent les données, de sorte que chaque transfert ultérieur devra automatiquement être soumis aux mêmes clauses contractuelles. Il est de la responsabilité des responsables de traitement de s'assurer que leurs fournisseurs de services cloud s'interdisent d'externaliser les traitements de données qui leur sont confiés sans imposer à leur propre sous-traitant les mêmes garanties auxquelles ils sont eux-mêmes soumis.

concerne la protection des données à caractère personnel. Cependant, il importe que, lorsque des données à caractère personnel sont transférées de l'Union à des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale. En tout état de cause, les transferts vers des pays tiers et à des organisations internationales ne peuvent avoir lieu que dans le plein respect du présent règlement. Un transfert ne pourrait avoir lieu que si, sous

Le bouclier de protection des données UE-Etats-Unis

Lorsqu'une entreprise souhaite transférer des données de l'UE vers les Etats-Unis, elle peut demander à l'entreprise américaine de signer des clauses contractuelles types ou d'adhérer au bouclier de protection des données UE-Etats-Unis, le « Privacy Shield » (qui remplace et améliore le système précédent de sphère de sécurité, dit « Safe Harbor », invalidé en octobre 2015).

Le Privacy Shield prévoit les garanties suivantes : les entreprises adhérentes sont soumises à des obligations fermes, assorties d'une mise à exécution rigoureuse, l'accès par les autorités américaines aux données est étroitement encadré, les citoyens de l'UE se voient offrir la possibilité de recours, et l'interdiction d'effectuer tout transfert ultérieur de données à des entreprises non adhérentes au dispositif.

Les entreprises américaines doivent renouveler leur adhésion au Privacy Shield tous les ans. Ce dispositif est géré et administré par le département américain du commerce et la Federal Trade Commission (Commission fédérale du commerce). Vous pouvez trouver la liste des entreprises ayant adhéré au Privacy Shield à l'adresse :

https://www.privacyshield.gov/list .

SUPPRESSION ET EFFACEMENT DES DONNÉES

Le règlement dispose que les données ne doivent être conservées que pendant la période nécessaire, et doivent ensuite être supprimées. En outre, les personnes concernées ont le droit d'obtenir l'effacement de leurs données. Le responsable du traitement doit donc disposer d'une procédure de suppression de données lui permettant de garantir que les données sont complètement supprimées de tous ses systèmes. Cela peut paraître simple en théorie, mais dans la pratique, il en va tout autrement. En effet, les données sont souvent partagées entre différents systèmes informatiques et s'assurer que les données sont bien supprimées de tous les systèmes simultanément, sans que le processus de synchronisation automatique entre les systèmes ne restaure les données supprimées, n'est pas tâche aisée.

VIOLATION DE DONNÉES

Quelle que soit la technologie et les procédures utilisées par le responsable du traitement, il peut arriver que certaines données soient perdues ou modifiées de manière incorrecte.

L'entreprise se doit de disposer d'un plan complet détaillant les actions à prendre lors de la survenance d'une violation de données. Ce plan devrait être élaboré par une équipe transverse, composée de membres des différents services ou départements de l'entreprise, et ne devrait probablement pas être piloté par le service informatique. Un volet majeur de ce plan est la gestion de la communication à l'extérieur de l'entreprise, et notamment quand et comment informer les autorités, les personnes concernées et (éventuellement) le grand public d'une violation de données.

(87) Il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement.

Le DSI doit être en mesure de fournir des détails sur la nature de la violation des données intervenue, le nombre de données concernées et les causes de la violation. L'équipe informatique doit pouvoir être capable de stopper toute violation de données en cours et de communiquer efficacement au reste de l'entreprise des informations complètes sur l'incident et ses conséquences probables. A cette fin, il lui faut se doter de la technologie nécessaire à l'identification des violations des données, qu'elle qu'en soit l'origine : piratage informatique, machines infectées par un virus, perte d'identifiants, partage de données sur des clouds non sécurisés, etc.

En cas de violation de données, le responsable du traitement a normalement 72 heures après en avoir pris connaissance pour en notifier l'autorité de contrôle, à moins que « la violation en question de soit pas susceptible d'engendrer un risque » (Cf. section sur le chiffrement). Le délai de notification est assez court, et il est indispensable de mettre en place au sein de l'entreprise un processus lui permettant d'analyser l'ampleur de la violation de données rapidement, afin de respecter des délais prescrits par le règlement.

Article 33

Notification à l'autorité de contrôle d'une violation de données à caractère personnel

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Article 34

Communication à la personne concernée d'une violation de données à caractère personnel

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.

Les personnes concernées doivent également être informées de la violation de données « dans les meilleurs délais ». Il y aura sans aucun doute de nombreux débats quant au sens exact de l'expression « dans les meilleurs délais », le responsable du traitement souhaitant naturellement disposer du plus de temps possible afin de réaliser les vérifications qui s'imposent et de rassembler les informations nécessaires. Quoi qu'il en soit, le règlement est clair : les violations des données ne doivent pas être dissimulées aux personnes concernées.

(88) Lors de la fixation de règles détaillées concernant la forme et les procédures applicables à la notification des violations de données à caractère personnel, il convient de tenir dûment compte des circonstances de cette violation, y compris du fait que les données à caractère personnel étaient ou non protégées par des mesures de protection techniques appropriées, limitant efficacement la probabilité d'usurpation d'identité ou d'autres formes d'abus. Par ailleurs, ces règles et procédures devraient tenir compte des intérêts légitimes des autorités répressives lorsqu'une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation des données à caractère personnel.

Aux termes du règlement, le type d'informations que vous aurez à communiquer aux personnes concernées en cas de violation de données varie en fonction des circonstances de la violation (ampleur de la violation, type des données concernées) et des mesures de protection prises par l'entreprise pour y remédier. Pour cette raison, le responsable du traitement doit anticiper les différents cas de figure et disposer en amont de plusieurs modèles de communication prêts à l'emploi. N'oubliez pas que toutes les données n'ont pas la même valeur, et que les données sensibles doivent être soumises à un contrôle plus strict. Par exemple, il est conseillé de ne pas divulguer les données relatives aux transactions financières aux salariés qui ont seulement besoin de connaître un sous-ensemble d'informations sur les clients.

(86) Le responsable du traitement devrait communiquer une violation de données à caractère personnel à la personne concernée dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent. La communication devrait décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Il convient que de telles communications aux personnes concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes, telles que les autorités répressives. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données à caractère personnel ou la survenance de violations similaires peut justifier un délai plus long pour la communication.

De l'utilité du chiffrement

Les technologies permettant de chiffrer les données avant qu'elles soient transférées à un sous-traitant ou à un service cloud (en particulier si les clés de cryptage sont conservées séparément des données elles-mêmes) peuvent réduire immédiatement les risques susceptibles d'être engendrés par une violation de données. En effet, en cas de violation de données, les éventuelles conséquences négatives seront beaucoup moins importantes car le destinataire ne pourra consulter les données sans procéder d'abord à leur déchiffrement, un processus qui peut prendre du temps pour les techniques de chiffrement les plus sécurisées.

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 œuvre 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;

Le règlement précise bien que la communication à la personne concernée n'est pas nécessaire si les données concernées par la violation sont « incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès ». L'utilité du chiffrement est claire et est un atout certain. Une analyse des différentes techniques de chiffrement s'impose, afin de choisir la bonne pour votre entreprise - Skyhigh a conçu un guide spécialement dédié au chiffrement dans le cloud qui décrit les différentes méthodes de chiffrement existantes et analyse les forces et faiblesses de chacune. Il existe des techniques de chiffrement qui peuvent laisser la possibilité aux utilisateurs d'effectuer des opérations de recherche et de tri, mais dans ce cas, chaque champ d'un système CRM pourra nécessiter différents types de chiffrement en fonction de la sensibilité des données et des actions que les utilisateurs doivent effectuer sur ces données.

TENIR DES REGISTRES

Le règlement impose au responsable du traitement de tenir un registre des activités de traitement effectuées. En cas d'enquête par une autorité de contrôle, celle-ci peut demander des détails sur les données enregistrées dans le système (origine et date de l'enregistrement, preuve du consentement de l'utilisateur à la collecte, finalités des données), ainsi que d'autres informations telles que la politique de conservation des données appliquée par le responsable du traitement, l'existence de transferts de données vers des tiers (et notamment les prestataires de services cloud) et les mesures, procédures et techniques mises en œuvre au sein de l'entreprise afin de garantir la sécurité des données.

