Connexions

La newsletter
du réseau
Crowe Horwath

RGPD*,
ce qu'il faut savoir

* Règlement Général sur la Protection des Données

Crowe Horwath

#14

Sommaire

Connexions est la revue trimestrielle de **Crowe Horwath France**
Comité de rédaction de ce numéro : Arnaud Devoucoux, Marc Luccioni, Khaled Sabri, Thierry Grattery, Xavier Labarlette, Julien Benatar.
Conception, création : OneSelf
Crédits photos : 123RF

Suivez nos actualités sur

@CroweHorwath_fr

crowehorwathfrance.fr

Le chiffre

31 % des entreprises françaises se disent "préoccupées" par leur capacité à se conformer au RGPD et 26 % d'entre elles déclarent qu'elles seront en conformité avec le RGPD lors de son entrée en vigueur.

Source : Enquête Senzing (société de technologie logicielle / Californie) réalisée en février 2018

Edito

RGPD, les nouvelles règles de bonne conduite des entreprises.

Marc Luccioni
Associé Crowe Horwath Avvens

La blockchain, le big data, mais aussi la récente affaire Facebook (acquisition illégale des données de 50 millions d'utilisateurs de Facebook par Cambridge Analytica pour influencer la présidentielle aux Etats-Unis), montrent l'enjeu de la sécurisation des données personnelles et de leur utilisation. C'est dans cet esprit que l'Europe a souhaité renforcer et unifier la protection des données pour les individus par la mise en place du Règlement Général sur la Protection des Données (RGPD).

Désormais, les entreprises sont clairement responsables des données qu'elles détiennent. Conséquence : elles doivent se plier à de nouvelles règles de bonne conduite afin de conserver et traiter de manière sécurisée les informations personnelles qu'elles détiennent, que celles-ci émanent de leurs salariés ou de leurs clients.
Un certain nombre d'entre elles a déjà lancé un programme de mise en conformité. Ce dernier, propre à chaque entreprise, varie selon le métier, la taille ou bien encore le marché de l'entreprise.

Cette exigence entraîne inéluctablement des bouleversements conséquents pour le responsable de traitement dans son organisation. La CNIL, en charge du contrôle de l'application du règlement, a annoncé qu'elle fera preuve de souplesse et de pragmatisme pour accompagner les entreprises dans cette période de transition. A condition toutefois qu'elles soient engagées dans ce dossier. Pour ne pas se laisser prendre de court, voici les grands principes et quelques points de détail qui comptent.

Qu'est-ce que le RGPD ?

Khaled Sabri
Associé Crowe Horwath RSA

Le 25 mai prochain sera applicable le nouveau Règlement Général sur la Protection des Données (RGPD). Ce texte européen, qui tient compte des nouvelles réalités numériques, réforme en profondeur l'exploitation des informations personnelles par les acteurs économiques.

Partant du constat que les réglementations nationales ne répondaient pas suffisamment aux menaces issues de l'exploitation des données personnelles, le législateur européen a souhaité revoir les règles applicables en profondeur.

Mieux protéger les données des personnes physiques

Le règlement européen n°2016/679, dit règlement général sur la protection des données (RGPD) renforce les droits des personnes physiques en matière de contrôle de leurs données personnelles. Il impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données. Lorsque leurs données personnelles sont collectées, elles devront y avoir accès (principe du consentement) et pourront en demander l'effacement (droit à l'oubli), la rectification ou la récupération (droit à la portabilité).

Ce règlement, adopté le 27 avril 2016, abroge la directive européenne de 1995 et harmonise le droit européen en matière de protection des données personnelles. D'application directe, il laisse néanmoins des marges de manoeuvre aux Etats membres. C'est pourquoi, en France, un projet de loi relatif à la protection des données personnelles modifiant la loi n°78-17 « Informatique et Libertés » de 1978 est en cours d'examen au parlement.

