REUNION D'INFORMATIONS RGPD

Maison des Associations de TOURCOING

AXIS EXPERTS CONSEILS
Expertise comptable • Conseil • Audit

Partie 1 : Principes du RGPD

Le règlement n° 2016/679, dit règlement général sur la protection des données (RGPD), constitue le texte de référence **européen** en matière de protection des données à caractère personnel.

Le RGPD renforce et unifie la protection des données pour les individus au sein de l'Union européenne et a été publié le 27 avril 2016.

Le nouveau **règlement européen sur la protection des données personnelles** paru au journal officiel de l'Union européenne est entré en application :

le 25 mai 2018

Le Règlement Général Européen sur la Protection des Données (RGPD) définit six principes de protection des données que les associations doivent suivre lors de la collecte, du traitement et du stockage des données personnelles des individus. Le responsable du traitement des données est chargé de faire respecter ces principes et doit pouvoir démontrer les pratiques de conformité de l'association.

S'agissant des **amendes administratives**, elles peuvent s'élever, selon la catégorie de l'infraction, entre **de 10 ou 20 millions d'euros si rétractation.** Elle est calculé **de 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial en premier lieu sinon calcul ci-dessus**.

Principes du RGPD

Vous trouverez ci-dessous les six principes ainsi que des conseils sur la meilleure façon de les suivre.

✓ Légitimité, honnêteté et transparence

Le premier principe est relativement évident : les associations doivent s'assurer que leurs pratiques de collecte des données ne violent pas la loi et qu'elles ne cachent rien aux personnes concernées.

Afin de rester légitime, vous devez avoir une compréhension approfondie du RGPD et des règles de collecte des données. Vous devez indiquer le type de données collectées ainsi que la raison pour laquelle vous les collectées dans votre politique de confidentialité afin de rester transparent avec les personnes concernées.

✓ Limitation du traitement

Les associations ne doivent collecter des données personnelles qu'à des fins spécifiques, indiquer clairement leur objectif et ne conserver les données que pour une durée nécessaire afin d'atteindre cet objectif.

Le traitement effectué à des fins d'archivage dans l'intérêt public ou à des fins scientifiques, historiques ou statistiques bénéficie de plus de libertés.

Principes du RGPD

✓ **Minimisation des données**

Les associations doivent uniquement traiter les données personnelles dont elles ont besoin afin d'atteindre l'objectif initial. Cela présente deux avantages majeurs. Tout d'abord, en cas de violation de données, la personne non-autorisée n'aura accès qu'à une quantité limitée de données. Deuxièmement, la minimisation des données permet de conserver des données exactes et à jour.

✓ **Exactitude**

L'exactitude des données personnelles fait partie intégrante de la protection des données. Le RGPD stipule que « toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder. »

✓ **Limitation de stockage**

De la même manière, les associations doivent supprimer les données personnelles lorsqu'elles ne sont plus nécessaires au traitement.

Principes du RGPD

Comment savoir lorsque les données ne sont plus nécessaires ?

La réponse à cela variera selon l'industrie et les raisons pour lesquelles les données sont collectées. Toute association n'étant pas certaine de la durée de conservation des données personnelles devraient consulter un spécialiste.

✓ **Intégrité et confidentialité**

Ce principe est le seul traitant explicitement la problématique de sécurité. Le RGPD indique que les données à caractère personnel doivent être « traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. »

Le RGPD est délibérément vague quant aux mesures que les associations devraient prendre, car les meilleures pratiques technologiques et organisationnelles évoluent constamment. Actuellement, les entreprises devraient crypter et/ou pseudonymiser les données personnelles dans la mesure du possible, mais devaient également considérer toutes les autres options qui pourraient convenir.

Partie 2 : Les Notions à retenir

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

Cette notion est définie à l'article 4 du RGPD. Il s'agit de toute information se rapportant à une personne physique identifiée et identifiable.

Une personne physique identifiable est une personne physique qui peut être identifiée, directement ou indirectement, par référence à un identifiant, tel qu'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.

