CHANTIER ecole
RÉSEAU NATIONAL
Les entreprises sociales apprenantes

Règlement Général de Protection des Données (RGPD) – Eléments de repère

Le RGPD, adopté par le Parlement Européen en avril 2016, entrera en application le 25 mai. En sa qualité de règlement européen, son application dans les Etats membres est immédiate (malgré l'adoption attendue, en France, de la loi informatique et libertés adaptée à ce nouveau cadre). Il est évoqué une possible tolérance sur un délai de mise en conformité de 2 ans, qui pourrait être négocié entre la CNIL et les organisations concernées, dès lors que celles-ci apportent la preuve qu'un plan d'action existe et qu'il est suivi (existence d'un registre (voir plus bas), les mesures de protection déployées/bonnes pratiques et la vérification qu'elles sont bien faites). Par ailleurs, il semble que CNIL ait une approche bienveillante envers le secteur associatif.

Une donnée à caractère personnel désigne toute donnée qui « désanonyme » une personne que ce soit de façon directe (nom, adresse, et toute information se rapportant aux données d'identification) ou de façon indirecte : un traitement statistique peut avoir pour effet de produire un nombre de résultats restreints, portant un risque pour l'anonymat des personnes.

Une donnée sensible désigne une donnée à caractère personnel ayant trait aux croyances religieuses, opinions politiques, à la santé, une condamnation judiciaire…

A l'exception de rares cas, toute organisation est concernée, une association employeuse l'est pour le traitement des données se rapportant aux salariés, bénévoles, adhérents et bénéficiaires. En notant que le traitement d'un nombre d'entre elles peut être délégué à un prestataire (par exemple : plate-forme de routage pour laquelle prévoir des mesures de vérification par le prestataire, comme le retrait régulier d'adresses pour les personnes ne souhaitant plus être destinataires de diffusions).

Le RGPD introduit 8 grands principes directeurs pour la mise en conformité des entités concernées, on peut citer ceux qui de notre point de vue, sont les plus caractéristiques :

La limitation des finalités : les données personnelles ne peuvent être obtenues que pour des « finalités déterminées, explicites et légitimes ».

La minimisation des données : les données recueillies sur un sujet doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement ».

La responsabilité : le responsable du traitement des données (celui qui les recueille) est responsable de sa mise en conformité. Il lui appartient de prendre toutes les mesures nécessaires pour garantir la protection des données, la déclaration préalable à la Cnil est supprimée, remplacée par d'autres obligations reposant sur l'autocontrôle.

Parmi les principales nouveautés introduites :

Le renforcement des droits des personnes : est rendu obligatoire le recueil et la conservation du consentement au traitement des données personnelles ; sont reconnus les droits d'accès aux données, de rectification, à la portabilité, de retrait du consentement des personnes.

Des sanctions lourdes : le RGPD met en place des sanctions dissuasives, pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial d'une organisation (Il semblerait que l'Union Européenne cible des types d'entreprises pour ses sanctions lourdes, notamment les GAFAM).

Les mesures de protection des données sont de différentes natures : juridique, technique, organisationnelles et logiques.

Afin de prendre la mesure des dispositions à prendre, nous prenons comme référence, le guide des 6 étapes de mise en conformité réalisé par la CNIL.

Etape 1 : La désignation d'un délégué à la protection des données (DPO)

La désignation d'un DPO est obligatoire pour les organismes publics et les entreprises traitant de données à grande échelle ou des données sensibles. Toutefois, en dehors des cas soumis à l'obligation, il est fortement recommandé de désigner une personne, chargée de s'assurer de la mise en conformité, et correspondre avec les autorités de protections de données.
Cette personne, référente technique, doit être en mesure d'informer et conseiller les décideurs sur les obligations et leurs impacts, réaliser l'inventaire de traitement des données (à l'aide ou non d'un accompagnement, dans ces étapes de mise en place du dispositif), piloter la conformité en continu.
Cette fonction peut être externalisée et/ou mutualisée.

