URIOPSS Bretagne

NOTE TECHNIQUE :

Le Règlement Général sur la Protection des Données et son application

Propos introductif :

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. *L'article 8 paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne* disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

De ce fait, le Règlement Général sur la Protection des Données (RGPD) du 27 avril 2016, adopté par le Conseil et le Parlement européen, remplace et étend les dispositions de la Directive 95/46/CE, et est directement applicable depuis le 25 mai 2018, dans tous les pays membres de l'Union européenne afin d'assurer cette protection des données à caractère personnel.

Alors que l'ancienne directive 95/46/CE du 24 octobre 1995 *reposait en grande partie sur la notion de formalités préalables* (déclaration, autorisations), le règlement européen y *substitue une logique de conformité*, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement de la Cnil.

Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne et fixe *de nouveaux droits* prévus *aux articles 15 à 21 du RGPD* (droit de rectification, droit à l'effacement droit à la limitation du traitement, droit à la portabilité des données…) pour les personnes dont les données sont collectées. Par ailleurs, ce texte réglementaire définit de *nouvelles obligations* pour les entreprises, établissements et associations qui collectent ces données.

Les responsables de traitements doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, dès la conception du produit ou du service et de façon continue, ils doivent ainsi être en mesure de démontrer la conformité de leurs traitements à tout moment.

I/ Le champ d'application du RGPD

- **Qui est concerné par le RGPD ?**

Selon l'article 3 du RGPD, tout organisme, quelque soient sa taille, son pays d'implantation et son activité, peut être concerné. En effet, l*e RGPD s'applique à toute organisation, publique et privée*, qui traite des données personnelles pour son compte ou non, dès lors :

- qu'elle est établie sur le territoire de l'Union européenne ;

- que son activité cible directement des résidents européens.

Le RGPD *concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organisme*s, notamment les entreprises *(article 3 du RGPD).*

Les sous-traitants sont soumis à des obligations particulières : protection des données personnelles et de la vie privée dès la conception de leur service ou de leur produit, conseil auprès de leurs clients, tenue d'un registre des activités de traitement effectuées pour le compte de leurs clients. Le contrat de sous-traitance doit prévoir une clause spécifique sur la protection des données personnelles.

Le responsable du traitement, selon l'article 4 du RGPD, est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement et sur lequel reposent les obligations prévues par le règlement. Pour notre secteur cela peut donc être l'association, la fondation ou la congrégation par exemple.

La personne concernée par un traitement est celle à laquelle se rapportent les données objet du traitement. Pour notre secteur cela peut donc être les usagers, les salariés ou encore les bénévoles ou personnes extérieures en lien avec l'association, la fondation ou la congrégation.

Le destinataire d'un traitement, *au titre de l'article 4 du RGPD*, est toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers, ce dernier s'entendant de toute personne autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel. Pour notre secteur cela peut donc être le cas lorsqu'une association communique des données à caractère personnel à une autre association, fondation ou congrégation.

- **Qu'est-ce qu'une donnée personnelle ?**

Au titre de l'article 4 du RGPD, une *« donnée personnelle »* est *« toute information se rapportant à une personne physique identifiée ou identifiable* ».

A noter :
Un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.

Une personne peut être identifiée :

- directement (exemple : nom, prénom)
- ou indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : numéro de sécurité sociale)
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour…)

A noter : Les adresses IP et Mac constituent des données personnelles (voir à propos d'une adresse IP : Cass. 1e civ. 3-11-2016 n° 15-22.595 FS-PB).

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

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par

transmission diffusion ou toute autre forme de mise à disposition, rapprochement*) selon l'article 4 du RGPD*.

Exemple : tenue d'un fichier des usagers, collecte de coordonnées de prospects via un questionnaire, etc.

Un traitement de données doit avoir un objectif, une finalité, pour valablement pouvoir être constitué. Une association, fondation ou congrégation ne peut pas collecter ou traiter des données personnelles simplement au cas où cela lui serait utile un jour. A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle menée. Cela conduit à s'interroger sur la pertinence des données collectées.