Article 30

Registre des activités de traitement

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

Autre point important à souligner, qui n'a pas été mis en exergue précédemment : les amendes prononcées par les autorités de contrôle seront d'autant plus élevées que la tenue des registres sera considérée insuffisante. Le responsable du traitement doit, dès à présent, mettre en place un système pour documenter ses procédures, et ne pas oublier d'y inclure tous les sous-traitants qui travaillent sur ses données.

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

DÉMONTRER LA CONFORMITÉ

Le responsable de traitement doit être en mesure de démontrer qu'il respecte le règlement. Il doit notamment apporter la preuve qu'il a compris le règlement et mis en œuvre les politiques, les procédures et les mesures techniques nécessaires pour s'y conformer, qu'il a informé ses éventuels sous-traitants de leurs responsabilités, et qu'il a veillé à ne transférer des données qu'à des sous-traitants présentant les garanties appropriées. Il est probable que le montant des amendes imposées pour des violations du RGPD sera fixé en prenant en compte le dossier documentaire ainsi constitué par le responsable du traitement, comme cela est déjà le cas pour les amendes actuellement prononcées par les autorités de contrôle conformément à la directive de 1995.

(74) Il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe, en particulier, que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le présent règlement, y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques.

ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNÉES

Le règlement impose aux responsables du traitement d'effectuer des analyses d'impact lorsqu'un traitement « en particulier par le recours à de nouvelles technologies (…) est susceptible d'engendrer un risque élevé pour les (...) personnes physiques ».

Il sera intéressant de voir comment cette obligation sera mise en œuvre. L'expression « risque élevé » devra éventuellement être définie par la jurisprudence. En tout état de cause, il est recommandé de procéder à des analyses d'impact préalablement à l'introduction de toutes nouvelles technologies dans votre entreprise. S'agissant des services cloud, Skyhigh peut vous aider grâce à son registre d'attributs destinés aux fournisseurs de services cloud.

Article 35

Analyse d'impact relative à la protection des données

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

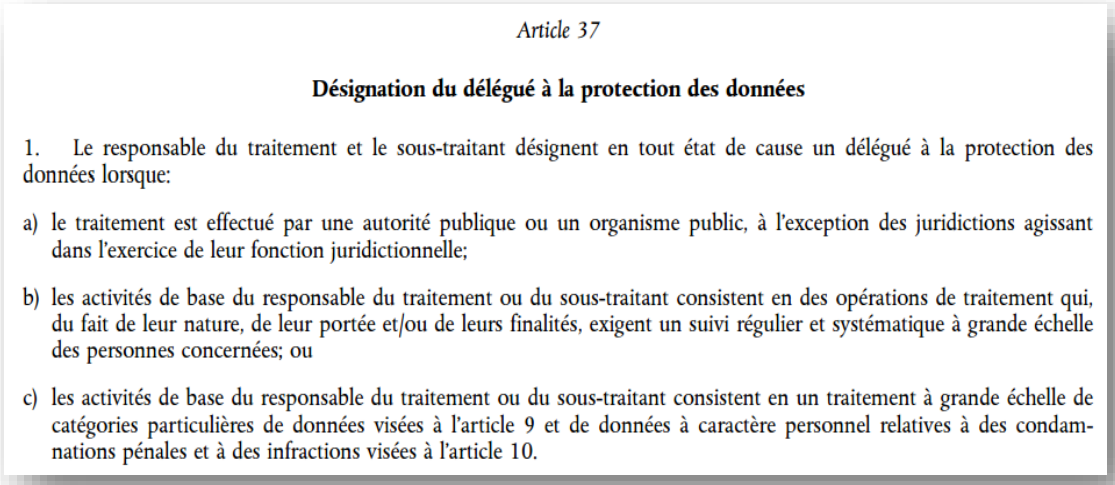
DÉLÉGUÉ A LA PROTECTION DES DONNÉES

Aujourd'hui, selon l'interprétation dominante de la directive sur la protection des données dans la plupart des Etats membres de l'UE, toutes les entreprises (à l'exception des PME) disposant de données sur des personnes physiques, sont tenues de désigner un délégué à la protection des données.

Le RGPD réduit cette obligation, et ne l'impose qu'aux seules organisations du secteur public, ou aux entreprises qui effectuent des opérations de traitement qui exigent un suivi « à grande échelle », des personnes concernées. Le règlement laisse toutefois, aux Etats membres une certaine marge de manœuvre quant à la question de la désignation d'un délégué à la protection des données, et il est fort probable que certaines autorités de contrôle nationales décident d'imposer aux entreprises de désigner un interlocuteur privilégié pour toutes les questions relatives à la protection des données.

Le rôle et les missions du délégué à la protection des données sont décrits en détail par les articles 38 et 39 du règlement.

PRÉCISIONS – PORTABILITÉ DES DONNÉES



Article 37

Désignation du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Par communiqué de presse daté du 13 décembre 2016, le Groupe de travail « article 29 » sur la protection des données de l'UE a diffusé plusieurs lignes directrices, accompagnées de FAQ, portant sur différentes thématiques liées à la mise en œuvre du RGPD, et notamment sur la portabilité des données. Début avril 2017, une version révisée de ces textes a été publiée.

Ces documents précisent que les responsables du traitement doivent offrir aux personnes concernées la possibilité de recevoir leurs données dans un format standard, sous forme électronique, afin de les transmettre à un autre responsable du traitement, et que les données doivent être transmises dans un délai d'un mois à compter de la demande, sans frais pour la personne concernée.

Le texte de ces lignes directrices est accessible à l'adresse : http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

PRÉCISIONS – DÉLÉGUE A LA PROTECTION DES DONNÉES

Par communiqué de presse daté du 13 décembre 2016, le Groupe de travail « article 29 » sur la protection des données de l'UE a diffusé plusieurs lignes directrices, accompagnées de FAQ, portant sur différentes thématiques liées à la mise en œuvre du RGPD, et notamment sur le délégué à la protection des données (DPO).

Ces documents précisent les cas dans lesquels un DPO doit être désigné (pour les organismes publics et les entreprises qui effectuent des opérations de traitement qui exigent un suivi « à grande échelle »), et insistent sur les qualités et compétences requises du DPO, ainsi que sur l'indépendance nécessaire du DPO à l'égard de l'organisme qui le désigne.

Le texte de ces lignes directrices est accessible à l'adresse : http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

PRÉCISIONS – AUTORITÉ DE CONTRÔLE CHEF DE FILE

Par communiqué de presse daté du 13 décembre 2016, le Groupe de travail « article 29 » sur la protection des données de l'UE a diffusé plusieurs lignes directrices, accompagnées de FAQ, portant sur différentes thématiques liées à la mise en œuvre du RGPD, et notamment sur la désignation d'une autorité de contrôle chef de file.

Ces documents précisent les cas de désignation d'une autorité de contrôle chef de file dans le cadre de la collecte et du traitement transfrontaliers ou dans plusieurs Etats membres de l'UE/l'EEE.

Le texte de ces lignes directrices est accessible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/lead_authorityen.pdf

RGPD vs. DIRECTIVE ET RÈGLEMENT « VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES »

La directive concernant la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) a été adoptée en 2002 afin de réglementer les communications électroniques, les services téléphoniques, et la prospection directe électronique. Elle a notamment imposé aux exploitants de sites Web l'obligation d'informer les internautes de l'UE/l'EEE de l'installation de témoins de connexion (cookies) sur leurs appareils (et de leur donner la possibilité de refuser l'installation de ces cookies).

Destiné à remplacer cette directive, le nouveau règlement concernant la protection de la vie privée, dont l'application devrait coïncider avec l'entrée en vigueur du GDPR le 25 mai 2018, a été revu pour s'assurer de sa conformité avec le RGPD. Son champ d'application est étendu puisqu'il couvre tous les acteurs du secteur, des fournisseurs de services internet aux fournisseurs de services de communication par contournement (dits services « over-the top » ou « OTT ») tels que WhatsApp et Skype. Comme le RGPD, il s'appliquera aux fournisseurs de communications électroniques qui sont établis en dehors de l'UE/l'EEE mais qui offrent leurs services à des utilisateurs se trouvant dans l'UE/l'EEE.

Le règlement « protection de la vie privée » doit encore être examiné et adopté par le Parlement européen et le Conseil avant d'entrée en vigueur.

Le texte complet de la proposition de règlement est accessible à l'adresse : https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Comment Skyhigh peut-elle vous aider ?

Les solutions proposées par Skyhigh peuvent aider, de différentes façons, les entreprises à se conformer au RGPD.