Exemples de données personnelles classiques : les données d'identification comme le nom, le prénom, le sexe, les initiales, la date et lieu de naissance … , l'adresse IP ou l'adresse MAC, la situation familiale, la situation militaire, la formation, les diplômes, les distinctions, l'adresse, les caractéristiques du logement, la vie professionnelle, la situation économique et financière, les moyens de déplacement des personnes, l'utilisation des médias et les moyens de communication.

Les Notions à retenir

Qu'est-ce qu'une donnée sensible ?

Il s'agit des origines raciales ou ethniques, des opinions politiques, philosophiques ou religieuses, des appartenances syndicales des personnes, des données biométriques aux fins d'identifier une personne de manière unique, des données concernant la santé, des données génétiques, des données concernant la vie sexuelle ou l'orientation sexuelle, des données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes (articles 9 et 10 du RGPD).

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

Il s'agit de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensemble de données telles que 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, la limitation, l'effacement ou la destruction (article 4 RGPD). Les fichiers papier entendus comme « tout ensemble structuré de données à caractère personnel, accessibles selon des critères déterminés », constituent donc des traitements de données au sens du RGPD.

Les Notions à retenir

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

Il s'agit de la personne, l'autorité publique, la société ou l'organisme qui décide de la création du traitement et détermine les finalités et les moyens de celui-ci (article 4 RGPD).

Qu'est-ce qu'un responsable conjoint de traitement ?

Le RGPD créé la notion de responsable conjoint de traitement. Celui-ci assume une responsabilité solidaire avec le responsable de traitement vis-à-vis des personnes physiques dont les données sont traitées. Le contrat liant les deux responsables peut cependant répartir différemment les rôles et responsabilités.

Les Notions à retenir

Qu'est-ce qu'un sous-traitant ?

Toute personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (article 4 RGPD). Ces données sont traitées sur instruction du responsable de traitement et il n'y a pas d'utilisation des données pour son propre compte (par exemple, le prestataire qui établit les bulletins de paies des salariés de son client sur la base d'instructions claires données par le client et définies dans la lettre de mission : qui payer, quels montants, à quelle date etc.

Il s'agit donc par exemple des prestataires de services informatiques (hébergement, maintenance, …), des intégrateurs de logiciels, des sociétés de sécurité informatique, des sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données, des prestataires de service (agences de marketing ou de communication, distributeurs, …) qui traitent des données personnelles pour le compte de leurs clients.

Les Notions à retenir

Qu'est-ce qu'un DPO ?

Le délégué à la protection des données (DPD) ou le data protection officer (DPO), est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné.

Il est ainsi chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés, de contrôler le respect du règlement et du droit national en matière de protection des données, de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution, de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Sa désignation est obligatoire pour les autorités ou les organismes publics, les responsables de traitement ou sous-traitant dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle, ou dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.

Partie 3 : Etapes du RGPD

1. Désigner une personne responsable des données personnelles au sein de votre association

Il vous faut désigner une personne qui interviendra sur ce sujet pour votre structure et qui sensibilisera l'ensemble du personnel sur la protection des données personnelles au travers de réunions d'information et de formations régulières.

Certaines structures ont par ailleurs l'obligation de désigner un délégué à la protection des données personnelles - DPO. (Voir Définition dans la partie 1 de la documentation)

Etapes du RGPD

2. Cartographier les domaines concernés et les différents traitements de données

NOM DU TRAITEMENT	LISTE DES DONNEES PERSONNELLES COLLECTEES	LISTE DES DONNEES PERSONNELLES NECESSAIRES	DUREE CONSERVATION INFORMATION	PERSONNES UTILISANT CES DONNEES	NOM SOUS TRAITANT	COMMENTAIRE

Si votre structure identifie des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées (notamment les traitements de données sensibles (Voir définition partie 1 de la documentation) et les traitements reposant sur le profilage (Voir définition ci-dessous)), il faudra obligatoirement réaliser une étude d'impact sur la protection des données (Privacy Impact Assessment PIA – article 35 du RGPD).