Exemple : une association collecte sur ses usagers ou résidents de nombreuses informations afin d'assurer une prise en charge personnalisée et adaptée aux besoins des individus. Toutes les opérations sur ces données constituent un traitement de données.

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

A noter que *l'article 6 du RGPD* prévoit notamment qu'un *traitement de données personnelles est licite* dès lors que *la personne concernée a consenti* au traitement de ses données à caractère personnel.

II/ La démarche à suivre pour une mise en conformité

Les données à caractère personnel doivent être (*RGPD, art. 5.1*) :

- traitées de manière licite, loyale et transparente au regard de la personne concernée ;

- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;

- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

- exactes et tenues à jour ;

- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

- 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 (intégrité et confidentialité).

Concrètement, les différentes actions à mener pour se conformer à ces principes sont les suivantes :

- désigner un pilote au sein de l'association, la fondation ou la congrégation ;

- recenser les fichiers concernés ;

- ***repérer les traitements à risque*** ;

Les critères permettant de caractériser les types de traitements susceptibles de présenter un risque élevé défini par le RGPD ont été affinés par le Comité européen de la protection des données, qui rassemble des représentants des différentes autorités nationales de contrôle. Ainsi sont considérés comme à risques les traitements ayant pour objet ou pour effet : l'évaluation d'aspects personnels ou

la notation d'une personne, une prise de décision automatisée, la surveillance systématique de personnes (exemples : la télésurveillance, la surveillance des réseaux sociaux des salariés, l'analyse des pages des réseaux sociaux des candidats à un emploi, les outils de gestion du temps de présence, les systèmes de géolocalisation), le traitement de données sensibles sont considérées comme des données sensibles les données révélant l'origine prétendument raciale ou ethnique, portant sur les opinions politiques, philosophiques ou religieuses, relatives à l'appartenance syndicale, concernant la santé ou l'orientation sexuelle, les données génétiques ou biométriques, les données d'infraction ou de condamnation pénale, le traitement à grande échelle de données personnelles , le croisement d'ensembles de données, des usages innovants ou l'application de nouvelles technologies (exemple : objets connectés), l'exclusion du bénéfice d'un droit, d'un service ou contrat.

Si le traitement de données concerné répond à au moins deux critères sur neuf cités ci-dessus, une analyse d'impact sur la protection des données doit être conduite. Cette analyse d'impact a pour objectif de garantir les droits et libertés de chaque individu.

- respecter le droit des personnes visées par les traitements de données personnelles ;

- sécuriser les données ;

- s'assurer, en cas de sous-traitance que le prestataire respecte le RGPD. Sur les obligations des sous -traitants.

- **La désignation d'un DPO**

DPO signifie un « Data protection officer » qui a été traduit en France comme le délégué à la protection des données.

Selon l'article 37 du RGPD, la désignation d'un délégué à la protection des données n'est obligatoire que pour les organisme publics et les entreprises dont l'activité de base les amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites sensibles ou relatives à des condamnations pénales et infractions.

Toutefois, même si l'entreprise n'est pas formellement dans l'obligation de désigner un tel délégué, la Cnil recommande de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen.

Chef d'orchestre de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé *selon l'article 39 du RGPD* :

- 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'entreprise sur la réalisation d'études d'impact sur 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.

Le délégué peut être désigné en interne parmi les salariés de l'entreprise ou en externe (*point 6 de l'article 37 du RGPD*). Il peut aussi être mutualisé entre plusieurs organismes ou au sein d'associations ou fédérations professionnelles.

A noter : La notion de traitement à grande échelle n'est pas définie par le RGPD. La CNIL donne sur ce point les exemples suivants : les traitements gérant les données des voyageurs utilisant les

transports en commun ou ceux relatifs aux données de leurs clients administrés par les banques, les compagnies d'assurance, les opérateurs téléphoniques ou fournisseurs d'accès internet sont des traitements de données à grande échelle.

- **Réaliser un état des lieux et recenser les traitements de données personnelles**

L'obligation de tenir un registre des traitements de données personnelles ne concerne que les entreprises d'au moins 250 salariés au titre de *l'article 30 du RGPD* mais la CNIL en préconise la réalisation de manière plus large.