SERVICES CLOUD

Skyhigh peut tracer l'utilisation du cloud par vos salariés – et ainsi élaborer des rapports détaillant les services cloud utilisés, ainsi que l'origine et la destination des flux de données sur ces services cloud. Grâce à ces rapports, les entreprises sont en mesure d'identifier d'éventuels transferts de données hors de l'UE, de l'EEE ou des pays à protection adéquate, et d'évaluer la quantité de données transitant par ces services.

Votre entreprise est considérée comme responsable de toutes ses données, et de toutes opérations de traitement effectués sur ces données, qu'elles aient ou non été officiellement autorisées. Par conséquent, lorsque dans le cadre de l'utilisation d'un service cloud, un salarié perd, par inadvertance, des données, la responsabilité de la perte reste à la charge de l'entreprise. Skyhigh vous accompagne dans la gestion de cette responsabilité : Skyhigh recueille des données sur les services cloud approuvés et non approuvés (ce que l'on appelle l'informatique fantôme ou « Shadow IT ») afin que l'entreprise soit au courant de tous les trafics de données ayant lieu en son sein et puisse bâtir des politiques appropriées tenant dûment compte de tous les équipements réseau.

ANALYSE D'IMPACT

Skyhigh tient un registre contenant plus de soixante attributs par service cloud qu'il met à la disposition des responsables du traitement afin de les aider à mesurer le profil de risque de chaque service cloud et ainsi à adapter ses politiques en conséquence afin de garantir sa conformité au règlement.

TÉLÉCHARGEMENT DE DONNÉES

Les rapports élaborés par Skyhigh contiennent les noms de fichiers téléchargés vers des services cloud, que ces services bénéficient ou non de l'approbation de l'équipe informatique. Ces rapports peuvent faciliter les enquêtes menées sur d'éventuelles violations de données : lorsqu'un utilisateur tente d'exfiltrer du contenu, il peut accéder à une quantité inhabituelle de données ou les télécharger à partir d'un service approuvé et ensuite les transférer vers un service non approuvé dans un délai très court.

VIOLATION DE DONNÉES

Skyhigh peut réaliser un examen de vos fichiers afin de s'assurer que des données personnelles ne sont pas transférées en dehors de l'UE. A cette fin, Skyhigh peut utiliser sa propre technologie de prévention des fuites de données (DLP), ou bien travailler avec les outils propres à votre entreprise. Les données sont analysées afin de rechercher si elles contiennent des données à caractère personnel au moment de leur téléchargement sur le service cloud. Skyhigh peut également réaliser des analyses ponctuelles à la demande portant sur l'historique des données déjà stockées dans le cloud.

SUIVI DES UTILISATEURS PRIVILEGIÉS

Skyhigh peut élaborer des rapports sur les actions effectuées par des utilisateurs ayant le statut d'administrateurs. Cela permet d'une part de connaitre et d'encadrer le nombre d'utilisateurs disposant de droits d'accès privilégiés au sein de l'entreprise et de surveiller tout accès abusif aux données.

TRANSFERT DE DONNÉES EN DEHORS DES PAYS DE L'UE / L'EEE

Le registre tenu par Skyhigh contient trois entrées différentes relatives aux pays :

- le pays où sont détenues les données ;
- le pays où se trouve le siège social du fournisseur de services ;
- et le pays du droit applicable.

En s'appuyant sur ces données, les entreprises peuvent vérifier et contrôler les transferts de données en dehors de l'UE/l'EEE.

CONFORMITÉ DES FOURNISSEURS DE SERVICES CLOUD

Le registre de Skyhigh comprend de nombreuses informations sur les normes techniques et de protection des données appliquées par chaque fournisseur de services cloud, telles que les normes ISO 27001, ISO 27018, SOC2, SOC3, PCI, HIPAA.

Grâce à ces informations, les entreprises ont en main les clés pour décider quels services elles souhaitent souscrire et offrir à leurs utilisateurs.

CHIFFREMENT

Avec sa technologie, Skyhigh peut ajouter plusieurs niveaux de chiffrement sur les données avant qu'elles ne soient téléchargées, et les clés de chiffrement peuvent être conservées dans les locaux de votre entreprise. De cette manière, les données des utilisateurs ne sont pas transférées dans le cloud, ce qui vous permet de résoudre l'une des principales difficultés liées à l'utilisation du cloud computing dans le respect du règlement.

SERVICES TIERS

L'un des maillons faibles de l'environnement informatique de l'entreprise est le risque de partage des données avec des tiers qui ne possèdent pas le même niveau de sécurité. Skyhigh peut surveiller les collaborations avec des services tiers et définir des stratégies adaptées - par exemple des répertoires partagés dans les services cloud - en veillant à ce que les utilisateurs ne partagent leurs données qu'avec des tiers de confiance. Le DSI pourra définir une liste blanche (répertoriant les domaines autorisés à partager un répertoire cloud) ou, au contraire, une liste noire (répertoriant les domaines pour lesquels tout partage est prohibé). En outre, les API proposées par les principaux fournisseurs de cloud permettent à Skyhigh de tracer les téléchargements de données par ces tiers, et d'implémenter des technologies de DLP (pour la prévention de fuites de données) aussitôt qu'un risque est identifié.

DISPOSITIFS INFECTÉS

Skyhigh n'inspecte pas les dispositifs pour identifier s'ils sont victimes de virus, mais peut néanmoins constater les actions réalisées par un dispositif infecté à partir du trafic des données. Ainsi, les DSI peuvent être alertés d'une éventuelle infection susceptible d'entraîner une opération sur les données en violation du règlement.

IDENTIFICATION DES SITUATIONS

À HAUT RISQUE

Lorsque des utilisateurs perdent leurs identifiants informatiques, cela ouvre la voie aux cybercriminels : ils peuvent tenter de se connecter aux systèmes informatiques depuis d'autres pays du monde, ou s'ils ne disposent que d'une partie d'un identifiant, essayer d'accéder aux systèmes de l'entreprise en effectuant plusieurs tentatives de connexion. Un employé mécontent ou démissionnaire peut également effectuer des transactions inhabituelles, comme procéder au téléchargement d'une base de données clients. Fort de sa technologie, Skyhigh est capable de détecter des trafics inhabituels et de les signaler au DSI.

PISTE D'AUDIT

Skyhigh met ses compétences et son expertise en matière d'audit à votre disposition : en cas de violation de données, Skyhigh pourra fournir des informations précieuses à votre équipe d'enquête, la mettant ainsi en mesure de remonter les actions prises et d'évaluer l'impact de l'incident.

VEILLE CONSTANTE

Les menaces pesant sur vos données évoluent constamment. Skyhigh assure une veille constante des nouvelles menaces et des modes de trafic inhabituels et met à jour ses solutions afin de pouvoir détecter et maîtriser les pertes de données via les services cloud.

RGPD – SERVICES PROPOSÉS PAR SKYHIGH

Skyhigh mesure de nombreux attributs qui peuvent indiquer le niveau de conformité d'un fournisseur de services cloud au RGPD. En septembre 2016, notre étude a révélé que seuls 6% environ des services cloud pouvaient être considérés conformes au RGPD.

http://www.cloudpro.co.uk/leadership/risks/6321/only-6-of-cloud-services-comply-with-incoming-gdpr-law

Afin d'aider nos clients à comprendre leur profil de risque, nous avons mis en place un service grâce auquel ils peuvent tester la conformité des services cloud qu'ils utilisent au regard du RGPD.

https://www.skyhighnetworks.com/press/skyhigh-networks-launches-new-eu-gdpr-readiness-service-for-customers/

Mise en œuvre de votre plan d'action

Conseil juridique

Nous attirons votre attention sur le fait que ce document ne constitue pas un conseil juridique, et il vous est par conséquent recommandé de vous adresser à des avocats spécialisés en matière de protection des données afin d'obtenir tous les éclairages dont vous pourriez avoir besoin.

DÉSIGNER UNE ÉQUIPE POUR PILOTER L'ÉVALUATION DES SERVICES CLOUD

La gestion du cloud ne relève pas uniquement du service informatique. Constituez une équipe transversale dont la mission sera de passer en revue l'utilisation actuelle des services cloud, de définir des politiques et des procédures adaptées à l'entreprise, et d'anticiper l'utilisation future de ces services. Cette équipe doit être composée de membres des différents services ou départements de l'entreprise :

- Architecture informatique
- Sécurité informatique
- Juridique
- Conformité et risque
- Comptabilité
- Salariés
- Secteurs d'activité
- Marketing (il ne faut pas oublier que ce service gère énormément de données personnelles)

Cette équipe aura également pour tâche de définir les processus nécessaires à l'évaluation des services cloud, ainsi que les modalités à suivre pour ouvrir l'accès à un nouveau service cloud. L'équipe se réunira régulièrement pour suivre les évolutions qui pourraient survenir dans l'utilisation des services cloud au sein de l'entreprise.

