https://ressources.anap.fr/numerique/publication/2742-comprendre-comment-passer-de-linventaire-au-registre-des-traitements-pour-le-rgpd

Avis d'experts

Passer de l'inventaire au registre des traitements pour le RGPD

Cet avis d'expert donne des indications pratique sur le mode opératoire pour passer d'un inventaire exhaustif de l'existant en termes de traitement de données personnelles à un inventaire des traitements à suivre dans le registre imposé par le RGPD.

Cet avis d'expert a été rédigé par Christian VIALLON, expert dans le collège d'experts de l'ANAP.

Rappels

- Une **donnée à caractère personnel** est définie par le RGPD (Règlement Général sur la Protection des Données) comme « toute information se rapportant à une personne physique identifiée ou identifiable »[1] ;
- Un **traitement de données** est défini comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, 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 »[2] ;
- Une **activité de traitement** de données à caractère personnel s'envisage comme le regroupement en grands blocs logiques et cohérents des traitements de données à caractère personnel lié à un processus métier. Par exemple, si l'on choisit de définir la gestion de l'admission de l'usager comme une activité de traitement, cette activité peut regrouper tous les traitements relatifs à l'instruction de la demande d'orientation, l'information de l'usager, le recueil de ses consentements, l'évaluation des besoins de l'usager, le suivi des orientations et notifications, etc.
- Le RGPD (article 30) institue **le registre des activités de traitement** : le responsable et, le cas échéant, le sous-traitant doivent tenir, sous leur propre responsabilité un registre des traitements[3]. Il s'agit d'une obligation et la CNIL peut demander communication de ce registre. L'absence de registre est susceptible d'être sanctionnée par une amende administrative[4] et/ou par une sanction pénale[5].

Le registre des activités de traitement

Comme rappelé ci-dessus, le RGPD (art. 30) prescrit la mise en place d'un **registre des activités de traitement**. La référence aux « activités » de traitement est importante. L'appellation courante « registre des traitements » donne à penser qu'il s'agit de collationner, « au fil de l'eau », tous les traitements de données à caractère personnel, alors que l'objectif est de les regrouper par grandes activités logiques pour produire un registre lisible, opérationnel et maintenable dans le temps. Par exemple, pour les activités liées aux ressources humaines les entrées de registre peuvent être (voir ci-après) : recrutement, gestion administrative des personnels, gestion des rémunérations, formation, etc.

Ce registre contient au moins toutes les informations suivantes :

- le nom et les coordonnées du responsable du traitement ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
- les délais prévus pour l'effacement des différentes catégories de données ;
- une description générale des mesures de sécurité techniques et organisationnelles.

À retenir : Le registre recense les **activités de traitement** et non les documents ou fichiers qui contiennent des données personnelles. On n'entre donc pas dans le registre en collationnant les supports de données ou les catégories de données, mais en dressant la liste des activités de traitement.

Exemple : les activités de traitement pour les ressources humaines

Dans un projet de document « Référentiel relatif aux traitements de données à caractère personnel mis en œuvre par des organismes privés ou publics aux fins de gestion du personnel »[6]. La CNIL liste les différentes finalités pour lesquels un traitement de gestion du personnel peut être mis en œuvre :

- recrutement sans recours à des outils innovants ;
- gestion administrative des personnels ;
- gestion des rémunérations et accomplissement des formalités administratives y afférentes ;
- mise à disposition du personnel d'outils informatiques ;
- organisation du travail ;
- suivi des carrières et de la mobilité ;
- formation ;
- gestion des aides sociales.

Chacun de ces objectifs peut constituer une entrée dans le registre des activités de traitement. Ainsi le fichier de tableur « gestion des données variables de paie du mois de février 2020 » n'est pas une entrée de registre, mais le traitement des données qu'il contient est englobé dans l'activité « gestion des rémunérations ».

Suivant la taille et les activités de la structure, le registre des traitements comporte entre 15 et 50 entrées. Il est important en effet de s'assurer que le registre peut fonctionner et être maintenu dans le temps. Ouvrir le registre et le renseigner procède d'une démarche organisée qui suppose des prérequis. Il est déconseillé de renseigner le registre « au fil de l'eau » au gré des traitements que l'on rencontre.

Le processus de construction du registre des traitements

La construction du registre s'effectue en 3 étapes

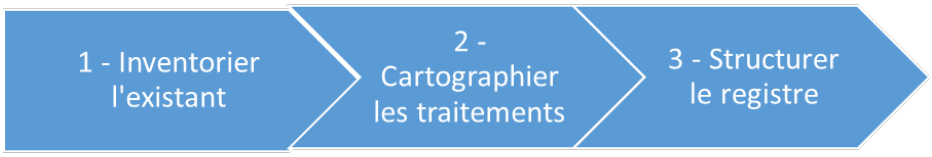

Figure 1 - Processus de construction du registre

Au centre du processus (cf. Figure 1) figure l'étape de la cartographie des traitements qui permet de passer de l'inventaire de l'existant à la réalisation du registre des activités de traitement.

Étape 1 : inventorier l'existant

Cette étape permet de donner à voir de la manière la plus exhaustive possible l'ensemble des traitements de données à caractère personnel qui sont à l'œuvre dans la structure. Deux approches sont possibles pour réaliser cet inventaire : l'approche descendante (« top-down ») ou l'approche ascendante (« bottom-up »).

L'approche descendante

Cette approche est fondée sur la cartographie des processus métiers, lorsqu'elle existe. Cette approche suppose que la structure possède une bonne culture et un solide bagage en matière de cartographie des processus métiers. Idéalement il est nécessaire que l'ensemble des processus métiers ait fait l'objet d'une cartographie raisonnée et normée[7]. On s'efforce alors d'identifier les traitements de données personnelles liés à chacun des processus métier. On confronte ensuite le résultat à la réalité du terrain.

Cette approche est rapide et peu coûteuse, mais elle présente deux inconvénients majeurs :

- Il est rare qu'une cartographie complète des processus métiers ait été réalisée. La cartographie risque donc de présenter des manques et des traitements (comportant parfois des données très critiques) peuvent être oubliés ;
- Si ce travail est mené « en chambre » et n'implique pas suffisamment les acteurs de terrain. Il ne crée donc pas de bonnes conditions pour garantir la sécurité organisationnelle.

L'approche ascendante

Cette approche repose sur l'inventaire exhaustif des traitements existants. Il faut rappeler que ces traitements peuvent être « automatisés ou non », autrement dit être réalisés sur des supports numériques ou sur des supports physiques. Concrètement il s'agit de solliciter l'ensemble des acteurs et d'inventorier, au sein de chaque service, tout ce qui est de l'ordre d'un traitement de données à caractère personnel dans les stations de travail ou dans les bureaux (au sens physique du terme).

Cette démarche peut se faire au moyen d'un tableur sur le modèle ci-dessous (cf. Figure 2)

Document et fichier	Créé par	Etablissement ou service	A quoi sert le document ou fichier ?	Support	Hébergement des données	Le traitement comporte des données sensibles	Personnes concernées (salariés, adhérents, partenaires, etc.)	Durée de conservation	Mesures de protection pour éviter la fuite de données	Circulation des données	Commentaires

Figure 2 - Trame de tableur pour inventaire

Cette approche présente des avantages :

- Elle est complète ;
- Elle associe l'ensemble des acteurs à la démarche et permet donc de les sensibiliser notamment à la sécurité organisationnelle des données ;
- Elle donne une image de l'existant et l'inventaire peut être utilisé :
  - pour mettre en œuvre des plans d'amélioration,
  - lors de l'audit de sécurité,
  - lors de la réalisation du plan d'archivage (si celui-ci n'existe pas).

Mais cette approche présente elle aussi deux inconvénients :

- Elle est longue et coûteuse ;
- Elle est peu attractive et nécessite donc une forte mobilisation des acteurs.

Suivant la taille et l'organisation de la structure, on peut restreindre l'inventaire à un échantillon représentatif des différents métiers et services. Il est possible aussi de programmer des entretiens avec des acteurs métiers. L'inventaire ne peut jamais être exhaustif. Il convient donc de se fixer un objectif, généralement entre 70 à 80 % des traitements supposés exister. Le but est d'avoir une image fidèle et représentative. L'intérêt de l'inventaire est aussi que le Responsable des Traitements puisse avoir une représentation d'une réalité qu'il n'appréhende pas toujours : traitements hors procédures, redondances, versionning, shadow it, etc.

Étape 2 : cartographier les traitements

Approche descendante

Si l'on a choisi d'inventorier l'existant selon la méthode descendante (voir ci-dessus) il suffit d'envisager le regroupement des traitements que l'on a recensés pour chacun des processus métiers en grands blocs d'activités de traitement logiques, cohérents, et les moins redondants possible.

Approche ascendante

Si l'approche ascendante a été choisie, il faut associer chacun des traitements recensés à une activité de traitement. Une fois l'inventaire réalisé, les différents fichiers de tableur sont consolidés en un seul. On peut alors rajouter une colonne « Activité de traitement » (cf. Figure 3). En groupe de travail ou

en Copil, une séance de brainstorming permet d'associer à chaque ligne du tableur une activité de traitement. Cette association est réalisée de manière empirique et itérative pour chaque ligne du tableur (ie pour chaque document ou fichier).

Document et fichier	**Activité de traitement**	Créé	Etablissement ou service	A quoi sert ce document ?	Support	Hébergement des données	Le traitement comporte des données sensibles	Personnes concernées (salariés, adhérents, partenaires, etc.)	Durée de conservation	Mesures de protection pour éviter la fuite de données	Circulation des données	Commentaires

Figure 3 - trame de tableur avec mention de l'activité

Au terme de la démarche, on obtient aisément la cartographie des activités de traitement (cf. Figure 4[8]).

N°	Processus	Activités de traitement	nb activités
1	**Gestion des accompagnements**		
	1.1	Gestion administrative et financière	1
	1.2	Suivi social des personnes	2
	1.3	Gestion du projet personnalisé	3
	1.4	Gestion des statistiques, études & enquêtes de satisfaction	4
2	**Gestion des informations et des contacts avec les personnes**		
	2.1	Suivi des contacts et des demandes	5
	2.2	Gestion des invitations	6
	2.3	Gestion de l'activité, statistiques, études, enquêtes de satisfac	7
3	**Gestion des ressources humaines**		
	3.1	Gestion du recrutement	8
	3.2	Gestion administrative des personnels et stagiaires	9
	3.3	Gestion des rémunérations et formalités associées	10
	3.4	Gestion de l'organisation et du temps de travail	11
	3.5	Gestion des relations sociales	12
	3.6	Gestion du parcours professionnel	13
3	**Gestion de la comptabilité**		
	3.1	Gestion de la facturation	14
	3.2	Gestion des frais de gestion des majeurs protégés	15
	3.4	Gestion budgétaire	16
	3.5	Gestion des fournisseurs et sous traitant	17
4	**Gestion des Systèmes d'Information**		
	6.3	Messagerie électronique et messagerie instantanée	18
	6.4	Gestion du parc informatique et téléphonique	19
	6.5	Gestion des annuaires	20
	6.6	Gestion des authentifications et habilitations	21
5	**Gestion de la vie associative**		
	7.1	Gestion des adhésions	22
	7.2	Gestion des bénévoles et administrateurs	23
	7.5	Gestion du développement associatif	24
	3.6	Gestion de la vie Institutionnelle	25
6	**Gestion de la communication**		
	8.1	Lettre d'info et emailings externes	26
	8.2	Emailings internes	27
	8.3	Photothèque et vidéothèque	28
	8.4	Réseaux sociaux	29
	8.5	Gestion du site internet	30
7	**Gestion de la sécurité des biens et des personnes**		
	9.1	Vidéosurveillance	31
	9.2	Suivi attribution des badges	32

Figure 4 - exemple de cartographie

De l'inventaire à la cartographie en mixant les deux approches

Il va de soi que lorsqu'une démarche de cartographie des processus métiers a précédemment été entreprise dans la structure, les deux approches, ascendante et descendante, peuvent être conjuguées. Cette approche mixte permet de gagner du temps et de produire une cartographie vraiment cohérente avec les orientations stratégiques et organisationnelles de la structure.

Étape 3 : structurer le registre des activités de traitement

Chacune des activités de traitement définies à l'étape précédente donne lieu à l'établissement d'une fiche du registre des activités de traitement. La CNIL donne à voir sur son site[9] son propre registre des activités de traitement. Ce document est à prendre comme une illustration et non comme un modèle : le registre de chaque organisme est fortement lié à ses activités spécifiques. Mais la CNIL publie aussi des modèles et des tutoriels de registre des activités de traitement[10]. Dans de nombreux cas, ces modèles suffisent à répondre aux obligations de la structure. L'acquisition d'un logiciel dédié ne doit être envisagée qu'après avoir testé ces modèles et identifié leurs limites.

Conclusion

Les étapes d'inventaire, de cartographie et d'ouverture du registre des activités de traitement sont les étapes clés de la démarche de mise en conformité d'une structure. Ces étapes demandent du temps, de la rigueur et de la méthode. Elles nécessitent aussi que les professionnels soient associés aux différents moments de la démarche.

1. RGPD art. 4-1?
2. RGPD art. 4-2?
3. RGPD art. 30?
4. RGPD art. 83?
5. Code pénal Art. 226-16?
6. [en ligne] https://www.cnil.fr/sites/default/files/atoms/files/referentiel-grh.pdf [consulté le 20/2/2020]?
7. ANAP - « Lancer une démarche processus : Les fondamentaux »?
8. Attention cette copie d'écran est un exemple d'un travail en cours elle n'est pas un modèle qui serait validé et reproductible.?
9. https://www.cnil.fr/sites/default/files/atoms/files/registre-rgpd-cnil_decembre-2019.pdf?
10. https://www.cnil.fr/fr/la-cnil-publie-un-nouveau-modele-de-registre-simplifie?

Glossaire

ANAP
audit
cartographie des processus
CNIL
personne
processus
RGPD
risque