Mise en place de la documentation relative à la protection des données personnelles au titre du principe d'« Accountability »

Le RGPD a posé le principe de responsabilisation des acteurs. A ce titre, les organismes, traitant des données, ont moins de formalités préalables à la mise en œuvre d'un traitement à effectuer auprès de la CNIL. Mais ils doivent, en contrepartie, être en mesure de démontrer qu'ils respectent la règlementation relative à la protection des données.

Pour s'assurer du respect de la règlementation, il est nécessaire de mettre en place des procédures et de politiques de protection des données, notamment qui définiront les étapes à effectuer pour être conforme.

Les documents listés ci-dessous permettront de s'assurer que l'organisme dispose des éléments essentiels concernant la protection des données. Cette liste n'est pas exhaustive.

1. Procédure générale de protection des données

Cette procédure contient l'ensemble des principes nécessaires pour garantir la mise en œuvre de traitements équitables et transparents, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées.

Elle indique notamment :

- les coordonnées de l'organisme

- les coordonnées du délégué à la protection des données

- les engagements de l'organisme concernant le respect des principes du RGPD concernant

- la mise en œuvre de traitements licites,

- le respect des droits des personnes,

- les éventuels transferts vers un pays tiers,

- les destinataires des données collectées,

- la durée de conservation des données collectées,

- les mesures de sécurité des données.

La procédure doit prévoir une revue régulière des mesures techniques et organisationnelles afin de s'assurer qu'elles sont toujours adaptées aux risques présentés par les traitements pour les personnes concernées.

La procédure doit prévoir également que les mesures techniques, organisationnelles et de mise en conformité, sont régulièrement testées, analysées et évaluées, afin de vérifier leur efficacité.

Chaque traitement de données doit être mis en place en respectant la règlementation relative à la protection des données, et doit donc notamment respecter les points suivants :

- de finalité du traitement,
- de proportionnalité du traitement au regard de la finalité,
- de minimisation des données collectées au regard de la finalité,
- de licéité du traitement,
- de sécurité des données collectées,
- de durée de conservation des données collectées,
- de destinataires des données collectées,
- d'encadrement des relations avec les sous-traitants,
- d'information claire et préalable des personnes concernées de conditions d'exercice des droits des personnes,
- et le cas échéant d'encadrement des transferts de données hors Union européenne.

Le respect de ces principes pour chaque traitement est documenté par l'organisme.

2. Politique de confidentialité

La politique de confidentialité est destinée à informer les personnes extérieures à l'organisme dont les données sont traitées de la façon dont l'organisme traite leurs données et applique la règlementation en matière de protection des données et ce, dans un format concis, transparent, compréhensible et aisément accessible. La politique de confidentialité reprend notamment les informations prévues à l'art. 13 et 14 du RGPD.

3. DPO

a. Sélection du DPO

Le DPO désigné l'est sur la base de qualités professionnelles, connaissances juridiques spécialisées et pratiques en matière de protection des données requises, et de ses connaissances des activités et du secteur de l'organisme.
Il dispose des ressources et des conditions de travail nécessaires pour exercer ses missions.

Sa fonction est incompatible avec certaines fonctions au sein de l'organisme.

La fiche de poste réalisée par l'AFCDP est disponible sur la plateforme Le Coin du DPO (document « fiche de poste du DPO »).

La CNIL a établi une liste de questions à se poser pour la désignation d'un DPO disponible sur la plateforme Le Coin du DPO (« questions à se poser pour la désignation d'un DPO »).

b. Désignation

La lettre de mission du DPO définit ses missions, ses ressources et son mode de reporting. Elle est signée par la direction de l'organisme.

Le récépissé de la désignation du DPO : Le DPO doit avoir été désigné auprès de la CNIL.

Les membres de l'organisme sont informés de l'existence du DPO, par exemple par la publication de la lettre de mission.

La lettre de mission réalisée par l'AFCDP, et celle de la CNIL sont disponibles sur la plateforme Le Coin du DPO (document « lettre de mission DPO AFCDP » et « lettre de mission DPO CNIL »).

c. Missions

Les missions du DPO comprennent a minima :

- informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;

- contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution ;

- coopérer avec l'autorité de contrôle ;

- faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable, et mener des consultations, le cas échéant, sur tout autre sujet.

Le DPO doit reporter directement au niveau le plus élevé de la direction de l'organisme.

4. Registre de traitement

a. **Si l'organisme est responsable de traitement**

Un registre des activités de traitement, est tenu par l'organisme (par le DPO ou par quelqu'un d'autre) comprenant, a minima par traitement :

- nom et coordonnées du RT, co-RT le cas échéant, du représentant du RT et du DPO ;
- les finalités du traitement ;
- une description des catégories de personnes concernées ;
- une description des catégories de données à caractère personnel ;
- la durée de conservation associée à chaque catégorie de données ;
- les catégories de destinataires, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale (y compris leur identification) ainsi que les documents attestant de l'existence de garanties appropriées ;
- une description des mesures de sécurité techniques et organisationnelles ;
- l'existence ou non d'une sous-traitance (avec contrat de sous-traitance)

b. **Si l'organisme est sous-traitant**

- nom et coordonnées du (ou des) sous-traitant(s) et de chaque RT, ainsi que, le cas échéant, les noms et coordonnées du représentant du RT ou du ST, et du DPO ;
- les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
- les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale (y compris leur identification) ainsi que les documents attestant de l'existence de garanties appropriées ;
- une description des mesures de sécurité techniques et organisationnelles.