CARTOGRAPHIER VOS DONNÉES

La première étape technique d'un programme de conformité au RGPD est sans doute la plus difficile : il s'agit d'avoir une image précise de la situation actuelle de l'organisation.

Conformité au règlement oblige, le responsable du traitement doit tout connaître sur toutes les données à caractère personnel en sa possession et être en mesure de répondre à des questions essentielles telles que : qui (salariés, sous-traitants collectant les données), quoi (catégories de données collectées), comment (les systèmes concernés) et où (lieu de stockage des données).

N'oubliez pas que les données à caractère personnel peuvent se présenter sous plusieurs formes, et parfois même ne pas être stockées sur des systèmes informatiques. Elles peuvent, en effet, être contenues dans des notes manuscrites, des fichiers papier ou encore sur des appareils enregistreurs. Elles peuvent, en outre, être conservées sous forme structurée ou non structurée. Si l'utilisation d'outils automatisés pour l'établissement de la cartographie de vos données était bien entendu essentielle pour rechercher et trouver les données concernées, l'utilisation d'outils manuels pourrait également être nécessaire afin d'identifier les points et les vulnérabilités qui pourraient ne pas avoir été identifiées par les outils automatisés.

COMMUNIQUER AVEC VOS SALARIES

Le succès de vos procédures en matière de services cloud repose en grande partie sur une bonne communication avec les salariés. Il est indispensable que vos collaborateurs soient au courant des politiques appliquées par l'entreprise et soient sensibilisés aux enjeux associés. Ils ont également besoin de connaître la liste de services cloud approuvés par l'entreprise et savoir à qui s'adresser pour demander l'accès à d'autres services. De cette manière, les salariés pourront comprendre et maîtriser le fonctionnement des services cloud, et adopter les bons réflexes en matière de cloud computing.

ASSURER UN SUIVI RÉGULIER

Le cloud computing est en plein essor, et l'utilisation du cloud se développe rapidement. En moyenne, une entreprise déploie, chaque jour, un nouveau système cloud. Vos politiques doivent être réexaminées régulièrement afin de s'assurer qu'elles restent d'actualité.

DOCUMENTER LES POLITIQUES, PROCÉDURES ET TECHNOLOGIES UTLISÉES

Conformément au RGPD, lorsqu'elle conduit une enquête, une autorité de contrôle peut demander l'accès aux politiques, procédures, technologies utilisées par l'entreprise, ainsi qu'aux formations dispensées aux salariés.

Les amendes qu'elle pourrait être amenée à prononcer seront calculées à la lumière des réponses données par l'entreprise aux demandes formulées par l'autorité dans le cadre de son enquête. L'autorité de protection des données française, la Cnil, fixe d'ailleurs déjà ses amendes en tenant compte des mesures prises par le responsable du traitement en faveur de la protection des données.

RGDP : LES QUESTIONS A SE POSER AVANT DE SE LANCER

Avant de commencer le processus de conformité de votre entreprise au RGPD, il est nécessaire de vous poser un certain nombre de questions, énumérées ci-dessous, qui peuvent vous servir de première liste de contrôle :

- La direction de votre entreprise est-elle sensibilisée à la question de la protection des données et du respect au RGPD ?
- Savez-vous où vos données sont stockées aujourd'hui ?
- Savez-vous exactement qui a accès aux données de votre entreprise ?
- Disposez-vous d'un processus permettant de supprimer les données des personnes concernées ?
- Existe-t-il au sein de votre entreprise une équipe transversale chargée d'analyser les obligations contenues dans le RGPD et d'en vérifier le respect ?
- Votre équipe marketing connaît-elle bien les règles relatives au consentement ?
- Documentez-vous les consentements obtenus ?
- Avez-vous une politique de suppression des données ?
- Savez-vous quels sous-traitants ont accès aux données ?
- Savez-vous quels services cloud sont utilisés par les utilisateurs ?
- Avez-vous mis en place un plan de formation et de sensibilisation à destination de votre personnel ?
- Collectez-vous des données relatives aux enfants ? Vérifiez-vous l'âge des personnes concernées, et demandez-vous, le cas échéant, le consentement du titulaire de la responsabilité parentale ?
- Êtes-vous sûr de pouvoir détecter les violations de données ?
- Appliquez-vous le principe de protection des données dès la conception pour les nouveaux systèmes ?
- Avez-vous élaboré un plan de communication à suivre en cas de violation de données ?
- Votre service informatique est-il capable de réagir dans les 72 heures ?
- Avez-vous désigné un délégué à la protection des données ?
- Recueillez-vous des données sensibles qui nécessitent des règles de protection plus strictes ?
- Avez-vous pris en compte toutes les sources de données, telles que les données relatives au personnel ?
- Procédez-vous régulièrement à l'audit de votre politique de confidentialité ?

- Vos équipes savent-elles qu'elles ne peuvent subordonner l'accès des utilisateurs à vos services à la collecte de leurs données ?
- Pouvez-vous garantir la réponse aux demandes des personnes concernées pour exercer leurs droits, et notamment le droit d'accès et le droit à la portabilité des données ?
- Avez-vous bien documenté toutes les opérations effectuées afin d'être en mesure de les justifier le cas échéant ?
- Connaissez-vous les bases juridiques sur lesquelles se fondent vos traitements ?
- Savez-vous si vos données sont transférées en dehors de l'UE et, dans l'affirmative, si ce transfert est effectué sur une base juridique appropriée ?
- Avez-vous effectué une analyse d'impact relative à la protection des données ?
- Quel processus avez-vous mis en place pour faire évoluer vos services et les maintenir à jour ?

FAQ - Questions fréquemment posées

Vous avez encore des interrogations après la lecture de ce guide ? Vous pourrez sans aucun doute trouver des éléments de réponse dans le tableau ci-dessous qui recense les réponses à certaines questions qui nous ont été posées à l'occasion d'événements récents et de webinaires que nous avons organisés.

Question	Réponse
Le texte du RGPD est divisé en 2 parties, la première contient des considérants numérotés de 1 à 173 et la seconde des articles numérotés de 1 à 99. Quelle est la différence entre ces deux parties ?	La première partie du règlement comprend les « Considérants » et a pour but d'exposer les raisons pour lesquelles le règlement est adopté. La seconde partie du règlement contient, quant à elle, les « Articles » qui constituent le texte du règlement. Ces deux parties forment bien entendu un tout harmonieux, mais ce sont les Articles qui constituent le cœur du règlement.
Le RGPD fait référence au chiffrement, mais ne précise pas le niveau de chiffrement requis. Existe-t-il des informations sur le niveau minimum de ce chiffrement (bases de données, in-flight etc.) ?	Le règlement ne donne pas de détails sur le chiffrement. Cela s'explique en partie par le souhait de ne pas devenir vite obsolète car les technologies évoluent rapidement, mais aussi par le fait qu'il est de la responsabilité du responsable du traitement et du/des sous-traitant(s) de décider quel type de chiffrement est « adapté au risque ».
Est-ce que le RGPD concerne également les données personnelles des salariés, des partenaires contractuels etc. ?	Oui, tout à fait. Le RGPD concerne toutes les informations collectées et traitées sur toutes les personnes physiques dans l'UE, peu importe le statut de ces personnes ou la manière dont sont collectées les données.