L'objectif est d'identifier les activités principales de l'entreprise qui nécessitent la collecte et le traitement de données (exemples en ce qui concerne la gestion des ressources humaines : le recrutement, la gestion de la paie, la formation, les déclarations sociales obligatoires, la gestion des badges et des accès, etc.).

Selon l'article 30 du RGPD, il s'agit de répertorier pour chaque activité recensée :

- le responsable du traitement ;

- l'objectif poursuivi ;

- les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;

- qui a accès aux données (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;

- la durée de conservation de ces données (durée pendant laquelle les données sont utiles d'un point de vue opérationnel et durée de conservation en archive).

Le registre est placé sous la responsabilité du dirigeant de l'entreprise. La Cnil en propose un modèle sur son site Internet.

Selon la CNIL, il n'est pas nécessaire de répertorier dans ce registre les traitements purement occasionnels.

Pour chaque traitement, il conviendra de vérifier :

- quelles ont été les circonstances de collecte des données : y-a-t-il eu consentement des personnes concernées ? Dans la négative la collecte répond-elle à des obligations particulières (collecte nécessaire au contrat, respect d'une obligation légale, par exemple le traitement de données relatives aux salariés pour les communiquer à la sécurité sociale ou l'administration fiscale…) ? ;

- quelle a été l'information délivrée aux personnes faisant l'objet de la collecte et du traitement : celles-ci ont-elles été informées de la finalité du traitement et de leurs droits ? ;

- la nature des données collectées au regard de la finalité du traitement : seules les données strictement nécessaires au traitement peuvent être collectées et traitées.

- que seules les personnes habilitées ont accès aux données dont elles ont besoin et que les données ne sont pas conservées au-delà de ce qui est nécessaire.

Certains traitements réclament une vigilance particulière. Il s'agit des ***traitements considérés à risque*** définis précédemment.

III/ Les mesures coercitives en cas de non-respect du RGPD

- **Quelle est l'autorité chargée d'assurer le respect du RGPD ?**

La Commission nationale de l'informatique et des libertés (CNIL) est l'autorité chargée du contrôle de l'application du RGPD et de veiller au respect et à l'application conforme du RGPD. Le RGPD suit pour cela une logique de contrôle.

La CNIL a donc un devoir de vigilance, de dissuasion et de fermeté vis-à-vis des manquements des responsables de traitements et des sous-traitants. Pour se faire, elle a à présent le droit d'imposer elles-mêmes des *sanctions administratives* (sous réserve de respecter certaines conditions exposées à *l'article 83 du RGPD*). Elle doit également s'assurer que les sanctions administratives prévues en cas de manquements au RGPD sont effectives, proportionnelles et dissuasives. Elle doit choisir le moyen le plus apte à atteindre l'objectif recherché : la mise en conformité de l'activité des entreprises et organismes au RGPD (voir les articles 57 et 58 du RGPD pour plus de précisions).

- **Quels sont les types de sanctions encourues ?**

L'ensemble des sanctions administratives auxquelles s'exposent les établissements en cas de non-conformité au RGPD sont exposées à *l'article 83 de ce règlement*.

Ces sanctions administratives peuvent se présenter sous forme de :

- ✓ *Sanctions financières* : amendes administratives pouvant s'élever jusqu'à 20 millions d'euros 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.

- ✓ *Des demandes d'indemnisation* : toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant, réparation du préjudice subi (les citoyens peuvent se faire représenter par des organismes spécialisés dans la protection des données ou profiter de la nouvelle possibilité d'actions de groupe, introduite par la loi pour la république numérique, recours collectifs qui n'étaient auparavant autorisés que dans les domaines de la santé et de l'environnement).

A noter que les Etats membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues *à l'article 83*, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont *effectives, proportionnées et dissuasives*.

Sources juridiques :

- https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
- https://www.cnil.fr/fr/rgpd-en-pratique
- https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000033346676
- https://www.cnil.fr/fr/fiches-pratiques