Etape 2 : Cartographier les traitements de données personnelles

Il s'agit de **recenser** tous les traitements de données personnelles assurés, de les **répertorier** et les **caractériser** au moyen d'un registre complet : Quelles sont les catégories de données traitées ? où sont-elles stockées ? Lesquelles sont sensibles ? Jusqu'à quand les conserver ? Pourquoi les traiter (finalité) ? Qui en sont les destinataires ? Par exemple, la Gestion du personnel est une catégorie de traitement (recensement par finalité principale), au sein de laquelle, les données seront traitées différemment selon qu'il s'agit de la gestion des recrutements ; de la gestion de paie. La caractérisation se fera pour chacune de ces sous-catégories.

↳ ***A quels services et ressources puis-je avoir accès pour être appuyé dans la réalisation de cet état des lieux ?***

Modèle de liste des traitements

Identification du traitement				Acteurs	Finalité du traitement	Transferts hors UE ?	Données sensibles ?
Nom / sigle	N° / REF	Date de réation	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui /non	Oui/non

Registre - Modèle de Fiche

Description du traitement	
Nom / sigle	
N° / REF	ref-000

Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images...		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		

Données sensibles	Description	Délai d'effacement
Données révèlant l'origine raciale ou ethnique		
Données révèlant les opinions politiques		
Données relatives à des condamnations pénales ou infractions		

Numéro d'identification national unique (NIR pour la France)		

Catégories de personnes concernées	Description
Catégorie de personnes 1	
Catégorie de personnes 2	

Destinataires	Description	Type de destinataire	
Destinataire 1			
Destinataire 2			
Destinataire 3			
Destinataire 4			

Etape 3 : Prioriser les actions

Après avoir identifié les traitements de données assurés, il s'agit d'identifier les actions à mener pour se conformer au RGPD. Ces actions sont à prioriser, notamment au regard des risques que font peser ces traitements sur les libertés des personnes. Les actions communes à tous les traitements de données sont les suivantes : identifier la base juridique sur laquelle se fonde le traitement/recueil (consentement de la personne ; intérêt légitime, contrat) ; les mentions d'information ; vérifier que ses sous-traitants connaissent, par clauses contractuelles, leurs nouvelles obligations en matière de confidentialité et protection des données ; prévoir les modalités d'exercice des droits des personnes concernées (accès, rectification de données…) ; vérifier les mesures de protection/sécurité mises en place.

↳ ***Comment être sûr d'avoir envisagé toutes les mesures requises, les moyens nécessaires pour leur suivi, et que cela soit proportionné aux enjeux de protection de données dans mon organisation ?***

Etape 4 : Gérer les risques

S'il a été identifié des traitements de données **susceptibles d'engendrer des risques élevés pour les libertés, une étude d'impact doit être menée pour chacun de ces traitements**.
Cette étude porte sur une appréciation de ces risques, les mesures à prévoir pour traiter ces risques…$

↳ ***Dans la mesure où des données sensibles sont traitées pour l'accompagnement des personnes, mon organisation peut-elle être concernée par l'étude d'impact?***

Etape 5 : Organiser les processus internes

Pour la mise en œuvre efficace des actions, mettre en place des procédures internes garantissant la protection des données à tout moment, tenant compte des évènements qui peuvent survenir au cours de la vie d'un traitement de donné (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, changement de prestataires…). Les mesures et process doivent être prévus **dès la conception** d'un traitement de données (toutes les mesures à envisager tout au long du traitement : minimisation de la collecte, consentement, sécurité et confidentialité, s'assurer du rôle et de la responsabilité des acteurs impliqués).

↳ ***Quels sont les process organisationnels adaptés ? Comment puis-je être appuyé dans leur détection et leur mise en place?***

Etape 6 : Documenter la conformité

Regrouper toute la documentation d'appui pour la mise en conformité et les pièces afférentes aux actions réalisées : registre des traitements ; analyse d'impact des traitements comportant des risques élevés ; mentions d'information des personnes, modèles de recueil de consentement ; procédures prévues pour l'exercice des droits des personnes ; les contrats définissant les rôles et les responsabilités des acteurs (clauses envers les sous-traitants …).