Passons à la pratique

Rédiger votre registre des traitements

Passons à la pratique

Registre

Pourquoi recenser les traitements?

- Pour savoir quels sont les traitements et vérifier ainsi leur conformité
- Pour documenter la conformité
- Pour faciliter les demandes des personnes fichées

Qui ? Quoi ? Pourquoi ? Où ? Jusqu'à quand ? Comment ?

La formalisation de cet exercice se retrouve dans le registre des traitements.

Registre du responsable de traitement et du sous-traitant

Mis à disposition sur demande

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Passons à la pratique

Registre

Dispositions pour les organismes de moins de 250 salariés

Les entreprises de moins de 250 salariés bénéficient d'une dérogation en ce qui concerne la tenue de registres. Ils doivent inscrire au registre les seuls traitements de données suivants :

- les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.)
- les traitements qui portent sur des données sensibles (exemple : données de santé, infractions, etc.).

En pratique, cette dérogation est donc limitée à des cas très particuliers de traitements, mis en œuvre de manière occasionnelle et non routinière, comme par exemple une campagne de communication à l'occasion de l'ouverture d'un nouvel établissement, sous réserve que ces traitements ne soulèvent aucun risque pour les personnes concernées. En cas de doute sur l'application de cette dérogation à un traitement, la CNIL vous recommande de l'intégrer dans votre registre.

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Passons à la pratique

Registre

Modèle de fiche de registre à compléter						
Cet onglet est un modèle de fiche opérationnelle à reprendre, adapter et compléter selon votre activité pour chaque traitement. Dans certains cas, des commentaires seront proposés pour vous aider à compléter votre registre (triangle rouge dans la cellule).						
Description du traitement						
Nom du traitement						
N° / REF	ref-001					
Date de création du traitement						
Mise à jour du traitement						
Acteurs	**Nom**	**Adresse**	**Code Postal**	**Ville**	**Pays**	
Responsable du traitement						
Délégué à la protection des données						
Société du DPO (si celui-ci est externe)						
Représentant						
Responsable(s) conjoint(s)						
Finalité(s) du traitement effectué						
Finalité principale						
Sous-finalité 1						
Sous-finalité 2						
Sous-finalité 3						
Sous-finalité 4						

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

https://www.cnil.fr/fr/liste-des-normes-et-des-dispenses

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

Passons à la pratique

Pré-Cartographie des données

Services/Domaines d'activités

Catégorie de données personnelles

Sources de données

Logiciels/applications

Passons à la pratique

Cartographie des traitements de données et Registre

https://www.cnil.fr/fr/declaration/ns-046-gestion-du-personnel

https://www.cnil.fr/fr/declaration/au-048-accompagnement-et-suivi-social-des-personnes-en-difficultes

https://www.cnil.fr/fr/dispense/di-008-associations-gestion-des-membres-et-donateurs

https://www.cnil.fr/fr/les-fichiers-des-associations-en-questions

https://www.legifrance.gouv.fr/jo_pdf.do?numJO=0&dateJO=20060603&numTexte=80&pageDebut=&pageFin=

https://www.cnil.fr/fr/declaration/au-049-accompagnement-et-suivi-social-dans-le-cadre-de-la-prevention-et-de-la-protectio

Archivage

REFERENTIEL DUREE DE CONSERVATION

2012
En attente
d'un nouveau référentiel

Mais aussi données sensibles, traitements à risques …

https://www.fcga.fr/wp-content/uploads/2018/04/20120719-REF-DUREE_CONSERVATION-VD.pdf

https://www.cnil.fr/fr/liste-des-normes-et-des-dispenses

Passons à la pratique

Sous-traitant

Qui ?

- les prestataires de services informatiques (hébergement, maintenance, ...), les agences de marketing ou de communication

Obligation

- Une obligation de transparence et de traçabilité.
- La prise en compte des principes de protection des données dès la conception et de protection des données par défaut
- Une obligation de garantir la sécurité des données traitées.
- Une obligation d'assistance, d'alerte et de conseil

Sous traitance en chaîne

- après avoir obtenu l'autorisation écrite du client.
- soumis aux mêmes obligations que celles prévues dans le contrat

https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

Passons à la pratique

Sous-traitant

Exemples de clauses

Exemple d'engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel :

Je soussigné/e Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :
- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à xxx, le xxx, en xxx exemplaires

Nom :
Signature :

https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf (p 8)
https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf (Page 13 et 14)

Passons à la pratique

Analyse d'impact

Une AIPD aide à construire des traitements de données respectueux de la vie privée et à démontrer leur conformité au RGPD.

Elle doit obligatoirement être menée quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

- évaluation/*scoring* (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ou données à caractère hautement
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, *etc.*) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

CNIL.

Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

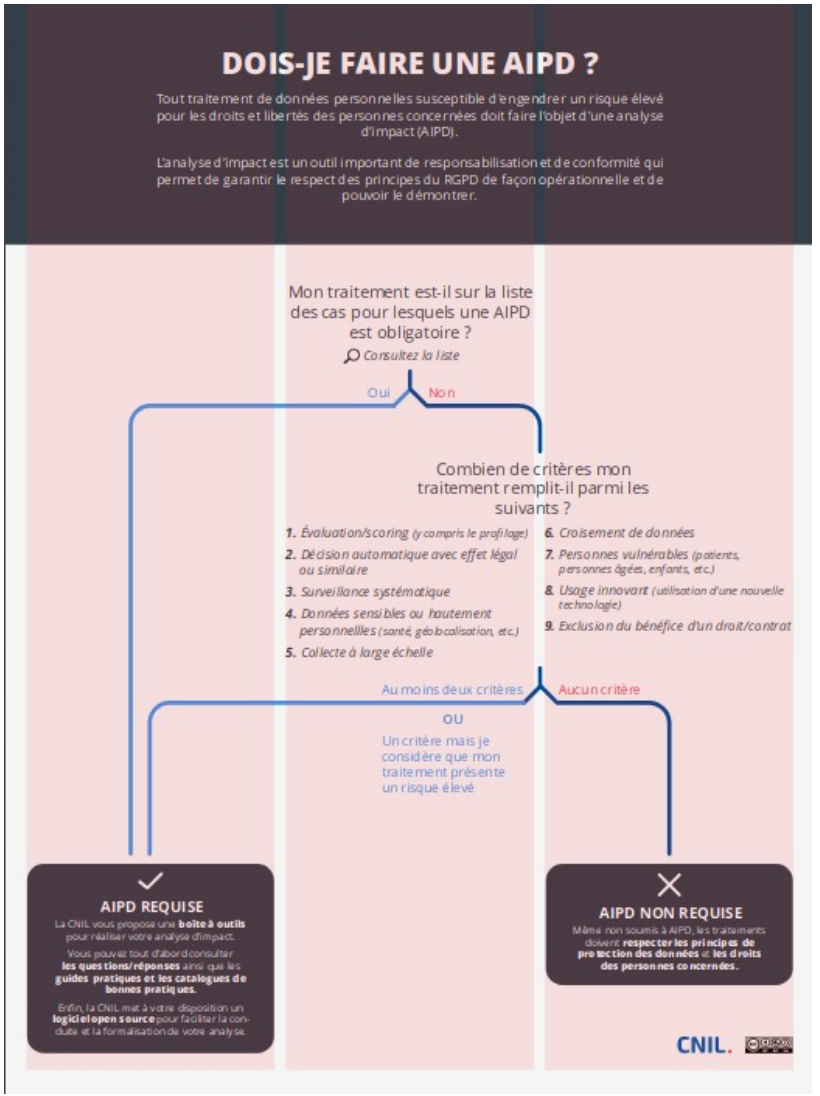
Types d'opérations de traitement	Critères issus des lignes directrices du CEPD qu'ils remplissent	Exemples
Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes.	- collecte de données sensibles - personnes dites « vulnérables »	- traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) : • dossier « patients » ; • algorithmes de prise de décision médicale ; • dispositifs de vigilances sanitaires et de gestion du risque ; • dispositifs de télémédecine ; • gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc. - traitement portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ou par un établissement d'hébergement pour personnes âgées dépendantes (EPHAD).
Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.).	- collecte de données sensibles - personnes dites « vulnérables »	- mise en œuvre d'une recherche médicale portant sur des patients et incluant le traitement de leurs données génétiques ; - traitement utilisé pour la gestion d'une consultation de génétique dans un établissement de santé.