Le profilage a donc pour but de collecter des informations sur un individu ou un groupe d'individus afin d'analyser leurs caractéristiques et leurs comportements pour les placer dans une certaine catégorie et/ou de prédire ou d'évaluer certaines de leurs caractéristiques tels que la capacité à réaliser une tâche, leurs intérêts, ou anticiper leur comportement.

Etapes du RGPD

3. Réaliser un audit technique et un audit des prestataires

L'audit technique de votre organisation a pour objectif d'évaluer le niveau de sécurité des applications clés en conformité avec les exigences du RGPD.

L'audit technique peut être limité aux différents systèmes et processus impliqués dans la collecte, la transmission, la conservation ou le traitement des données personnelles. Il peut être utile de regarder les systèmes d'information et de communication utilisés dans l'association sans forcément que la direction en ait connaissance (fichiers stockés localement par les salariés, clouds personnels etc.).

Lors de cette évaluation du niveau de sécurité, il faut prendre en compte les risques de destruction, de perte, d'altération, de divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou de l'accès non autorisé à ces données de manière accidentelle ou illicite.

L'audit des prestataires est également indispensable.

Etapes du RGPD

La structure doit renforcer son contrôle et vérifier le niveau de sécurité et de conformité des sous-traitants en se faisant remettre une attestation de conformité au RGPD.

Il permet à la structure d'obtenir des informations sur les mesures mises en place par le sous-traitant en matière de gestion des données, de contrôle des accès, de protection des équipements et des réseaux.

Il permet d'identifier et ensuite de réduire les risques liés aux transmissions des données.

4. Arrêter un plan d'action

Votre structure après avoir réalisé ces audits est en mesure de déterminer les actions à mettre en œuvre pour respecter les nouvelles règles du RGPD et diminuer les risques pesant sur votre organisation.

Il faut que vous vous assuriez notamment que seules les données strictement nécessaires à la poursuite de l'objectif du traitement sont collectées et traitées. Il faut en conséquence revoir les mentions d'information à destination des personnes physiques afin qu'elles soient conformes aux exigences du RGPD, les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement etc.)

Etapes du RGPD

5. Documenter l'ensemble des actions et procédures prouvant votre conformité au RGPD

Il s'agit de répondre à la nouvelle obligation prévue par le RGPD d'accountability (responsabilité). Selon celui-ci il est nécessaire de mettre en oeuvre des mécanismes et procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

La structure doit donc élaborer des procédures internes pour assurer la protection des données tout au long du traitement.

Ces procédures seront mises en place en cas de faille de sécurité, de demandes de rectification ou d'accès, de demande de modification des données collectées, de changement de prestataire etc…

La personne chargée de la protection des données doit établir une politique de protection des données personnelles de l'association.

Afin de prouver la conformité de l'association au RGPD en cas de contrôle, il sera nécessaire de constituer et de regrouper la documentation nécessaire. Il est également important que les procédures et documents réalisés à chaque étape soient réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Partie 4 : Questions

Contacts

Maison des Associations de TOURCOING

100 Rue de Lille

59200 TOURCOING

03 20 26 72 38

contact@mda-tourcoing.fr

Emmanuel TANFIN

Conseiller RGPD

4 Rue de la Cousinerie

59650 VILLENEUVE D'ASCQ

03.28.09.90.70

tanfin@axisconseils.fr

Charte RELATIONS FOURNISSEUR RESPONSABLES

Université de Lille 1 SCIENCES ET TECHNOLOGIES

LUCIE LE LABEL RSE DE REFERENCE

CLUB noé L'économie autrement

Biom attitude

CJD CENTRE DES JEUNES DIRIGEANTS D'ENTREPRISE

CLUB GAGNANTS

PARTENAIRE Ardan PARTENAIRE

AXIS EXPERTS CONSEILS
Expertise comptable • Conseil • Audit

FBC

UNIVERSITÉ CATHOLIQUE DE LILLE

MOUVES MOUVEMENT DES ENTREPRENEURS SOCIAUX

epa

Réseau ALLIANCES
ENTREPRENEURS DE CROISSANCE RESPONSABLE

dirigeants responsables de l'ouest

Entreprise et Progrès