De nouvelles obligations pour les entreprises

Le RGPD s'applique à toutes les entreprises traitant des données personnelles de résidents de l'U.E., basées en Europe ou non. Il demande aux entreprises d'assurer un respect des textes sur la durée : la gouvernance des entreprises, ses politiques internes et des dispositifs de contrôle doivent être revus afin de garantir le respect des données personnelles. Il repose sur une logique de conformité, dont les organisations sont responsables.

La charge de la preuve est désormais inversée. Il n'incombe plus aux consommateurs de prouver que leurs données personnelles ont été exploitées contre leur gré ou de façon abusive mais aux entreprises de prouver qu'elles ont respecté leurs obligations réglementaires en matière de traitement de données, sous peine d'être sanctionnées jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires consolidé.

Le règlement leur impose ainsi des exigences spécifiques en matière de confidentialité, de sécurité et d'intégrité des données. Elles devront notamment prendre en compte les exigences de protection des données personnelles dès la conception des systèmes de traitement ("Privacy by design"), mettre en place un registre des traitements des données, prendre des mesures de protection des données. Quant aux formalités CNIL, elles sont désormais allégées.

Qu'est-ce qu'une donnée à caractère personnel ?

C'est une donnée qui permet d'identifier une personne physique : un nom, une adresse, un numéro de téléphone, un numéro de sécurité sociale ou un matricule, une photo, une vidéo, des données biométriques, etc.

Les données liées à la santé, la religion et la politique sont considérées comme sensibles par le règlement. Il en découle un régime de protection accru. Les données relatives aux personnes morales ne sont pas considérées comme des données personnelles.

Patrick Soenen, Associé Crowe Horwath Callens Pirenne & Co

RGPD, les points d'attention

Beaucoup d'entreprises pensent que le règlement ne s'applique qu'aux grandes organisations. Non ! Le RGPD concerne également les petites et moyennes entreprises, les associations, les structures publiques. Quels que soient leur taille et leur statut, les organisations sont impactées par ces nouvelles exigences. Revue des principaux points d'attention.

Patrick Soenen
Associé Crowe Horwath
Callens Pirenne & Co

1. La base légale

Les données personnelles collectées doivent répondre aux finalités des traitements. Les informations supplémentaires utilisées pour des campagnes de marketing, par exemple concernant des loisirs, doivent faire l'objet de consentement.

2. Une protection appropriée

Les données personnelles traitées doivent faire l'objet d'une protection adéquate. En cas de violation des données, une notification devra être faite dans les 72 heures à la CNIL et éventuellement aux personnes concernées. En outre, les données personnelles doivent être effacées lorsque la finalité est terminée, par exemple en fin de relation contractuelle, en l'absence de toute autre obligation légale.

3. Une gestion responsable

Le traitement de données personnelles doit être inscrit dans un registre interne tenu à disposition de la CNIL. Et en cas de traitement de données personnelles à large échelle ou de données sensibles (médicales, opinions, condamnations…), un délégué à la protection des données (DPD) doit être désigné qui conseille et veille à la conformité avec le RGPD. Sur base de ce registre, il conviendra d'évaluer les risques en cas de vol, d'altération, de suppression… des données personnelles.

4. Transfert hors espace européen

En cas de transfert de données personnelles hors de l'espace européen, même dans vos propres filiales, des mesures de protection adéquates telles que des règles d'entreprise contraignantes doivent être prévues.

5. Sous-traitance

Les tierces parties qui traitent vos données personnelles doivent respecter de nouvelles exigences : traitement uniquement sur base d'instructions écrites, mise en œuvre de mesures adéquates de protection, communication transparente sur leurs propres sous-traitants, contribution aux inspections de la part de la CNIL, restitution et destruction des données en fin du contrat…

6. Information transparente

Sur votre site web et vos autres supports de communication doivent figurer les informations requises, tels que finalités, durée de rétention, coordonnées de l'éventuel DPD, destination des données, transfert hors UE, etc…

7. Droits des personnes

Les personnes concernées pourront avoir accès à leurs propres données personnelles, les mettre à jour, les oublier, s'opposer aux ciblages commerciaux, etc…

Qui utilise les données à caractère personnel ?

Marketing
via la personnalisation des produits et des services

Ressources Humaines
à des fins de recrutement, de gestion de carrière et d'expertises

R&D
afin de connaître et d'anticiper les opportunités potentielles à développer.
Les modèles prédictifs et l'Intelligence Artificielle sont essentiels à l'innovation.

En pratique, comment se préparer ?

Voici les questions à se poser pour se mettre en conformité avec les nouvelles exigences du RGPD.

Thierry Grattery
DSI Crowe Horwath RSA

1/ Traite-t-on des données à caractère personnel ?

Faites un audit de vos données. Identifiez les types de données et les traitements effectués en faisant une cartographie de ces traitements.

2/ Qui va piloter le projet de mise en conformité ?

Nommez une personne responsable du projet et de son suivi. La nomination d'un délégué à la protection des données ou DPO n'est obligatoire que dans certaines conditions.

Si vous n'y êtes pas soumis, choisissez une personne ayant une vision générale de l'entreprise qui puisse être un chef d'orchestre de la conformité, c'est-à-dire ni le responsable informatique ou RH, ni un administrateur.

3/ A-t-on le consentement des personnes sur le traitement de leurs données ?

Contactez toutes les personnes physiques dont vous possédez des données à caractère personnel pour obtenir leur consentement explicite.

4/ Ces traitements sont-ils sécurisés ?

Étudiez les risques attachés à ces données en matière de stockage et de traitement. Pour vous aider, la CNIL propose un outil appelé PIA qui permet d'identifier les risques en répondant à des questions spécifiques. Cet outil est disponible sur le site de la CNIL.

5/ Les sous-traitants ont-ils mis en œuvre le RGPD ?

Si vous externalisez votre SI et/ou votre site internet par exemple, assurez-vous que ces entreprises présentent des garanties en matière de sécurité de traitement des données. Intégrez dans les contrats avec les fournisseurs et/ou les sous-traitants des clauses pour qu'ils s'engagent à respecter le RGDP.

6/ Que faire en cas de violation de données ?

Vérifiez le dispositif de sécurité de votre SI. Cela peut passer par le renforcement des pare-feux pour éviter une cyber attaque, la mise en place de logiciels spécifiques pour chiffrer les données, la définition de procédures en cas de violation de données : procédure d'alerte, plan d'action, information de la CNIL, de l'assureur, des entités/personnes concernées.

7/ Tous les collaborateurs sont-ils concernés ?

Tous ceux qui ont un ordinateur et sont connectés au SI sont potentiellement concernés par la gestion de données. Il faut donc les sensibiliser aux nouvelles exigences du RGPD. Définir une charte de bonne conduite informatique précisant les règles gestion des données personnelles peut également être une bonne pratique.

8/ Combien cela va-t-il coûter ?

Le coût de la mise en conformité au RGPD varie en fonction des entreprises. Tout dépend si vous effectuez des traitements à grande échelle ou de données sensibles, si vos équipements informatiques sont bien protégés ou non, si vous devez nommer un DPO ou un chef de projet.

Qu'est-ce qu'un traitement de données ?

Il s'agit de toute opération ou de tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel. Cela recouvre la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, l'effacement ou la destruction de données.

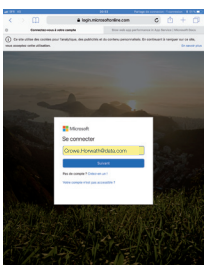
Comment se mettre en conformité ? L'exemple du cabinet Avvens.

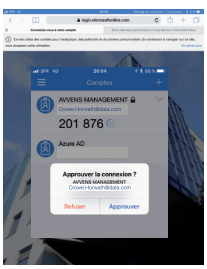
Marc Luccioni,
Associé Crowe Horwath
Avvens

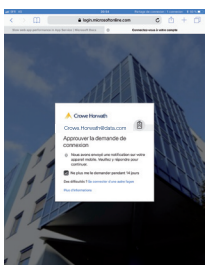
Nos cabinets doivent se mettre en conformité avec le RGPD et sa mise en œuvre passe nécessairement par le recours à des outils adaptés. Le RGPD représente un changement de paradigme dans les exigences de confidentialité mondiales régissant la manière dont les organisations gèrent et protègent les données personnelles, tout en respectant les choix individuels, quel que soit l'endroit où les données sont envoyées, traitées ou stockées. Il introduit de nouvelles exigences en matière de confidentialité, de sécurité et de conformité pour les organisations qui proposent des biens et des services aux résidents de l'Union européenne (UE).