Question	Réponse
Quelle sera la situation du RGPD au Royaume-Uni après le BREXIT ? Le Data Commissionner va-t-il continuer à appliquer le RGPD en intégralité une fois le Royaume-Uni sorti de l'UE ?	S'agissant du BREXIT, le gouvernement britannique a, à ce jour, apporté deux précisions : 1. Le 31 octobre 2016, le gouvernement a confirmé que le RGPD sera bien promulgué. https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/ 2. Si le Royaume-Uni quitte l'UE, la « Great Repeal Bill » (une « grande loi d'abrogation ») assurera la reformulation des lois européennes existantes dans le droit national. Si, par la suite, le Royaume-Uni décide de modifier les dispositions du RGPD, il risque de ne plus être considéré comme un « pays adéquat » par l'UE et sera donc traité comme un pays ne garantissant pas la sécurité des traitements des données des citoyens de l'UE. Ce scénario catastrophe en matière de protection des données ne ferait pas du Royaume-Uni un pays adapté au monde des affaires, ce qui n'est pas le souhait de son gouvernement. Bien entendu, si vos données ne concernent que des personnes situées dans les vingt-sept autres pays de l'UE, la sortie de l'UE du Royaume-Uni n'aura pas de conséquence pour votre entreprise, et vous devez respecter le RGPD dès lors que vos données concernent des personnes physiques dans l'UE. https://www.skyhighnetworks.com/cloud-security-blog/how-does-the-brexit-vote-affect-gdpr-compliance/
Pourriez-vous préciser si le point de départ du délai de 72 heures pour la notification d'une violation de données à l'autorité de protection des données commence à compter de la survenance de la violation ou à compter de sa détection ?	Selon les termes du règlement : « En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance ».
Comment gérer le phénomène de « Shadow IT », et plus particulièrement les appareils utilisés sans notre approbation par les utilisateurs ? C'est une pratique qui n'est pas sous notre contrôle...	Il incombe au responsable du traitement de savoir où ses données sont stockées et traitées, y compris dans le cadre de l' « informatique fantôme », plus connue sous l'expression « Shadow IT ». Vous ne pouvez pas vous défendre en disant ne pas savoir, ou prétendre ne pas savoir. Vous êtes tenu d'avoir en place des processus, des procédures et des technologies appropriées afin d'être en mesure d'inventorier et de sécuriser le « Shadow IT » dès lors qu'il implique des données à caractère personnel relatives à des personnes physiques dans l'UE.
Quelles sont les autorités en charge de prononcer les amendes ?	Chaque pays possède une ou plusieurs autorités de protection des données (l'Allemagne, par exemple, en a plusieurs). En France, l'autorité compétente est la Commission nationale de l'Informatique et des libertés (Cnil) (https://www.cnil.fr/professionnel)

Question	Réponse
Quid des organismes du secteur public? Certains estiment que comme ils n'exercent pas d'activités commerciales, ils ne sont pas concernés par le RGPD et ne peuvent donc se voir infliger des amendes en cas de non-conformité. Est-ce vrai ?	Non, c'est faux. Le RGPD s'applique à quiconque détient des données sur des personnes physiques dans l'UE, qu'il s'agisse d'un organisme de droit privé commercial, d'un organisme de droit public, d'un organisme à but non lucratif, ou même d'une personne physique.
Si un ordinateur portable de l'entreprise contenant des données personnelles est perdu, mais que cet ordinateur est protégé par un chiffrement complet du disque, l'entreprise est-elle quand même obligée de déclarer la perte aux autorités ?	La perte doit dans tous les cas être signalée aux autorités. En revanche, il n'est pas toujours obligatoire d'en informer les personnes concernées. Selon les termes du règlement : « La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si (…) a) le responsable du traitement a mis en œuvre 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 ».
Qu'est-ce qu'un traitement « à grande échelle » ?	L'expression « à grande échelle » est utilisée à plusieurs reprises dans le règlement, sans toutefois n'y être jamais définie expressément.
Pensez-vous que, dans le cadre de la conformité au RGPD, les grandes entreprises mondiales mettront en œuvre des actions différentes à l'égard des personnes concernées en fonction qu'elles se situent dans l'UE ou en dehors de l'UE?	Il semblerait que la tendance au sein des multinationales soit de considérer le RGPD comme la « meilleure pratique » à suivre à l'échelle mondiale, et qu'elles comptent ainsi mettre en œuvre des politiques, des procédures et des technologies sur cette base pour l'ensemble des personnes concernées dans le monde entier sans discrimination, plutôt que d'essayer d'opérer une distinction dans leurs bases de données entre UE et hors UE. De nombreux pays vont adopter de nouvelles lois sur la protection des données et beaucoup vont s'aligner sur le RGPD et s'inscrire dans une approche commune.

Question	Réponse
Les entreprises qui développent et fournissent des solutions logicielles destinées à être utilisées pour collecter, traiter et gérer des données personnelles sont-elles également soumises au RGPD, ou est-ce au sous-traitant qui fait appel à elles de s'assurer que ces solutions sont adaptées au RGPD avant de les utiliser ?	Si l'entreprise ne stocke pas ou ne traite pas elle-même les données, elle n'a pas à assumer de responsabilité à cet égard, et il appartient au responsable du traitement ou au sous-traitant qui décide d'utiliser ces solutions de prendre les mesures adaptées. Cependant, les logiciels livrés en tant que service cloud peuvent avoir pour effet de placer le stockage et le traitement des données sous le contrôle du fournisseur de la solution. Dans ce cas, le fournisseur sera considéré comme un sous-traitant et deviendra coresponsable avec le responsable du traitement de la protection des données. Il convient de noter que dès lors que les données sont transférées à une entreprise de services d'externalisation, un service cloud, un infogérant ou tout autre organisme similaire, tous ces acteurs deviennent immédiatement des sous-traitants coresponsables avec le responsable du traitement. Inversement, si le sous-traitant du responsable du traitement perd, détruit ou modifie les données, le responsable du traitement qui a initialement collecté ces données sera également coresponsable avec le sous-traitant. Les responsables du traitement doivent donc sensibiliser leurs sous-traitants sur les responsabilités qui sont mises à leur charge.
Est-ce que l'enquête conduite par les autorités de contrôle à la suite d'une violation de données porte seulement sur les politiques, les procédures et la documentation ? Ou peut-elle également vérifier si l'entreprise dispose de professionnels de la sécurité au niveau managérial et opérationnel ?	L'autorité de protection des données peut enquêter sur tous les aspects relatifs à une violation de données au sein de l'ensemble de l'entreprise.
Quel est le meilleur programme de formation/certification dédié RGPD disponible actuellement sur le marché pour maîtriser la conformité au GDPR ?	De très nombreux organismes proposent des livres, des outils, des formations et des conseils sur le RGDP. La Cnil propose notamment sur son site des outils et des guides pour guider les professionnels dans leur mise en conformité. https://www.cnil.fr/fr/se-preparer-au-reglement-europeen
Pouvez-vous donner un bref aperçu de ce que doit contenir un rapport sur une violation de données.	La Cnil a publié des articles à ce sujet au regard de la loi Informatique et liberté, que vous pouvez utilement exploiter afin de préparer votre conformité au RGPD (https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles)

Question	Réponse
Après le Brexit, le Royaume-Uni sera-t-il toujours considéré comme assurant un niveau de protection « adéquat » au sens du RGPD à la lumière du projet de loi britannique relative au renseignement, le « Investigatory Powers Bill » (« IP Bill ») ?	Tant que le Royaume-Uni est dans l'UE, le niveau de protection n'est pas un problème et la situation est claire. Si le Royaume-Uni quitte l'UE, l'IP Bill pourrait être incompatible avec les critères utilisés par l'UE pour décider si un pays offre un niveau « adéquat » de protection des données. Dans ce cas, on peut raisonnablement penser que le Royaume-Uni et l'UE essaieront de mettre en place des mesures similaires à celles appliquées pour le transfert de données entre les Etats-Unis et l'UE (Safe Harbor et Privacy Shield). Toutefois, il est également hautement probable que ces mesures soient remise en cause devant les tribunaux, de la même manière que l'a été le Safe Harbor, et il est difficile d'en prédire le résultat.
Il est important de distinguer les données à caractère personnel des données à caractère personnel sensibles. Où peut-on trouver des informations expliquant les différences entre ces deux types de données ?	De très nombreuses sources existent à ce sujet. Par exemple : https://www.cnil.fr/fr/definition/donnee-sensible
Quel sera l'impact du RGPD si vous êtes certifié ISO27001 ? Quelles sont les principales différences entre ces deux textes, notamment en termes de documentation ?	Il existe en effet de nombreux thèmes et domaines communs entre ces textes, et de manière générale nous recommandons aux entreprises de se conformer aussi bien au RGPD qu'à la norme ISO27001. Cependant, n'oubliez pas que RGPD impose de notifier les autorités de protection des données et les personnes concernées des violations de données, prévoit de lourdes amendes en cas de manquement, et peut donner lieu à des recours collectifs qui peuvent impacter votre image de marque – pour toutes ces raisons, la protection des données n'est plus une question qui doit être à gérer exclusivement par le service informatique, mais bien par la direction de l'entreprise.
Est-ce que le RGDP autorise le stockage des données dans les services cloud mondiaux (par exemple, Microsoft Azure/Amazon AWS) ou l'utilisation des services fournis sur ces plateformes ?	Oui. De nombreux services cloud permettent aux clients de conserver leurs données dans l'UE, et pour ceux qui n'offrent pas cette possibilité, ils devront fournir au responsable du traitement une base juridique justifiant le transfert des données en dehors de l'UE. Le chiffrement des données, avant leur transfert, permet de réduire les risques (et d'éviter d'informer les personnes concernées en cas de perte des données). Mais par principe, le responsable du traitement doit obtenir la confirmation de tous ses sous-traitants qu'ils connaissent bien leurs obligations et leur coresponsabilité.
Le RGPD s'applique-t-il aux données personnelles relatives à des clients américains contenues dans des serveurs localisés sur le territoire de l'UE ?	Non, le RGPD ne s'appliquent pas aux citoyens américains, même si le RGPD est de plus en plus considéré dans le monde comme une meilleure pratique à respecter au niveau international.

Question	Réponse
On parle d'amende représentant jusqu'à 4% du chiffre d'affaires mondial consolidé ou 20 millions d'euros. Mais comment et sur quels critères sera fixé au final le montant exact des amendes infligées ?	Ce sont les autorités de protection des données qui sont en charge de prononcer l'amende en fonction notamment du nombre de données perdues, de la sensibilité de ces données et du contexte de la violation de données, tels que les processus et procédures mis en œuvre, la formation dispensée aux salariés, les technologies utilisées, etc. Le système d'imposition des amendes mis en place par le RGPD est très similaire à celui appliqué actuellement : par exemple en France l'amende maximale prévue est de 3 millions d'euros, et lorsque l'on compare ce montant à celui des amendes réellement prononcées, il est clair que tous les faits entourant la violation sont pris en compte. (https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil)
Savez-vous comment l'Europe sanctionnera les entreprises ayant des clients en Europe mais établie en totalité à l'étranger ?	Si une organisation se trouve « en totalité » à l'étranger, il sera évidemment difficile de la sanctionner. Cependant, des affaires récentes, telles que Vidal-Hall c/Google Inc. au Royaume-Uni et Weltimmo en Hongrie montrent que les entreprises qui ont des activités dans l'UE ne peuvent se soustraire à leurs responsabilités et invoquer que leur lieu d'établissement se trouve en dehors de l'UE.
Le Privacy Shield est-il actuellement conforme au RGPD ?	Pour l'instant, il est fort probable que le Privacy Shield soit remis en cause devant les tribunaux, au cours de l'année prochaine, afin d'évaluer sa compatibilité avec la directive européenne actuellement applicable en matière de protection des données.
Quelles sont les cinq actions qu'une entreprise (pas un fournisseur de services) doit prendre en priorité dans les prochains mois afin de se préparer au RGPD ?	Les actions à prendre sont multiples. De manière très générale, voici par exemple les actions qui pourraient être prises : 1. Désignez une équipe dédiée chargée de piloter la conformité au RGPD, comprenant des membres issus des services risque et conformité, informatique, RH ainsi que des représentants de la direction générale. 2. Réaliser l'inventaire des traitements de données de votre entreprise, en tenant compte des appareils utilisés par vos salariés, vos sous-traitants, vos partenaires et vos prestataires de services cloud. 3. Procédez à un audit de cet inventaire et identifier les domaines et applications présentant le plus de risques. 4. Commencez à documenter les politiques et les procédures mises en œuvre pour la gestion de vos données. 5. Identifiez les services de confiance que votre personnel peut utiliser. 6. Formez votre personnel à vos politiques et vos procédures. 7. Elaborez un plan de communication pour gérer les violations de données Pour une liste complète des actions pouvant être prises, vous pouvez consulter ce livre électronique : http://bit.ly/GDPR-Action-Guide

Question	Réponse
Quand est-il obligatoire de désigner un DPO ?	La désignation d'un DPO est obligatoire pour les organismes publics et pour les organismes privés dont les « activités de base (…) consistent en des opérations de traitement qui (…) exigent un suivi régulier et systématique à grande échelle des personnes concernées ». De nombreux commentateurs en ont déduit que le nombre de DPO allait exploser, mais ils ont peut-être un peu exagéré la situation. Chaque pays dispose néanmoins d'une marge de manœuvre pour adapter les critères de désignation d'un DPO en fonction de sa situation nationale. Ainsi, à l'heure actuelle, l'Allemagne impose la désignation de DPO dans davantage de situations qu'au Royaume-Uni. C'est une question qui aura besoin d'être clarifiée d'ici mai 2018.
Le RGPD couvre-t-il également les données personnelles des salariés ? Qu'adviendrait-il, par exemple, si les coordonnées bancaires de salariés étaient perdues ou volées ?	Oui, absolument. Un tel cas constituerait une violation de données à caractère personnel. Il est recommandé de s'assurer de notifier cette violation dans un délai de 72h à l'autorité de contrôle compétente. Il est nécessaire d'indiquer les faits concernant la violation, sa nature et ses effets ainsi que les mesures prises pour y remédier. La documentation permettant à l'autorité de contrôle de vérifier le respect des exigences imposées par le règlement doit également être transmise. Comme la violation des données bancaires engendre un risque élevé pour les droits et les libertés des personnes physiques, il convient de communiquer directement à la personne concernée la violation. Il est conseillé de mettre en place, en amont, des mesures d'urgence afin de pouvoir remédier à la violation et en atténuer les conséquences.
Est-ce que le RGPD s'applique aux données qui ne sont pas nominatives (pas de nom, pas d'adresse, etc.) mais qui pourraient être rattachées à des personnes (adresse IP, géolocalisation, habitudes, etc.) ?	Oui. Toute donnée pouvant être utilisée pour identifier un individu relève du champ d'application du RGPD. Ainsi, si vous possédez des données relatives à un appareil qui vous permet de connaître l'emplacement d'une personne (au moyen d'un historique des déplacements d'une personne en particulier), ces données sont soumises au RGPD.
Les obligations mises à la charge du responsable du traitement et du sous-traitant par le RGPD sont-elles identiques ?	Oui, dans presque tous les cas, la responsabilité est partagée, mais le responsable du traitement reste le responsable principal.
Il semblerait que le RGPD s'inscrive dans la lignée de mesures prises par d'autres pays dans le monde, telles que le DFARS aux Etats-Unis. Cela peut-il justifier l'implémentation d'un système de gestion de la sécurité de l'information (SGSI) ?	Oui.

Question	Réponse
Le RGPD n'est pas une révolution pour les responsables du traitement déjà en activité, ils devront tout au plus vérifier l'adéquation de leur politique de gestion des failles de sécurité et, de manière générale, s'assurer de la maîtrise globale de leurs processus. En revanche, les analyses d'impact sur la protection des données (PIA), et en particulier pour les anciens systèmes, pourraient constituer un bouleversement et nécessiter des investissements financiers supplémentaires. Quelle serait l'estimation des coûts nécessaires et comment évaluer efficacement l'impact sur les personnes concernées ?	Il est difficile de répondre précisément à cette question, chaque cas étant différent. Il est recommandé de contacter plusieurs cabinets spécialisés dans la protection des données afin d'obtenir et comparer leurs propositions.
Pourquoi un sous-traitant qui ne fait qu'offrir des services cloud avec des machines virtuelles qui ne sont en rien impliquées dans le système d'exploitation /les contenus/les finalités du traitement etc. est-il concerné par le RGPD ?	En théorie, ces entreprises peuvent être considérées coresponsables avec le responsable du traitement. Toutefois, le règlement précise que « la réparation peut être répartie en fonction de la part de responsabilité de chaque responsable du traitement ou de chaque sous-traitant dans le dommage causé par le traitement ». Les différentes parties ont donc la possibilité de conclure un accord qui décrirait la part jouée par chacune dans la collecte et le traitement des données afin de gérer proactivement le prononcé éventuel de sanctions.

Question	Réponse
Les PME comptant moins de 250 employés sont-elles obligées de désigner un DPO ?	Le règlement dispose, dans son article 35, que la désignation d'un DPO est obligatoire pour les autorités publiques ou pour les autres organismes dont les activités de base consistent en des opérations de traitement. Les Etats ont la possibilité d'édicter des règles supplémentaires relatives aux DPO. A l'heure actuelle, l'Allemagne exige la désignation de DPO dans des cas où le Royaume-Uni ne l'impose pas.
Pour une entreprise de taille moyenne, combien de temps serait nécessaire pour se mettre en conformité avec le RGPD ?	Comme indiqué par le responsable Privacy de Sky Europe en début d'année : « Si votre entreprise est aussi complexe que la nôtre et que vous n'avez pas encore commencé, vous êtes déjà en retard ». Il ne vous reste plus que 18 mois, alors il vous est fortement recommandé de ne plus attendre et de commencer votre processus de mise en conformité dès maintenant.

Question	Réponse
Quel est le délai pour répondre aux demandes d'accès formulées par les personnes concernées en vertu du RGPD : 28 jours ouvrables ou 28 jours calendaires ?	« ... sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande ».
Quelle certification recommandez-vous en matière de conformité au RGPD? Que pensez-vous de la CIPP / E ?	Je n'ai pas encore vu de certification spécifique, mais de nombreux organismes offrent des formations, outils, etc., et notamment en matière de gouvernance informatique.
Ce webinaire sera-t-il disponible en replay ?	https://www.isc2.org/emea-focused-webinars/default.aspx?commid=231387?bb
En pratique, comment mettre en œuvre le droit à l'oubli ? Faut-il l'appliquer aux anciens systèmes de sauvegarde, alors qu'il est quasiment impossible de revenir en arrière ?	Il est supposé que la suppression des données des systèmes front end sera considérée suffisante pour respecter le RGDP, à condition de bien documenter les mesures que vous prendrez ainsi que tout écart constaté. Cela permettra de pouvoir garder une trace dans le cas où il serait nécessaire de remettre une sauvegarde en production. Les dispositions relatives au droit à l'oubli peuvent sembler en contradiction avec d'autres réglementations existantes imposant aux entreprises de conserver certaines données.
Un sous-traitant est-il obligé de désigner un DPO, ou seul le responsable du traitement est-il concerné par cette obligation ?	La bonne nouvelle est que tout le monde n'est pas obligé d'en désigner un. Vous pouvez consulter des lignes directrices et une FAQ consacrée aux DPO aux adresses suivantes : http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
La Cnil encaisse-t-elle à son profit les amendes payées ?	A ce jour, les amendes payées à la Cnil sont versées au bénéfice du gouvernement français, la situation restera la même à l'avenir.
Les fournisseurs SaaS, tels que Salesforce, qui peuvent accéder aux données du client sans les stocker dans le cloud, ont souvent recours à différentes techniques de mise en cache. Lorsque des données personnelles sont mises en cache, et que ce fournisseur peut transférer en miroir ces données vers un autre site dans le monde, que peut faire le client pour ne pas manquer à ses obligations en matière de protection des données dès la conception, de stockage des données hors EEE, de conservation des données, etc. ?	Votre fournisseur SaaS doit vous confirmer qu'il accepte les responsabilités qu'il lui incombe en vertu du RGPD - il vous est d'ailleurs recommandé d'insérer une clause à cet effet dans le contrat que vous lie à votre fournisseur. Les données peuvent être transférées en dehors de l'EEE à condition que le contrat que vous avez conclu avec votre fournisseur soit considéré comme assurant une protection adéquate – à cette fin, reportez-vous par exemple aux clauses contractuelles types de la Commission européenne : https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne

Question	Réponse
Que conseilleriez-vous à un petit organisme à but non lucratif comptant douze salariés pour commencer à se mettre en conformité avec le RGPD ? Cela va-t-il lui demander beaucoup de temps et de moyens ?	Pas nécessairement (heureusement) - un document unique pourrait être suffisant afin de décrire les données que vous détenez et comment vous les utilisez. Le but du RGPD n'est pas d'entraver vos activités, mais de vous aider à adopter les bons réflexes.
S'agissant du cloud, il serait intéressant de comprendre comment le RGPD s'applique aux données CRM (Salesforce) et aux données stockées dans Office 365 (SharePoint), par exemple	Ces deux fournisseurs ont déjà publié leur propre documentation relative au RGPD. Pour faire un peu d'autopromotion, plusieurs guides concernant la sécurité d'Office 365 et de Salesforce sont disponibles sur le site de Skyhigh : www.skyhighnetworks.com
De ce que je comprends, le RGPD ne décrit pas en détail les contrôles qui doivent être mis en place en matière de sécurité, mais peut-on supposer que ceux contenus dans les normes ISO27001 et ISO27018 seraient « adéquats » ?	Le respect des normes ISO 27001 et ISO 27018 démontrerait que l'entreprise prend ses responsabilités au sérieux, mais elles ne seront probablement pas considérées comme adéquates pour couvrir toutes les dispositions du RGPD. Par exemple, le RGPD contient de nombreuses clauses, relatives notamment au consentement de l'utilisateur, au droit d'accès, à la clarté des termes utilisés pour informer les personnes concernées, etc. – qui ne sont contenues ni dans la norme 27001 ni dans la norme 27018.
Le critère d'intérêts légitimes permettra-il aux entreprises de continuer à traiter les données pour lesquelles un consentement « opt-in » a été collecté avant l'entrée en vigueur du RGPD, sans avoir à redemander leur consentement aux personnes concernées ?	Il est recommandé de contacter toutes les personnes figurant dans votre base de données afin de leur permettre de confirmer leur consentement ou de le retirer avant l'application du RGPD. Si vous souhaitez continuer à traiter les données qui ont été collectées avant l'entrée en vigueur du RGPD, vous devez le mentionner dans vos politiques en matière de protection des données.
Pourquoi y-a-t-il deux montants différents pour les amendes : 2% ou 10M€, et 4% ou 20M€ ?	Le montant de l'amende dépend du type de violation et il s'agit en tout état de cause d'un montant maximal. Le montant des amendes est fixé notamment en fonction du type de données perdues et des systèmes et des technologies que vous avez mis en place.
Si nous procédons au chiffrement des données que nous sommes tenues légalement de conserver pendant un certain temps, cela suffirait-il pour être en conformité avec le « droit à l'oubli » ?	Le chiffrement et le « droit à l'oubli » sont deux choses différentes, et je ne pense pas que vous puissiez prétendre que le fait de chiffrer les données qu'une personne vous demande d'effacer soit considéré comme une réponse adéquate à sa demande.
Comment doit-on procéder pour informer les clients dont nous détenons actuellement les données ? Et que faire si un client nous fournit de fausses informations sur un autre client.... Comment pouvons-nous contrôler cela ?	Vous pouvez prendre contact avec les personnes concernées de la manière dont vous le souhaitez, mais nous vous recommandons de documenter toutes les mesures que vous prendrez dans ce cadre. Il reste quelques mois avant l'entrée en vigueur du RGPD, ce qui vous laisse suffisamment de temps afin d'élaborer un plan de communication.
Si un client A met à jour nos systèmes en entrant des informations sur un client B qui s'avèrent fausses, est-il de notre responsabilité de nous assurer que les données entrées dans le système sont exactes ?	Malheureusement, oui. Tout d'abord je pense que vous ne devriez pas autoriser le client A à mettre à jour les informations relatives au client B. Lorsqu'un client A souhaite mettre à jour les informations d'un client B, il est recommandé de demander sa confirmation au client B, et lorsque le client A vous informe que des données sont incorrectes, il est de votre responsabilité de les mettre à jour.

Question	Réponse
Vous indiquez que seulement 9,1% des services cloud cryptent les données au repos, ce qui semble assez peu. D'où tenez-vous ces chiffres ?	Oui, à première vue, ce chiffre semble faible, mais Skyhigh répertorie environ 25.000 services cloud dans son registre, et beaucoup ne sont pas axés sur des entreprises clientes et ne procèdent pas au chiffrement des données.
Que faire si mon entreprise ne dispose pas des processus techniques requis pour supprimer des données ?	Désolé, mais vous devez vous doter de ce type de processus - vous avez une année pour tout mettre en place, et n'oubliez pas de prendre en compte vos sous-traitants et vos fournisseurs de services cloud.
Une fois le RGPD entré en vigueur, des obligations supplémentaires seront-elles mises à la charge des sous-traitants qui stockent les données qui leur sont transmises par le responsable du traitement sur le cloud ?	Oui – actuellement en France, les sous-traitants ne sont pas visés par la loi Informatique et libertés (ou par d'autres lois similaires dans l'UE), mais le RGPD va instaurer une coresponsabilité entre le sous-traitant et le responsable du traitement.
Si je demande à l'ANTS (l'agence qui gère les permis de conduire en France) de ne pas fournir mes données personnelles à des entreprises comme les sociétés gestionnaires de parking, de stationnement, etc., devra-t-elle se conformer à ma demande ?	J'en doute, mais il sera intéressant de voir si quelqu'un conteste son refus devant les tribunaux. Selon les dispositions du RGPD faisant référence aux infractions pénales : « La protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données, fait l'objet d'un acte juridique spécifique de l'Union ». Le règlement ne devrait donc pas s'appliquer aux activités de traitement à ces fins.
En Allemagne, l'adresse de courrier électronique professionnelle et les numéros de téléphone professionnels des salariés sont considérés comme des données à caractère personnel, alors qu'il me semble que ce ne soit pas le cas au Royaume-Uni. À partir du 25 mai 2018, comment les entreprises multinationales ayant des salariés à la fois en Allemagne et au Royaume-Uni devront-elles procéder pour être en conformité avec les lois applicables ? Faudra-t-il s'aligner sur la loi la plus stricte ?	Toutes les données qui identifient une personne sont considérées comme des données à caractère personnel – l'argument avancé par certains au Royaume-Uni, qui consistait à considérer que les données professionnelles n'étaient pas des données à caractère personnel, a été rejeté depuis plusieurs années. De nombreuses clauses du RGPD ont pour but d'harmoniser les approches qui seront adoptées par les différentes autorités de contrôle pour les affaires qui leur seront soumises. Nous vous recommandons donc de vous aligner sur la loi européenne la plus stricte.

Question	Réponse
Ne faut-il pas distinguer les citoyens des résidents ? Il me semble que le RGPD s'applique aux personnes traitants les données de n'importe quel citoyen de l'UE, quel que soit son statut de résidence. Si une entreprise de santé située en Nouvelle-Zélande détient des données personnelles relatives à la santé de citoyens de l'UE ... est-ce que le RGPD s'applique ?	Le RGPD parle des « personnes concernées qui se trouvent dans l'Union », à mon avis, c'est la résidence, et non la citoyenneté, qui est le critère pertinent. Dans votre cas, le RGPD ne devrait pas s'appliquer aux données concernant des citoyens de l'UE résidant en Nouvelle-Zélande sauf si ces personnes retournent sur le territoire de l'UE.
Le RDPG s'applique-t-il si une organisation établie dans l'UE traite les données client en dehors de l'UE ?	Oui, si les données concernent un résident de l'UE ou de l'EEE, le RGPD s'applique, quel que soit le lieu où les données se trouvent dans le monde.
Doit-on insérer des informations relatives au consentement dans les formulaires de contact d'un site Web destinés à être utilisés par une personne physique ou morale pour simplement demander de plus amples informations ou d'être rappelée par nos services ?	Oui. Dès lors que vous collectez des données de citoyens de l'UE, vous devez les informer des données que vous collectez et pour quelles finalités vous les collectez, ceci est d'autant plus valable si vous souhaitez partager ces informations à l'extérieur de l'UE. Le consentement doit être clair et univoque et ne peut être noyé au sein d'autres clauses contractuelles. Vous ne pouvez pas conditionner l'accès d'une personne à un service à la fourniture de son consentement pour collecter ses données (ce point est très important pour l'équipe marketing).
Le droit d'accès instauré par le RGPD est-il différent du droit d'accès actuel ?	Oui – les droits des personnes concernées ont été renforcés, et les responsables de traitement doivent mettre en place un processus pour les respecter.

POUR PLUS D'INFORMATIONS : LES WEBINAIRES

Webinaire, organisé conjointement par Skyhigh et The Cloud Security Alliance destiné à un public non européen : https://www.brighttalk.com/webcast/10415/225057/20-months-to-a-new-global-data-privacy-law-what-you-need-to-do

Webinaire, organisé conjointement par Skyhigh et ISC2, sous forme de questions/réponses (novembre 2016) : https://www.isc2.org/emea-focused-webinars/default.aspx?commid=231387?bb

Entretien avec Anthony Lee, directeur chez DMH Stallard : https://player.vimeo.com/video/130506236?autoplay=1

Blog et infographie dédiés au RGPD publiés par Skyhigh : https://www.skyhighnetworks.com/cloud-security-blog/may-the-fourth-be-with-eu/

Conclusion

Le règlement général sur la protection des données est un acte législatif majeur qui concerne toutes les entreprises, dans le monde entier. Par exemple, si votre entreprise exploite un site Web, vous êtes susceptible de recueillir des données sur les citoyens de l'UE et de les transférer dans d'autres régions du monde. C'est pourquoi l'impact du RGPD ne doit pas être pris à la légère, et chaque entreprise doit, dès à présent, auditer ses techniques de traitement des données et organiser et prioriser les actions nécessaires pour garantir sa conformité au RGPD.

Skyhigh peut notamment vous aider à évaluer les risques attachés à l'utilisation du cloud computing dans votre entreprise et à gérer ces risques afin de pouvoir bénéficier pleinement des avantages offerts par le cloud computing, tout en réduisant autant que possible les risques potentiels.

En résumé

Le respect du RGPD peut, à première vue, vous sembler contraignant, surtout si vous êtes responsable du traitement. Pour mieux comprendre le RGPD, mettez-vous à la place de la personne concernée. Lorsque vous achetez le produit d'une entreprise ou signer un contrat avec elle, celle-ci sera certainement amenée à collecter des données vous concernant. Vous vous attendez sûrement à ce que cette entreprise traite vos données avec tout le soin nécessaire et les conserve en toute sécurité. Les mesures introduites par le règlement ont pour but d'aider les entreprises à mettre en place à l'égard des données des personnes concernées le même niveau de sécurité que vous aimeriez que l'on applique à vos propres données.

Gardez-également à l'esprit que les données que vous collectez en qualité de responsable du traitement ne vous appartiennent pas. En effet, elles vous sont simplement prêtées par les personnes concernées. Quand une personne vous prête une chose, il est normal qu'elle puisse vous demander de lui restituer cette chose, vérifier si vous l'utilisez correctement, exiger que vous ne la prêtiez pas à quelqu'un d'autre sans son consentement, et conserver un droit de regard sur toutes les actions que vous pouvez effectuer sur cette chose.

Vous l'avez compris, la clé de la conformité au RGPD consiste à traiter les données que l'on vous confie comme si elles étaient les vôtres, et comme des objets précieux qui vous seraient prêtés en toute confiance.

GLOSSAIRE

Personne concernée : la personne physique dont les données sont collectées et qui peut être identifiée à partir de ces données.

Responsable du traitement : l'organisation qui détermine les finalités de la collecte de données, des moyens du traitement et des modalités de gestion des données, et qui assume, en définitive, la responsabilité de leur garde.

Sous-traitant : la personne physique ou morale qui stocke ou traite les données pour le compte du responsable du traitement

Autorités de contrôle (également appelées « régulateurs ») : les organismes publics institués par les gouvernements des pays de l'UE chargés d'aider les responsables du traitement et les sous-traitants à se conformer au règlement et à surveiller la bonne application du règlement.

Elles peuvent enquêter sur les infractions et imposer des amendes aux responsables du traitement et aux sous-traitants.

BIBLIOGRAPHIE

http://globalriskinsights.com/2016/01/eu-poised-to-adopt-worlds-most-stringent-data-laws/

http://www.lexology.com/library/detail.aspx?g=6dce6624-1d70-4ebe-8084-a93c6086a5b6

http://accessdata.com/blog/new-eu-data-protection-compliance-challenges

http://marketing.accessdata.com/l/46432/2016-01-18/2slrln

http://europa.eu/rapid/press-release_IP-15-6321_en.htm

RÉFÉRENCES

http://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html

https://www.cnil.fr

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-

10/cp150111fr.pdf

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

http://www.theguardian.com/technology/2015/apr/09/class- action-privacy-lawsuit-filed-against-facebook-in-austria

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

https://www.skyhighnetworks.com/cloud-security-blog/safe- harbor-invalid-whats-the-impact-to-companies-using-us-based- cloud-services/

A propos de Skyhigh

Skyhigh est un éditeur leader de solutions de sécurité des données dans les applications cloud (« Cloud Access Security Broker » ou CASB), utilisées par plus de 600 entreprises pour gérer et contrôler en toute sécurité plus de 25.000 services cloud, qu'ils soient ou non homologués par l'entreprise (prise en compte du phénomène de « shadow IT »). Grâce à Skyhigh, les entreprises peuvent, au moyen d'une plateforme cloud unique, obtenir la visibilité des services cloud utilisés et des risques associés, garantir leur conformité à la réglementation, assurer la sécurité des données, et détecter et gérer les menaces potentielles.

www.skyhighnetworks.com