Un modèle de registre de traitement en tant que Responsable de traitement , ainsi qu'un modèle de registre de traitement en tant que sous-traitant, établis sur la base de celui de la CNIL est mis à disposition sur la plateforme le Coin du DPO (document « Modèle de registre de traitement », et « Modèle de registre de traitement en tant que sous-traitant »)

5. **Analyse d'impact**

Pour chaque traitement, il est nécessaire de vérifier la nécessité de réaliser une analyse d'impact :

- vérifier si le traitement figure sur la liste des traitements nécessitant la réalisation d'une AIPD, ou sur la liste des traitements ne nécessitant pas la réalisation d'une AIPD(délibération n°2019-118 du 12 sept 2019 Liste traitements ne nécessitant pas d'analyse d'impact et délibération n°2018-327 du 11 octobre 2018 liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise)
- si le traitement est réalisé conformément à un référentiel (type méthodologie de référence par exemple), vérifier que le référentiel n'impose pas la réalisation d'une AIPD

- vérifier que le traitement ne rentre pas dans les critères prévus par le CEPD pour les traitements nécessitant la réalisation d'une AIPD (**voir l'infographie « CNIL - Infographie - Dois-je faire une AIPD ? » sur la plateforme Le Coin du DPO**)

L'analyse d'impact relative à la protection des données comprend a minima :

- une description systématique des opérations de traitement envisagées et des finalités, y compris l'intérêt légitime poursuivi,
- une évaluation de la nécessité et de la proportionnalité des opérations de traitements au regard des finalités,
- une évaluation des risques pour les droits et libertés des personnes concernées,
- les mesures envisagées pour faire face aux risques

L'analyse d'impact prévoit la possibilité de demander l'avis des personnes concernées. L'analyse effectuée permet de déterminer les mesures techniques et organisationnelles adaptées au risque présenté par le traitement pour les personnes concernées.

L'analyse d'impact devra être revue régulièrement pour s'assurer de la conformité du traitement, et a minima lorsqu'il y a modification dans la mise en œuvre du traitement pour vérifier le risque présenté par une telle modification.

Un outil d'analyse d'impact est disponible sur le site internet de la CNIL.

6. Sous-traitance

A - Sélection du sous-traitant

Le recours à des sous-traitants est encadré. L'organisme doit sélectionner un sous-traitant qui est en conformité avec la règlementation sur la protection des données.

La mise en place d'une procédure de sélection de sous-traitants permet d'assurer que le sous-traitant auquel il recourt :

- présente des garanties suffisantes concernant la mise en œuvre de mesures techniques et organisationnelles adaptées afin que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes,
- recrute des sous-traitants ultérieurs uniquement sur la base des modalités définies avec le responsable de traitement (autorisation préalable spécifique, ou autorisation générale)

Le recours à des sous-traitants exige la mise en place et conclusion d'un contrat écrit et signé.

Le contrat respecte les prescriptions de l'article 28 du RGPD. Il définit, notamment :

- l'objet

- la durée du traitement
- la nature et la finalité du traitement
- le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et droits du demandeur.

7. Gestion des réclamations et de l'exercice des droits des personnes

L'organisme met en place une procédure de gestion de l'exercice des droits des personnes conforme à l'article 12 du RGPD, comprenant a minima :

- les modalités d'identification/authentification de la personne concernée exerçant ses droits, le cas échéant, son mandataire,
- le respect des délais de réponse, le cas échéant, de prorogation des délais
- les motifs de refus,
- la traçabilité des actions menées.

Si un DPO a été désigné, la procédure prévoit que le DPO supervise la gestion des demandes des personnes concernées relatives au traitement de leurs données et à l'exercice de leurs droits.

La procédure prévoit les modalités de traçabilité des réponses apportées à chaque demande d'exercice de droits permettant de démontrer que les demandes ont été traitées conformément à la règlementation, notamment au travers un tableau de suivi des demandes d'exercice.

Un modèle de registre de suivi des demandes d'exercice des droits est disponible sur la plateforme le Coin du DPO (document « registre des demandes d'exercice de droit »).

8. Gestion des violations de données

L'organisme met en place une procédure de gestion des violations de données, incluant la notification d'une violation de données à caractère personnel à l'autorité de contrôle compétente.

La procédure indiquera le respect du délai de notification dans les 72 heures après en avoir pris connaissance, sauf motifs valables. Si l'organisme est sous-traitant, les modalités de notification au responsable de traitement ainsi que les éléments à transmettre et fixer le délai d'information.

La notification à l'autorité compétente doit comporter a minima :

- la nature de la violation,
- les catégories et nombre de personnes concernées par la violation,
- les catégories et nombre approximatif d'enregistrements de données à caractère personnel concernés,
- le nom et les coordonnées du délégué,
- les conséquences probables de la violation de données,

- ainsi que les mesures prises et/ou à prendre pour remédier ou atténuer les éventuelles conséquences négatives.

En cas de risque élevé, la procédure prévoit les modalités d'informer des personnes concernées dans les meilleurs délais.

Cette information devra comporter a minima :

- la nature de la violation,
- le nom et les coordonnées du DPO,
- les conséquences probables de la violation de données,
- ainsi que les mesures prises ou qui vont l'être pour remédier ou atténuer les éventuelles conséquences négatives.

La procédure devra prévoir le suivi des violations de données, et incidents de sécurité en traçant les incidents, les moyens mis en place afin d'y remédier, ainsi que les actions mise en place (notification ou non de la CNIL, information ou non des personnes concernées).

Un modèle de registre de suivi des violations de données est disponible sur la plateforme le Coin du DPO (document « registre violations de données »).

Date d'édition : 23 août 2024