TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

Introduction à la Règlementation européenne sur la protection des données

G DATA Software AG | Septembre 2017

Table des matières

Pour les entreprises, la protection des données personnelles de leurs clients n'est pas une option. La nouvelle règlementation européenne sur la protection des données (RGPD) vient renforcer la loi informatique et liberté française. Les entreprises ont jusqu'au 25 mai 2018 pour s'adapter à cette nouvelle directive et protéger les données de leurs clients de manière efficace. Les pénalités pour le non-respect du nouveau règlement sont dissuasives. Les employés doivent être informés, les processus d'activités et les outils correspondants doivent être analysés pour s'assurer que les données des clients soient traitées dans le respect de la loi. Ces dispositions impactent également le domaine de l'informatique dans les entreprises. Dans ce document, les exigences les plus importantes de la règlementation européenne sur la protection des données seront présentées. Concernant l'aspect technique, les avantages d'une solution de sécurité multicouche dans le respect de cette directive vous seront également présentés.

1. Qu'est-ce que le règlement européen sur la protection des données ?

Le règlement européen sur la protection des données (RGPD) a été adopté par le parlement européen en avril 2016. Il organise la modernisation et l'uniformisation des lois sur la protection des données au niveau européen. Le but est de garantir la protection des données relatives aux personnes au regard des principes suivants[1] :

- Légitimité, loyauté du traitement, transparence
- Finalité
- Minimisation des données
- Exactitude
- Limitation de l'enregistrement
- Intégrité et confidentialité

La règlementation remplace la directive européenne sur la protection des données personnelles de 1995. Elle se distingue par le fait qu'il ne s'agit plus d'une directive, qui laisse une plus grande latitude aux pays membres quant à son application, mais d'une règlementation européenne qui s'applique automatiquement à chaque État membre de l'Union européenne. La date d'entrée en vigueur était le 24 mai 2016. Pour donner aux entreprises le temps de s'adapter au nouveau règlement, un délai transitoire jusqu'au 25 mai 2018 a été accordé. Jusqu'à cette date, les entreprises ont le temps de mettre en place les règles de la RGPD.

[1] Article 5 de la RGPD. Le texte de loi complet est à lire ici : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

2. Les entreprises concernées par la RGPD

Le règlement sur la protection des données organise la protection de données à caractère personnel. Ainsi, toute entreprise au sein de l'Union européenne qui traite des données personnelles est concernée. Pour rendre plus clair à quelle(s) donnée(s) se réfère la loi, voici un extrait de l'article 4 du texte de loi :

> *Aux fins du présent règlement, on entend par « 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*.

Plus concrètement, les données communément collectées par les entreprises et qui entrent dans le cadre de la RGDP sont : le nom, le genre, l'âge, l'adresse postale ou encore l'adresse de messagerie électronique. Il s'agit de données traitées intentionnellement dans un système CRM, mais également de données collectées automatiquement dans des systèmes informatiques, tels que l'adresse IP, les habitudes de navigation ou tout comportement journalisé par exemple.

3. Des droits étendus pour les clients

La RGDP décrit le cadre que doivent mettre en place les entreprises quand elles traitent des données personnelles. Bien que beaucoup de mesures aient déjà été définies dans la Data Protection Directive, il y a quelques nouveautés qui peuvent représenter un défi. En bref :

- Le droit à l'effacement (« droit à l'oubli ») : le client « a le droit d'obtenir […] l'effacement […] de données à caractère personnel » (Article 17)[2].
- Traitement et consentement : chaque client doit être informé « en des termes clairs et simples » sur le traitement des données qu'il transmet. Le consentement d'utiliser ces dernières doit être « donné librement » – ne doit donc pas être contraint (par exemple : le consentement à l'utilisation à des fins publicitaires pour passer une commande) ; Raison 42 et 43 de la RGDP[3].
- Notification rapide aux autorités : « 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 […] 72 heures au plus tard après en avoir pris connaissance » (Article 33)[4]

[2] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article17
[3] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/
[4] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article33

- Droit à la portabilité des données : les clients ont le droit de recevoir les données enregistrées les concernant « dans un format structuré, couramment utilisé et lisible par machine » (Article 20)[5]

La mise en place de ces droits et leur forme dans les processus de travail ne sont pas à prendre à la légère. Par exemple, les directives présupposent que les entreprises sachent quelle est l'envergure et à quelle place exactement ont été enregistrées des données à caractère personnel. Dans une petite entreprise avec une banque de données clients centralisée, cela peut être le cas. Mais dans des structures d'entreprises plus complexes et éclatées ou lors d'utilisation de plateformes en Cloud, l'exercice est plus complexe. Certaines dispositions légales de conservation peuvent aussi engendrer de potentiels conflits. Par exemple, même si un client veut supprimer ses données, l'entreprise se doit de conserver ses informations de facturation.