La sécurité de notre réseau informatique est une priorité permanente chez Avvens. Nous avons entrepris, il y a maintenant 1 an une réorganisation complète de l'infrastructure de notre réseau en nous appuyant sur les technologies Microsoft Office 365 et AZURE. Office 365 est un service d'abonnement basé sur le cloud regroupant des outils adaptés aux méthodes de travail d'aujourd'hui. En associant les logiciels les plus performants, tels qu'Excel et Outlook, à des services cloud de pointe comme Exchange online, OneDrive et Microsoft Teams, Office 365 permet à tous les utilisateurs de créer et de partager des documents en tout lieu et sur tout type d'appareil, en mettant en oeuvre un niveau de sécurité satisfaisant les prescriptions du RGPD.

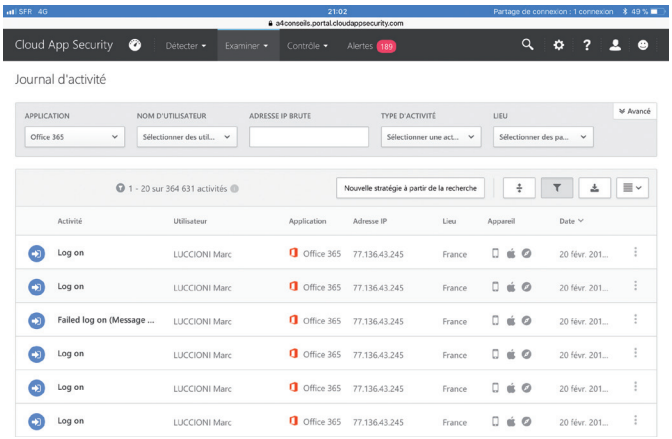
La sécurité de notre infrastructure repose sur 3 axes : authentification, fermeture du périmètre du réseau, gestion et audits des droits d'accès, sauvegardes. En matière d'authentification, l'ensemble des accès est piloté par un login et un pot de passe complexe. Les accès administrateurs et sensibles (certains associés notamment) font l'objet d'une authentification multi-facteur "MFA". Après saisie du login et du mot de passe, l'utilisateur reçoit une notification sur son mobile l'invitant à confirmer sa connexion.



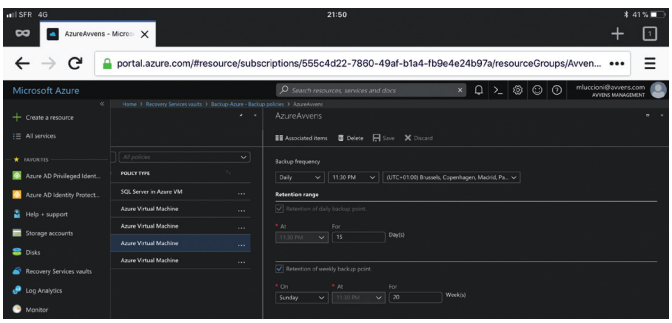




Les accès aux serveurs de production cegid, caseware, bureautique pour partie, se font sur la base du login et mot de passe, uniquement à partir d'ordinateurs appartenant à notre organisation. Ces accès, et les opérations sur les fichiers, sont ensuite consignés dans une base de données et analysés en vue d'identifier d'éventuels piratages par la mise en œuvre de stratégies de sécurité allant des téléchargements de masse, connexions simultanées impossibles (1 en France et quelques secondes plus tard en Chine par exemple).



Concernant les sauvegardes nous avons choisi un mode de sauvegarde dans le cloud reposant sur des sauvegardes journalières conservées selon un plan particulier. Ces sauvegardes sont conservées dans un data center Microsoft à Dublin et y sont redondées 3 fois à des endroits différents du data center puis répliquées à Amsterdam. Ces données peuvent ensuite être restaurées si nécessaire via le net.



Gaelle Patetta, Secrétaire général adjoint et directeur juridique du Conseil supérieur de l'Ordre des Experts-Comptable

L'expert-comptable peut accompagner les entreprises dans leur mise en conformité avec le RGPD.

Les experts-comptables sont-ils concernés par le RGPD ?
Le règlement européen met un certain nombre de nouvelles obligations à la charge des entreprises et donc des cabinets d'expertise comptable. Ces derniers sont concernés à plusieurs titres. En tant que cabinet, ils peuvent par exemple détenir une base de données clients et prospects, ainsi que des données RH pour leurs salariés (paie, base de CV etc.). Dans l'exercice de leurs missions, ils peuvent effectuer des traitements sur les données fournies par leurs clients (traitement technique du dossier, travaux de paie et gestion sociale etc.). Concrètement, cela signifie qu'ils doivent mettre en place des mesures techniques et organisationnelles dans le traitement de ces données pour garantir leur bonne utilisation, avec un niveau de sécurité adapté.

Quel impact cela a-t-il dans leurs relations avec leurs clients ?
Les experts-comptables doivent d'abord s'assurer qu'ils respectent eux-mêmes, dans leur activité, les obligations fixées par la nouvelle règlementation s'appliquant aux utilisateurs de données personnelles : sécurité des fichiers, confidentialité des données, durée de conservation limitée des données personnelles, information des personnes, finalité des traitements, etc.
Ils ont ensuite intérêt à s'assurer que leurs clients appliquent les mêmes règles. Ils peuvent alerter leurs clients sur leurs obligations légales de protection des données à caractère personnel.

Peuvent-ils accompagner leurs clients dans la mise en place de cette nouvelle réglementation ?
Bien sûr ! L'expert-comptable est un bon partenaire pour aider les entreprises à se mettre en conformité avec la nouvelle règlementation. Ils peuvent aider les entreprises à auditer les traitements existants, vérifier le niveau de conformité avec la règlementation, préconiser les adaptations nécessaires. Par exemple, ils peuvent aider leur client à auditer leur sécurité informatique, vérifier que les sous-traitants ont mis en place les mesures de sécurisation nécessaires, documenter les actions pour répondre aux contrôles de la CNIL. Pour mettre leur cabinet en conformité ou pour accompagner leurs clients, les experts-comptables peuvent s'appuyer sur des outils méthodologiques développés spécifiquement par les experts du Conseil supérieur et disponibles sur la plateforme Conseil Sup' Services. Elle propose un guide et des documents opérationnels tels que des questionnaires pour réaliser l'audit des traitements existants, un référentiel pour constater s'il existe des écarts entre ce qui est réalisé en interne et la règlementation, des exemple de plan d'action, des questionnaires sur la partie sécurité informatique à envoyer aux sous-traitants etc.

Gaelle Patetta
Secrétaire général adjoint et directeur juridique du Conseil supérieur de l'Ordre des Experts-Comptables

Les aides de la CNIL

La CNIL propose de nombreux outils pour aider les entreprises à se conformer aux obligations du RGPD. Parmi ceux-ci, des catalogues de bonnes pratiques permettant de traiter les risques que les traitements de données à caractère personnel peuvent faire peser sur les libertés et la vie privée des personnes concernées : les PIA.
Le logiciel open source PIA (Privacy Impact Assessment) facilite la conduite et la formalisation d'analyses d'impact sur la protection des données.
Cet outil "prêt à l'emploi" permet d'anticiper l'entrée en application du RGPD et de se mettre en conformité, en déroulant pas à pas la méthode d'analyse d'impact de la CNIL.

www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Et si le RGPD était une opportunité pour votre entreprise ?

Les 5 atouts clés du RGPD pour votre entreprise.