https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf

Passons à la pratique

Analyse d'impact



https://www.cnil.fr/sites/default/files/atoms/files/181029_infographie_pia.pdf

Passons à la pratique

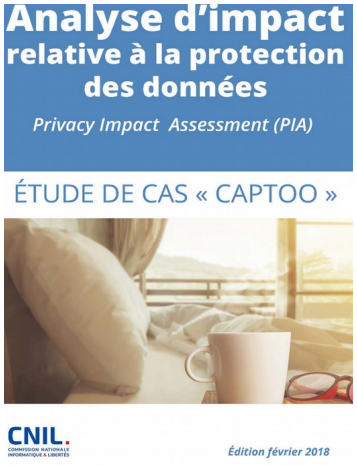
Analyse d'impact

https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Un AIPD contient à minima :

- une description systématique des opérations de traitement envisagées et les finalités
- une évaluation de la nécessité et de la proportionnalité des traitements
- une évaluation des risques sur les droits et libertés des personnes concernées
- les mesures envisagées pour faire face aux risques

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-captoo-fr.pdf



L'AIPD doit être transmise à la CNIL dans les cas suivants :

- si risque résiduel élevé
- quand la législation nationale d'un État membre l'exige ;
- en cas de contrôle par la CNIL.

Passons à la pratique

Analyse d'impact

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Audit

PROCESSUS D'AMELIORATION (ERREUR, NOUVEAU RISQUE...)

Objectifs d'un audit "informatique et libertés

- Voir où on se situe en protection des données
- Vérifier la conformité des pratiques
    - Mentions d'information
    - gestion des demandes des personnes
    - contrats avec sous-traitants
    - gestion des retraits de consentement
- Améliorer les pratiques par des actions correctives
    - process de gestion des demandes
    - Formation
    - Guide de négociation des contrats

Passons à la pratique

Audit

Critères de mise en œuvre :
temps nécessaire, budget nécessaire,
risque juridique, risque d'image
(perte de confiance, réputation),
attente des adhérant ....

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

	FICHES	MESURE	
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	☐
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	☐
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	☐
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	☐
		Stockez les supports de sauvegarde dans un endroit sûr	☐
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	☐
		Prévoyez et testez régulièrement la continuité d'activité	☐
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	☐
		Détruisez les archives obsolètes de manière sécurisée	☐
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	☐
		Encadrez par un responsable de l'organisme les interventions par des tiers	☐
		Effacez les données de tout matériel avant sa mise au rebut	☐
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des sous-traitants	☐
		Prévoyez les conditions de restitution et de destruction des données	☐
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	☐
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	☐
		Assurez-vous qu'il s'agit du bon destinataire	☐
		Transmettez le secret lors d'un envoi distinct et via un canal différent	☐
15	Protéger les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	☐
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	☐
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	☐
		Évitez les zones de commentaires ou encadrez-les strictement	☐
		Testez sur des données fictives ou anonymisées	☐
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	☐
		Conservez les secrets et les clés cryptographiques de manière sécurisée	☐

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

https://www.cigref.fr/wp/wp-content/uploads/2017/11/CIGREF-GT-AFAI-CIGREF-TIF-Donnees-Personnelles-et-Systemes-d-Informations-GDPR-2017.pdf