4. Les sanctions en cas d'infraction

Pour les entreprises françaises, les dispositions concernant la protection des données personnelles de la RGPD ne sont pas nouvelles. La loi informatique et liberté du 6 janvier 1978, modifiée en 2004, traitait déjà des principes de finalité, de pertinence, de conservation de droit et de sécurité des données. En France, la nouveauté réside dans le montant élevé des amendes. Dans le cas où les autorités de la protection des données constateraient une infraction, les amendes suivantes sont prévues :

- Jusqu'à 20 millions d'Euros ou 4% du chiffre d'affaires mondial de l'entreprise (le montant le plus haut sera pris en compte)
- Jusqu'à 10 millions d'Euros ou 2% du chiffre d'affaires mondial de l'entreprise (le montant le plus haut sera pris en compte)

La première catégorie d'amende sera utilisée pour les grosses infractions, telles que la divulgation accidentelle, la perte ou le vol d'une base de données. La seconde catégorie a été conçue pour les petites infractions, comme le non-respect de l'obligation de notification (Article 33). Les amendes ont été définies dans l'article 83 de la RGDP et doivent être « dans chaque cas, effectives, proportionnées et dissuasives ».

5. Préparer l'échéance

Pour les entreprises françaises traitant historiquement avec des données personnelles, la mise en conformité avec cette nouvelle règlementation ne devrait être qu'une formalité. Les travaux de la CNIL et la législation française en matière de protection des données personnelles apportent déjà une base solide afin de répondre aux nouvelles dispositions. Indépendamment du niveau de préparation de l'entreprise, cette nouvelle réglementation est une opportunité de réflexion sur la collecte et le traitement des données. C'est également un moment privilégié afin de faire un point

[5] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article20

sur les processus. Dans cet exercice, la check-list de la CNIL[6], destinée à estimer le niveau de sécurité de vos données, est une aide.

5.1. Désigner un délégué à la protection des données

Le premier pas est la désignation d'un délégué à la protection des données (Section 4)[7]. Selon l'article 37[8] pour les autorités ou organismes publics qui traitent des données à caractère personnel. Selon le point 2, les petites et moyennes entreprises peuvent s'organiser en groupe et désigner un unique délégué à la protection des données.

5.2. Identifier les points sensibles

Pour les entreprises de toute taille, les questions suivantes peuvent aider à identifier les points de difficultés dans la mise en place :

- Quelles données concernées par la RGDP sont traitées au sein de l'entreprise ?
- Ces données sont-elles suffisamment protégées ? La technologie mise en place correspond-elle au niveau technologique actuel ?
- Au cas où il y aurait atteinte à la protection des données, une notification peut-elle être envoyée en 72 heures aux autorités compétentes ?
- Les clients peuvent-ils recevoir des informations sur les données enregistrées les concernant ? Une suppression de ces données peut-elle être mise en place ?
- Des données sont-elles transférées à d'autres entreprises pour enregistrement ou traitement ? Les contrats de sous-traitance doivent-ils être modifiés ?

5.3. Régulariser les processus d'activité

Les processus d'accès, de collecte et de traitement des données de l'entreprise doivent être mis en conformité avec la nouvelle réglementation. La création de règles de conformité et de guide de bonnes pratiques est une nécessité. Elles seront demandées par les instances de contrôle en cas de fuite de données. Ces règles sont principalement d'ordre organisationnel, mais leur bonne application doit être assurée techniquement. Dans ce cadre, une gestion des droits d'utilisation des NTIC doit être assurée. Interdire la connexion de supports de stockage externes sur les terminaux, bloquer les services de Cloud privés (DropBox, Drive…) et les Webmails personnels sont par exemple quelques-unes des règles à prendre en compte afin de limiter les risques de vol de données au sein de l'entreprise. La gestion des habilitations et des accès aux bases de données est une autre démarche à mettre en place. La journalisation des accès et des activités sur les bases de données sont aussi nécessaires.