Xavier Larbalette,
DSI Crowe Horwath Fideliance

Toutes les données que nous produisons chaque jour sont répertoriées et réutilisées, qu'elles soient émises par nos ordinateurs, nos téléphones, les objets connectés, nos voitures… Le nouveau règlement définit un cadre d'utilisation de ces données personnelles, une opportunité de protéger le patrimoine digital de votre entreprise et de renouveler le pacte de confiance conclu avec vos différents interlocuteurs (clients …).

1. Valoriser son entreprise
À compter de l'application du RGPD, les entreprises devront être en mesure de démontrer leur conformité avec la réglementation en cas de contrôle de la CNIL. Les enjeux liés au risque de non-conformité sont importants puisque des sanctions sont prévues. En cas de cession de l'entreprise, garantir la conformité de son entreprise (c'est-à-dire avoir mis en place les procédures adéquates) rassure un acheteur et conforte la pérennité de celle-ci. C'est un critère de valorisation.

2. Sécuriser ses risques
La non-conformité est une source de risques multiples.

- Risque sur l'image et la réputation : en cas de contrôle de la CNIL, prouver qu'il n'y a pas de problème dans le traitement des données personnelles rassure les parties prenantes et permet d'éviter un potentiel "name and shame*" préjudiciable à la marque.
- Risque de cyberattaque : le RGPD appelle la mise en place d'un plan d'action pour sécuriser les données personnelles, une opportunité de revoir ses procédures en vue d'identifier les failles potentielles, avec comme objectif de protéger l'ensemble de son système.
- Risque sur le résultat : la pénalité prévue en cas de non-conformité peut s'élever à 4% du chiffre d'affaires. Autant allouer du temps et du budget pour prendre l'orientation de la transformation digitale.

3. Rationaliser ses processus
Le RGPD conduit à rationaliser ses processus de gestion des données. À la clé, une chasse au données redondantes, obsolètes voire erronées, donc sans intérêt.
Libérer cet espace de stockage devient une source d'économies potentielles (ces données "obscures" coûteront inutilement aux entreprises du monde entier 2 900 milliards d'euros d'ici 2020).

4. Développer le chiffre d'affaires
Les appels d'offres vont contenir des clauses de conformité au RGPD. Pour être éligible, il faudra prouver sa conformité en décrivant ses procédures, en communiquant les résultats d'un audit, ou en disposant d'un label... C'est un des leviers sur lesquels l'État entend s'appuyer pour mettre en œuvre la réglementation. Mieux vaut donc anticiper ces nouvelles exigences afin de ne pas être bloqué dans son développement commercial. Profitez-en pour que cela devienne un avantage concurrentiel !

5. Accroître la confiance
L'exigence de transparence du nouveau règlement se traduira par la mise en place de plateforme permettant un dialogue sécurisé entre l'entreprise et ses clients. Cette espace leur permettra de vérifier leurs données personnelles, les modifier, donner leur consentement à leur utilisation… (fini la transmission des fiches de paie par mail par exemple). La démarche de conformité au RGPD doit donc être abordée comme une opportunité stratégique. Elle permettra de mieux connaître ses partenaires et clients avec de la donnée pertinente. Enfin, ces nouvelles règles invitent à renouveler la relation autour d'une démarche "data responsable". Garantir aux citoyens la juste utilisation de ses données est un atout au service de la confiance !

* "Nommer et couvrir de honte" autrement dit montrer du doigt dans les médias comme cela est couramment pratiqué dans les pays anglo-saxons.

La donnée est le nouveau pétrole des entreprises. La confiance est la nouvelle monnaie. Sécuriser les relations va dans le sens de la confiance.

En chiffre

90% des données existantes aujourd'hui ont été créées au cours des deux dernières années et la production de ces données devrait exploser de 800% d'ici 5 ans selon les prévisions du cabinet Gartner. Les données proviennent des messages que nous envoyons, des vidéos que nous publions, des informations climatiques, des signaux GPS ou encore des transactions en ligne. Entre 50 et 100 milliards d'objets seront connectés en 2020.