[6] https://www.cnil.fr/sites/default/files/atoms/files/check_list.pdf
[7] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article21
[8] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article37

5.4. Sécuriser l'infrastructure

La sécurisation du réseau est un autre point important. La check-list de la CNIL invite les entreprises à vérifier la présence d'antivirus et de pare-feu sur les postes et serveurs du réseau. Une gestion sérieuse des mises à jour de sécurité est également conseillée. De nombreuses fuites de données sont rendues possibles par des vulnérabilités dans les systèmes et bases de données. Pour être sûr que les applications et les systèmes d'exploitation sont à jour, un système de gestion et de déploiement des correctifs est nécessaire. Enfin, la sauvegarde des données est également à prendre en compte : sa fréquence, afin d'en assurer une accessibilité en cas de problème, et sa sécurisation afin d'en éviter le vol.

6. Quelle solution pour la RGDP ?

6.1. Organisation et processus

Remplir les exigences de la RGDP repose à 80 % sur des questions juridictionnelles et organisationnelles. Quels sont les risques légaux de la RGPD pour l'entreprise en cas de perte de données et comment se mettre en conformité avec les exigences en termes de collecte (consentement) et de traitement (droit à l'oubli, désabonnement, demande d'accès aux données, etc.).

6.2. Protection des données

En fonction des risques juridiques et des contraintes organisationnelles définies préalablement, il conviendra alors de choisir le système de protection de données adéquat. Les techniques de protection des données reposent sur trois principes : l'anonymisation, la pseudonymisation et le chiffrement [9].

L'anonymisation consiste à ôter de manière irréversible toute information pouvant identifier un individu. Par exemple, pour un site de vente en ligne, cela équivaudrait à seulement conserver l'identifiant anonyme (pas une adresse email) et le mot de passe du client, les autres informations étant effacées. Une démarche difficile dans le cadre de livraison postale.

Plusieurs techniques de pseudonymisation sont possibles. Le principe général étant de décorréler volontairement les informations personnelles entre elles. Pour le site de vente en ligne, cela équivaudrait alors à mélanger selon un algorithme prédéfini et connu les informations du client. Ainsi, en cas de perte de la base de données, l'identifiant, le nom et l'adresse postale étant mélangés, sans connaître l'algorithme il sera impossible de connaître la véritable adresse postale correspondant au nom ou à l'identifiant d'un client.

Le chiffrement quant à lui consiste à garantir la confidentialité de l'information par procédé cryptographique. Celui-ci sera par exemple utilisé lors d'échange de données entre différents

[9] https://www.cnil.fr/sites/default/files/typo/document/FICHE10_PackConf_LOGEMENT_SOCIAL_web.pdf

acteurs. Des outils tels que OpenPGP[10], GPG[11] ou Gpd4win[12] permettent d'assurer un chiffrement des données.

Le groupe de travail du G29 sur la protection des personnes à l'égard du traitement des données à caractère personnel propose un guide sur les techniques d'anonymisation [13]

6.3. Protection des systèmes

En complément de cet ensemble de mesures, G DATA vient assurer la sécurité des systèmes et le respect des directives.

La solution G DATA multicouche garantit la sécurisation des terminaux fixes et mobiles ainsi que des serveurs contre les malwares et les attaques.

Avec Policy Management, les droits d'utilisation des postes et des serveurs sont maîtrisés. Les supports de stockage externes peuvent être bloqués afin d'éviter les vols de données dans l'entreprise.

Avec Patch Management les correctifs sur les systèmes et les programmes tiers sont appliqués de manière régulière, évitant ainsi les risques d'exploitation de failles de sécurité.

Plus d'informations sur les solutions pour entreprises G DATA sur https://www.gdata.fr/entreprises

Veuillez noter que ce Whitepaper a été conçu comme une réflexion sur les répercussions possibles de la RGDP et ne remplace pas une lecture complète des textes de loi.

[10] openpgp.org/
[11] https://gnupg.org
[12] https://www.gpg4win.org/
[13] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf