Mise en conformité RGPD et impact sur le milieu associatif

Terra Data
Données
Acteurs
& Territoires
Collaboratifs

Présentation

Data Terra : données, acteurs et territoires collaboratifs

Les données au service de l'intérêt général

Etude Accompagnement Formation

#RGPD #Sciences Participatives

#Territoires intelligents #Open Data

cnam

AFCDP Association Française des Correspondants à la protection des Données à caractère Personnel

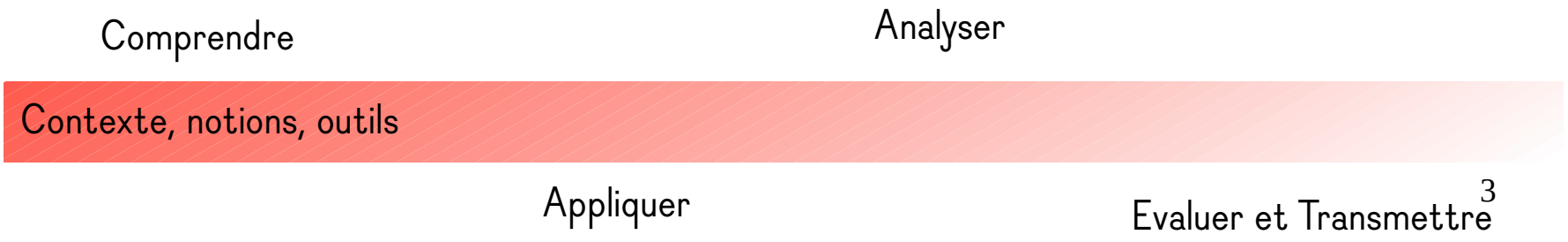
Déroulé

– Contexte numérique

– Principes et définitions essentielles (théorie)

- Passer à l'action (pratique)

– Synthèse et ressources pour aller plus loin



Mise en garde

CE QUE LA FORMATION NE FERA PAS , CAR UNE JOURNÉE C'EST TROP COURT !

– Des sujets ne seront pas traités : prospection commerciale, anonymisation, fraude, transferts européens et internationaux...

– Des questions resteront encore en suspends (accompagnement long terme)

- Des spécificités à certains contextes professionnels ne seront pas abordés en groupe

Le RGPD, pourquoi maintenant ?

Bienvenue

Une journée de traces numériques dans la vie d'un citoyen ordinaire

https://www.lemonde.fr/societe/infographie/2006/04/10/une-journee-de-traces-numeriques-dans-la-vie-d-un-citoyen-ordinaire_759979_3224.html

2006

Contexte

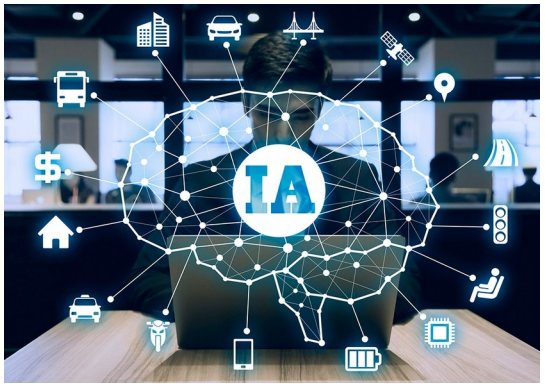
1978

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

2016 2018

https://youtu.be/i_k8ozkY2I4

2006



https://www.actualites.uqam.ca/2018/intelligence-artificielle-progres-ou-danger

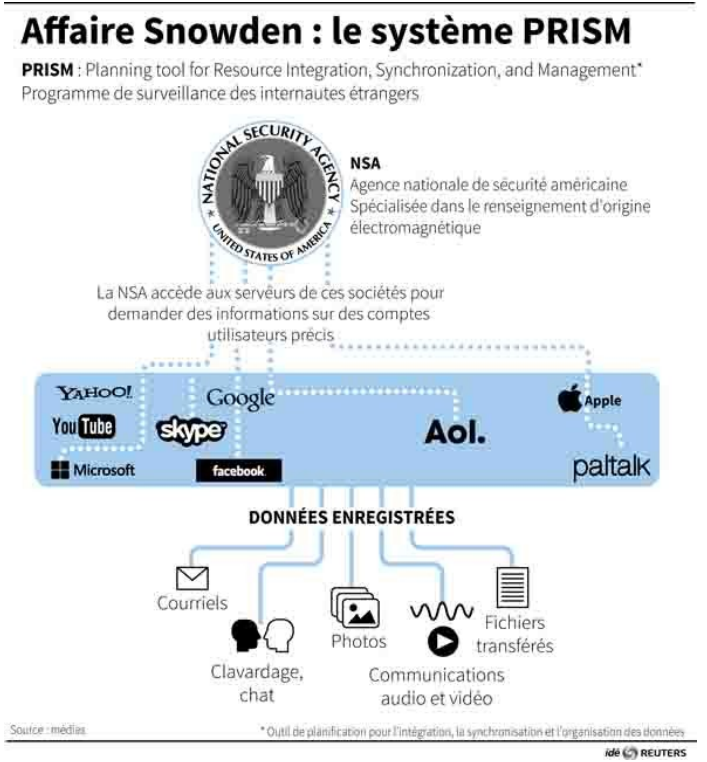
https://www.lemonde.fr/societe/infographie/2006/04/10/une-journee-de-traces-numeriques-dans-la-vie-d-un-citoyen-ordinaire_759979_3224.html

https://lalibrerie-solidaire.org/actualite-20180312-dossier-RGPD-pour-les-pros-1-sur-2.htm

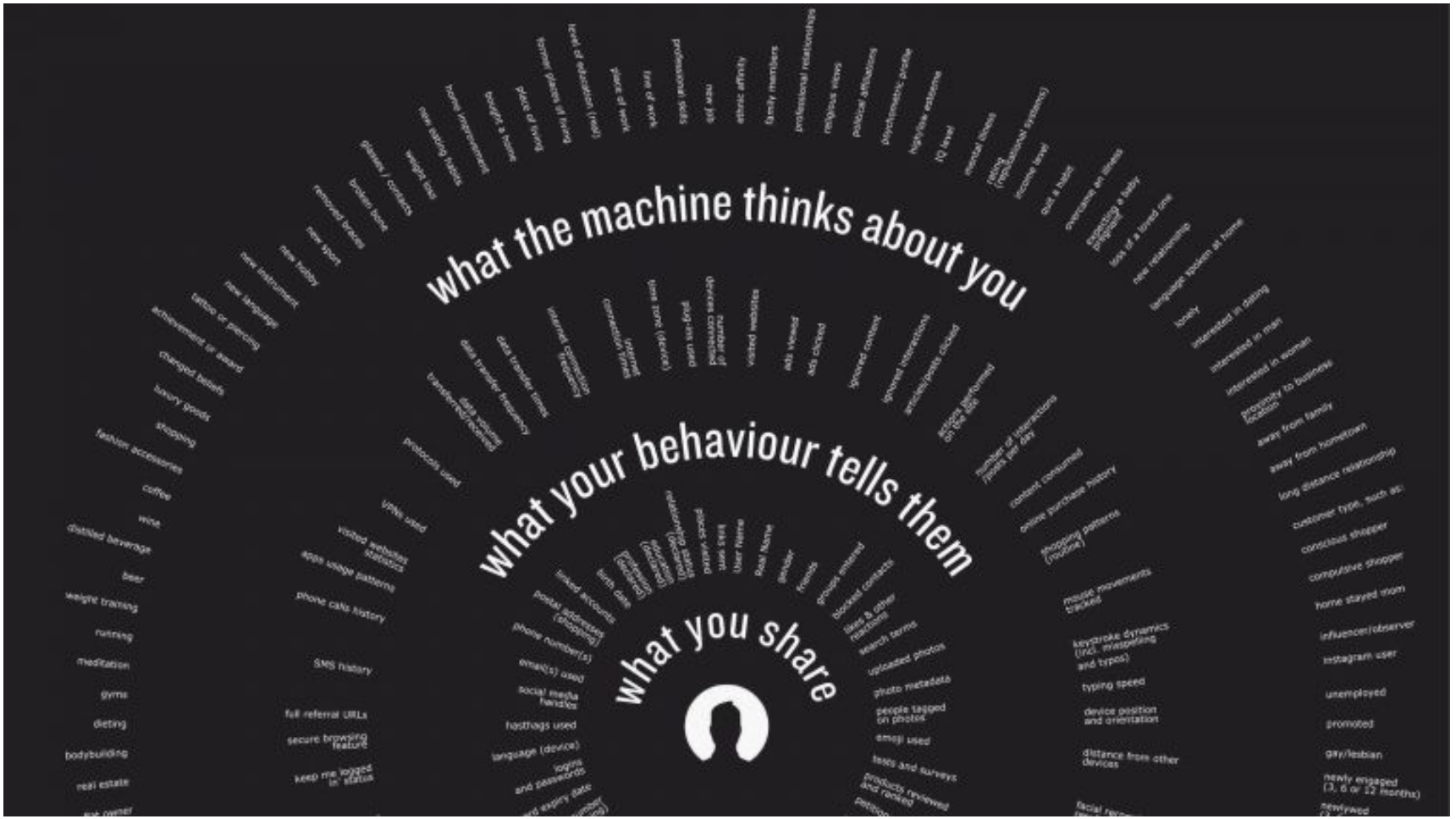
Contexte

2018

2013



https://www.arte.tv/fr/videos/082806-000-A/comment-trump-a-manipule-l-amerique/
https://www.lemonde.fr/pixels/article/2018/04/06/cambridge-analytica-2-7-millions-d-utilisateurs-europeens-de-facebook-pourraient-etre-concernes_5281717_4408996.html
http://blog.tamento.com/nsa-prism-ce-qu-il-faut-savoir-sur-laffaire-snowden.html



http://internetactu.blog.lemonde.fr/2019/02/02/les-3-niveaux-de-nos-identites-en-ligne/

https://panoptykon.org/sites/default/files/3levels.png

http://internetactu.blog.lemonde.fr/2019/02/02/les-3-niveaux-de-nos-identites-en-ligne/

https://panoptykon.org/sites/default/files/3levels.png

Contexte


e thinks about you
number of devices connected
visited websites
ads viewed
ads clicked
ignored content
ignored interactions
ticles/posts clicked
performed
ns
new job
ethnic affinity
family members
professional relationships
religious views
political affiliations
psychometric profile
high/low esteeme
IQ level
mental illness
rating (reputational systems)
income level
quit a habit
overcame an illness
expecting a baby pregnant
loss of a loved one
new relationship
language spoken at home
lonely
interested in dating
interested in man
interested in woman
ximity to business

Le RGPD, de quoi parle-t-on ?

Un peu de théorie

GENERAL
DATA
PROTECTION
REGULATION

RÉGLEMENT
GÉNÉRAL SUR LA
PROTECTION DES
DONNÉES

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

https://europa.eu/european-union/eu-law/legal-acts_fr

R comme règlement

UN CADRE JURIDIQUE UNIFIÉ POUR L'ENSEMBLE DE L'UE

Règlements, directives et autres actes législatifs

CONTENU

- Règlements
- Directives
- Décisions
- Recommandations
- Avis

L'Union européenne adopte différents types d'actes législatifs, qui visent à remplir les objectifs fixés dans les traités européens. Tous ne sont pas contraignants. Certains s'appliquent à tous les pays de l'UE, d'autres uniquement à quelques-uns.

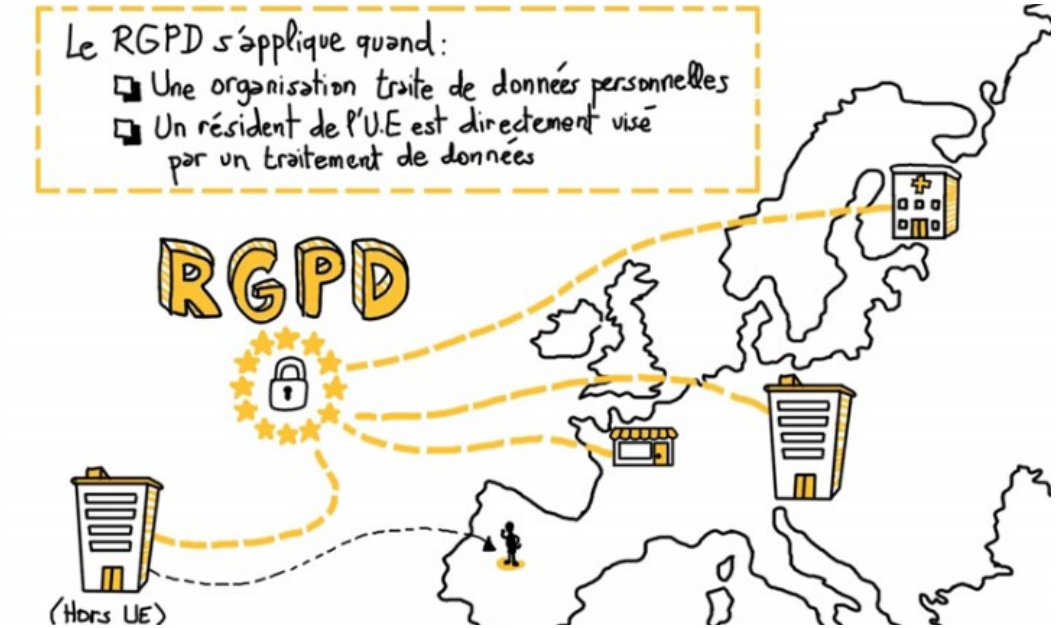
Règlements

Les règlements sont des actes législatifs contraignants. Ils doivent être mis en œuvre dans leur intégralité, dans toute l'Union européenne. Par exemple, quand l'UE a voulu garantir que des mesures de sauvegarde communes s'appliquent aux produits importés sur son territoire, le Conseil a adopté un règlement.

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

https://europa.eu/european-union/eu-law/legal-acts_fr

Champ d'application du RGPD



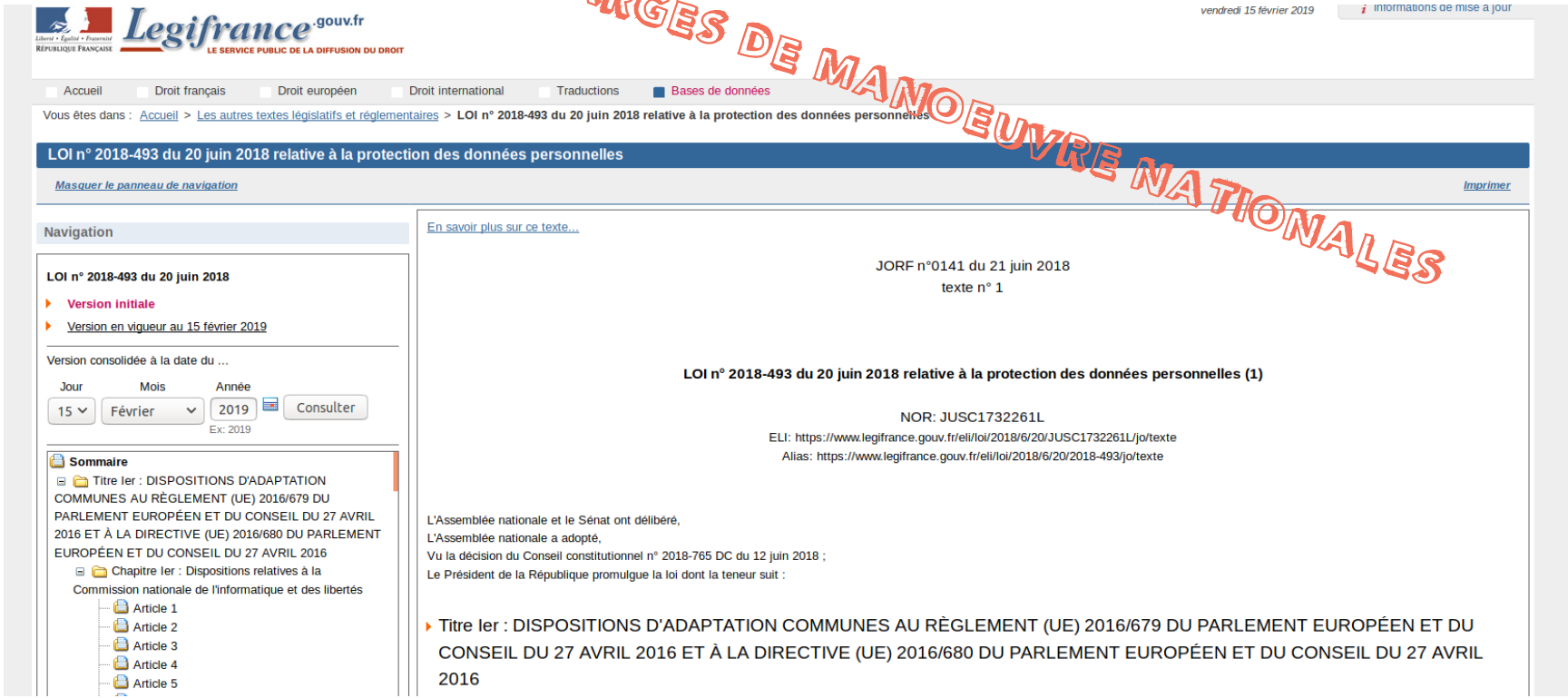
youtube.com/cookieconnecte

En pratique, le règlement s'applique donc à chaque fois qu'un résident européen, quelle que soit sa nationalité, est directement visé par un traitement de données, y compris par internet ou par le biais d'objets connectés (comme les appareils domotiques, les objets mesurant l'activité physique, etc.).

https://www.vie-publique.fr/actualite/dossier/securite-internet/reglement-general-protection-donnees-quoi-s-agit-il.html

https://www.youtube.com/watch?v=u4M5IVYv3UI
https://www.youtube.com/watch?v=OUMGp3HHeI4

Loi nationale



https://www.cnil.fr/fr/entree-en-vigueur-de-la-nouvelle-loi-informatique-et-libertes

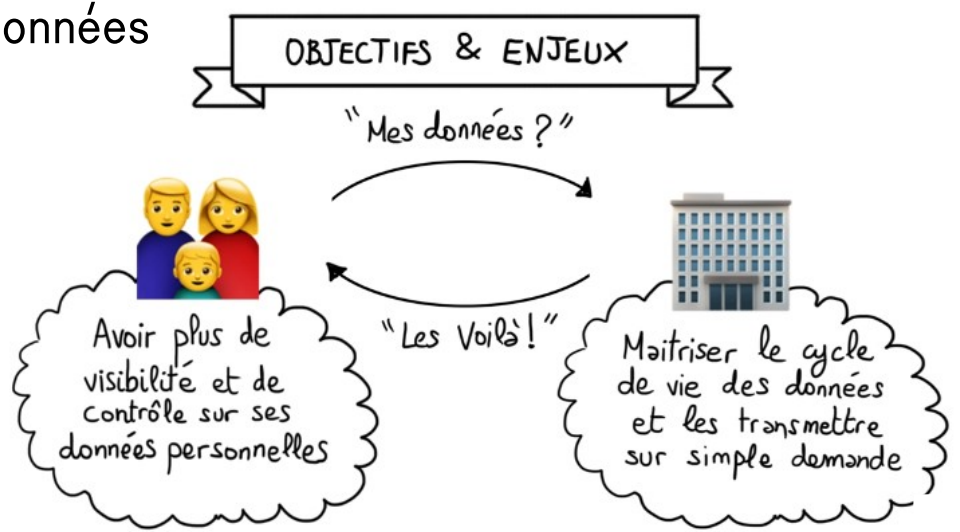
https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte

Objectifs

1-Renforcer les droits des personnes

2-Responsabiliser les acteurs traitant des données

3-Crédibiliser la régulation grâce à une coopération renforcée
entre les autorités de protection des données



youtube.com/cookieconnecte

https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

https://www.youtube.com/watch?v=u4M5IVYv3UI
https://www.youtube.com/watch?v=OUMGp3HHeI4

Données personnelles

≠ DONNEES STATISTIQUES
≠ DONNEES ANONYMISEES

« Toute information qui permet d'identifier une personne directement ou indirectement. »

«données à caractère personnel», **toute information se rapportant à une personne physique identifiée ou identifiable** (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Article 4. 1 RGPD.

Définitions

https://scintolex.com/2018/05/29/donnees-personnelles-et-vie-privee-ce-qui-va-changer-avec-le-rgpd-support-dintervention-et-video/#comment-48215

Données personnelles

Etat-civil, identité, données d'identification	Vie personnelle	Vie professionnelle
Nom, prénom	Habitudes de vie	CV
Adresse	Situation familiale	Situation professionnelle
Photographie		Scolarité, formation
Date, lieu de naissance		Distinction

Information d 'ordre économique et financier	Données de connexion
Revenus	Adresse IP
Situation financière (taux d'endettement)	Logs
	Identifiant des terminaux
	Identifiant de connexion
	Information d'horodatage

Exemples :

- Fichiers d'adhérents, bénévoles
- Fichiers bénéficiaires, salariés
- Fichiers contacts (partenaires, donateurs)
- Base de mails (newsletters)
- Adresses IP

...

Données interdites

Des types de données dont la collecte et le traitement sont en principe interdits.

« Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique **sont interdits**. »

Article 9.1. RGPD

Mais nombreuses exceptions…

+ données relatives à des infractions et sanctions pénales, données relatives aux enfants, NIR, etc.

- Consentement explicite de la personne concernée ;
- Traitement nécessaire en droit du travail, sécurité sociale, protection sociale ;
- Sauvegarde des intérêts vitaux de la personne concernée ;
- Traitement nécessaire pour des motifs d'intérêt public ;
- Traitement par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale ;
- Données à caractère personnel qui sont manifestement rendues publiques par la personne concernée.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2

https://scinfolex.com/2018/05/29/donnees-personnelles-et-vie-privee-ce-qui-va-changer-avec-le-rgpd-support-dintervention-et-video/#comment-48215

Données interdites

Données sensibles
Origines raciales
Origines ethniques
Opinions philosophiques
Opinions politiques
Opinions syndicales
Opinions religieuses
Vie sexuelle
Santé des personnes
Données biométriques
Donées génétiques
Infractions, condamnations et mesures de sécurité
Appréciation sur les difficultés sociales des personnes

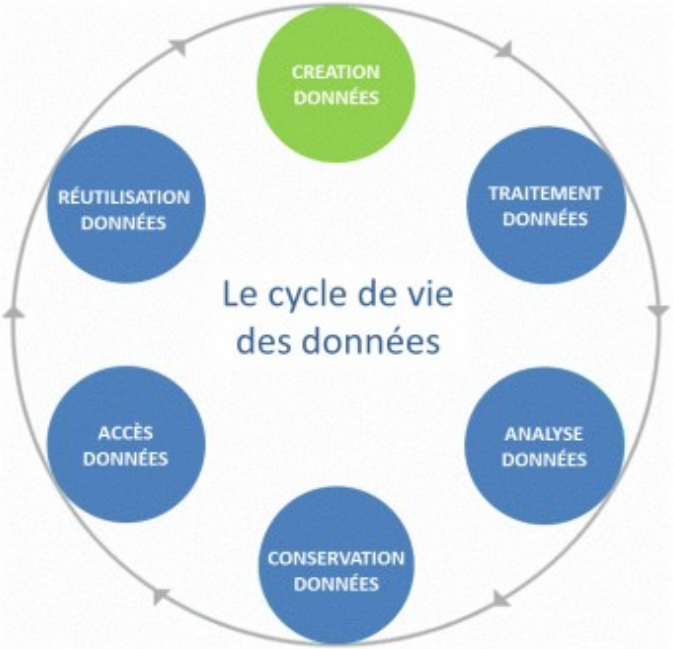
Données d'infraction et de sanctions pénales
NIR

ATTENTION AUX CHAMPS LIBRES ET AUX ZONES COMMENTAIRES

https://scinfolex.com/2018/05/29/donnees-personnelles-et-vie-privee-ce-qui-va-changer-avec-le-rgpd-support-dintervention-et-video/#comment-48215

Traitement

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;



https://www.inist.fr/

https://www.cnil.fr/fr/definition/traitement-de-donnees-caractere-personnel

https://espacechercheurs.enpc.fr/fr/donnees-recherche-intro

Traitement

Gestion du recrutement
Registre du personnel
Gestion des horaires et des tâches
Gestion de la paie
Gestion des dotations aux salariés
Gestion de la formation
Evaluation des salariés
Contrôle d'accès par badge
Vidéosurveillance
Enregistrement des conversations téléphoniques (contrôle de la qualité et de la formation)
Dispositif de géolocalisation
Elections professionnelles
Gestion des relations avec les IRP
Gestion des œuvres sociales mises en oeuvre par la société (et non pas le CSE)
Gestion de la messagerie professionnelle
Contrôle global de la messagerie professionnelle
Contrôle global des connexions à internet
Gestion de la téléphonie (cf pour les entreprises qui reçoivent des factures détaillées des appels sortants)
Infractions au code de la route
Site internet
Gestion des fournisseurs et des stocks
Gestion de la comptabilité générale
Clients et prospects
Gestion des événements
Procès verbaux des assemblées /commissions
Délibérations
...

SONT SEULEMENT EXEMPTES LES « TRAITEMENTS STRICTEMENT PERSONNELS » CARNET D'ADRESSES, D'UN AGENDA, ETC.

Responsable de traitement

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

youtube.com/cookieconnecte

Quel que soit
- la taille
- le nombre de salariés
- le nombre d'adhérents

<u>Exemple :</u>
personne morale
incarnée par son représentant légal :
président de l'association

https://www.youtube.com/watch?v=u4M5lVYv3UI
https://www.cnil.fr/fr/definition/responsable-de-traitement

Sous-traitant

Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

https://www.youtube.com/watch?v=u4M5lVYv3UI
https://www.cnil.fr/fr/definition/responsable-de-traitement

Sous-traitant

Exemple :

- les prestataires de services informatiques (hébergement, maintenance, sécurité…)
- les agences de marketing ou de communication
- les prestataires de vidéo surveillance
- …

Principes

Les données à caractère personnel doivent être :

Notion centrale de finalité du traitement

=> Ce que le responsable veut faire avec les données collectées.

Le fait de **lier les traitements à une finalité** précise conditionne pour les individus la possibilité d'exercer leurs droits sur les données.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5

https://scinfolex.com/2018/05/29/donnees-personnelles-et-vie-privee-ce-qui-va-changer-avec-le-rgpd-support-dintervention-et-video/#comment-48215

Principes - nouveauté

Principe d' *accountability*

Renversement important par rapport à la réglementation antérieure :
- avant : déclarations préalables à effectuer auprès de la CNIL
- RGPD : obligation de se mettre en conformité et de la documenter

https://scinfolex.com/2018/05/29/donnees-personnelles-et-vie-privee-ce-qui-va-changer-avec-le-rgpd-support-dintervention-et-video/#comment-48215

Principes-nouveauté

principe de minimisation et de *privacy by default*

On passe avec le RGPD d'une logique d'interdiction de l'usage excessif à une obligation de **minimisation** de la collecte.

« *Les données à caractère personnel doivent être [...] adéquates, pertinentes et limitées à* ***ce qui est nécessaire*** *au regard des finalités pour lesquelles elles sont traitées.* »
Art. 5.1.c) RGPD

Principe de minimisation

« *Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel* ***qui sont nécessaires*** *au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité.* »
Art. 25.2 RGPD

Privacy by default (Protection par défaut)

https://scinfolex.com/2018/05/29/donnees-personnelles-et-vie-privee-ce-qui-va-changer-avec-le-rgpd-support-dintervention-et-video

Bases Légales

Article 6 - Licéité du traitement

Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

a) la personne concernée **a consenti** au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'**exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au **respect d'une obligation légale** à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique;

e) le traitement est nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

f) le traitement est nécessaire aux fins des **intérêts légitimes poursuivis par le responsable du traitement** ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

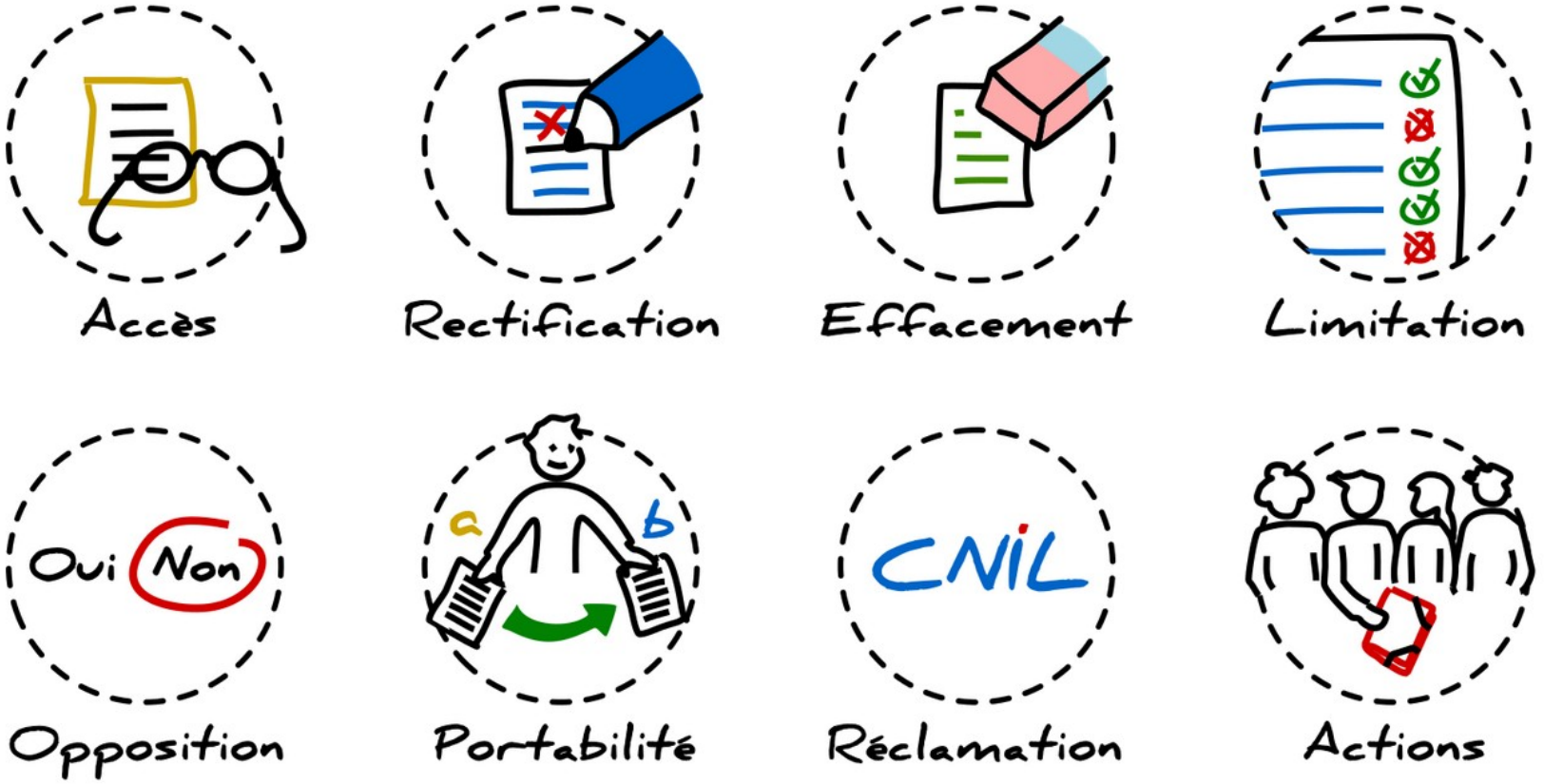
LE CONSENTEMENT PREALABLE N'EST PAS UNE OBLIGATION SYSTEMATIQUE AVEC LE RGPD.

CE N'EST QU'UNE DES SIX BASES LEGALES POSSIBLES POUR UN TRAITEMENT LICITE.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article6

https://lalibrerie-solidaire.org/actualite-20180312-dossier-RGPD-pour-les-pros-2-sur-2.html

RGPD : les droits de la personne



https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3

https://www.cnil.fr/fr/respecter-les-droits-des-personnes

Quels sont les outils de mise en conformité ?

Passons à la pratique

Respecter le droits des personnes

Rédiger votre registre des traitements

Trier vos données

Gérer vos sous-traitants

Sécuriser vos données

Analyser les risques

Réaliser un audit

ACCOUNTABILITY

1) Comprendre les exigences
2) Identifier les outils (CNIL)
3) Démarrer sa mise en conformité

http://www.rfi.fr/france/20190122-google-amende-non-respect-rgpd-cnil

Respecter le droits des personnes

Données personnelles: la Cnil inflige une amende de 50 millions d'euros à Google

Par RFI

Publié le 22-01-2019 • Modifié le 22-01-2019 à 12:07

Le géant de l'internet Google a été épinglé par la Cnil pour son non respect du RGPD.

REUTERS/Aly Song

N'explique pas suffisamment à ses utilisateurs à quoi servent leurs données personnelles.

Ne demande pas le consentement explicite des internautes pour pouvoir récupérer leurs données.

Informer

Pour être loyale et licite, la collecte de données personnelles doit s'accompagner d'une information claire et précise des personnes sur :

- l'identité du responsable du fichier et du délégué
- la finalité du fichier
- la base juridique
- le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse
- les destinataires des données
- la durée de conservation
- leurs droits (droit d'accès, de rectification, et d'opposition)
- le droits d'introduite une réclamation
- les éventuels transferts de données vers des pays hors UE

https://www.cnil.fr/fr/conformite-rgpd-information-des-personn

La transparence permet aux personnes concernées :

- de connaître la raison de la collecte des différentes données les concernant ;
- de comprendre le traitement qui sera fait de leurs données ;
- d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits.

https://www.cnil.fr/fr/rgpd-en-pratique-communiquer-en-ligne

https://www.cnil.fr/fr/respecter-les-droits-des-personnes

Passons à la pratique

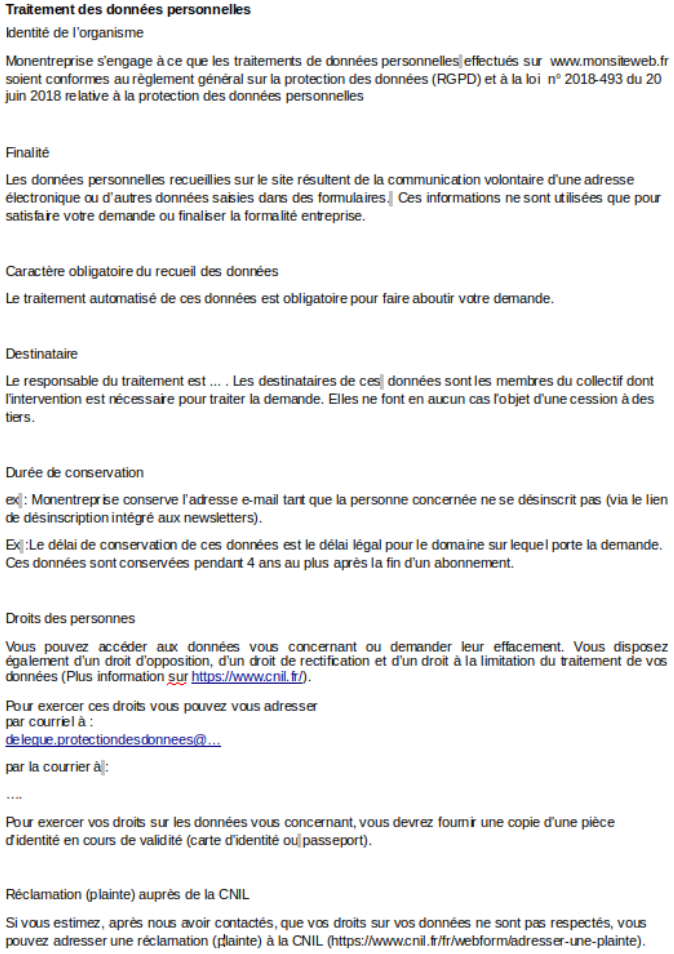
Informer

Exemples de mentions d'informations

https://www.cnil.fr/fr/donnees-personnelles

https://afcdp.net/

https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation



Traitement des données personnelles

Identité de l'organisme

Monentreprise s'engage à ce que les traitements de données personnelles effectués sur www.monsiteweb.fr soient conformes au règlement général sur la protection des données (RGPD) et à la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Finalité

Les données personnelles recueillies sur le site résultent de la communication volontaire d'une adresse électronique ou d'autres données saisies dans des formulaires. Ces informations ne sont utilisées que pour satisfaire votre demande ou finaliser la formalité entreprise.

Caractère obligatoire du recueil des données

Le traitement automatisé de ces données est obligatoire pour faire aboutir votre demande.

Destinataire

Le responsable du traitement est ... . Les destinataires de ces données sont les membres du collectif dont l'intervention est nécessaire pour traiter la demande. Elles ne font en aucun cas l'objet d'une cession à des tiers.

Durée de conservation

ex : Monentreprise conserve l'adresse e-mail tant que la personne concernée ne se désinscrit pas (via le lien de désinscription intégré aux newsletters).

Ex :Le délai de conservation de ces données est le délai légal pour le domaine sur lequel porte la demande. Ces données sont conservées pendant 4 ans au plus après la fin d'un abonnement.

Droits des personnes

Vous pouvez accéder aux données vous concernant ou demander leur effacement. Vous disposez également d'un droit d'opposition, d'un droit de rectification et d'un droit à la limitation du traitement de vos données (Plus information sur https://www.cnil.fr/).

Pour exercer ces droits vous pouvez vous adresser
par courriel à :
delegue.protectiondesdonnees@...

par la courrier à :

....

Pour exercer vos droits sur les données vous concernant, vous devrez fournir une copie d'une pièce d'identité en cours de validité ou passeport).

Réclamation (plainte) auprès de la CNIL

Si vous estimez, après nous avoir contactés, que vos droits sur vos données ne sont pas respectés, vous pouvez adresser une réclamation (plainte) à la CNIL (https://www.cnil.fr/fr/webform/adresser-une-plainte).

Informer

Mentions relatives aux cookies

En application de la directive européenne dite " paquet télécom ", les internautes doivent être informés et donner leur consentement préalablement à l'insertion de traceurs.

Parmi les cookies nécessitant une information préalable et une demande de consentement, on peut notamment citer :

- les cookies liés aux opérations relatives à la publicité ciblée ;
- certains cookies de mesure d'audience ;
- les cookies des réseaux sociaux générés notamment par leurs boutons de partage lorsqu'ils collectent des données personnelles sans consentement des personnes concernées.

Informer

Mentions relatives aux cookies

Modèle de bandeau d'information préalable

Voici un modèle à utiliser pour des cookies publicitaires et de mesure d'audience. Il doit être adapté en fonction de la finalité des cookies utilisés.

> *En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de* ***[Cookies ou autres traceurs]*** *pour vous proposer* ***[Par exemple, des publicités ciblées adaptés à vos centres d'intérêts]*** *et* ***[Par exemple, réaliser des statistiques de visites]****.*
>
> *Pour en savoir plus et paramétrer les traceurs*

https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs

Recueillir le consentement

Le consentement est une démarche active de l'utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée. Dans un formulaire en ligne, il peut se matérialiser, par exemple, par une case à cocher non cochée par défaut.

Le consentement est "préalable" à la collecte des données.

Le consentement préalable de la personne concernée est notamment requis :

- En cas de collecte de données sensibles
- De réutilisation des données à d'autres fins
- D'utilisation de cookies pour certaines finalités
- D'utilisation des données à des fins de prospection commerciale par voie électronique

https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

Passons à la pratique

Recueillir le consentement

Exemple de recueil du consentement

- [ ] J'accepte que ces données fassent l'objet d'un traitement

https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

Passons à la pratique

Recueillir le consentement

Que change le RGPD ? clarification et renforcement

- Droit au retrait
- Preuve du consentement

Un consentement obtenu et recueilli avant le 25 mai 2018 peut demeurer valide, à condition qu'il soit conforme aux dispositions désormais prévues par le RGPD. Cette situation peut tout à fait se produire, dans la mesure où ce nouveau cadre juridique est proche du cadre antérieur.

Si ce n'est pas le cas, les responsables du traitement doivent « rafraîchir » ou compléter le consenteme recueilli auprès des personnes afin d'être considéré valide et conforme aux exigences du RGPD.

https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

Rédiger votre registre des traitements

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

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Société (si DPO externe) :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliqu

Activités de l'organisme impliquant le traitement de données

Listez ici les activités pour lesquelles vous traitez des données personnelles

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects
Activité 3	Cliquez ici. ex. Gestion des fournisseurs
Activité 4	Cliquez ici. ex. Vente en ligne
Activité 5	Cliquez ici. ex. Sécurisation des locaux
Activité 6	Cliquez ici.
Activité 7	Cliquez ici.
Activité 8	Cliquez ici.

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

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

----> Début de section à copier pour chaque activité listée en page 2 <----

FICHE DE REGISTRE DE L'ACTIVITÉ

Cliquez ici. Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Catégories de données collectées

Cochez et listez les différentes données traitées

☐ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*
Cliquez ici.

☐ Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*
Cliquez ici.

☐ Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*
Cliquez ici.

☐ Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)*
Cliquez ici.

3

☐ Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
Cliquez ici.

☐ Données de localisation *(ex. déplacements, données GPS, GSM, ...)*
Cliquez ici.

☐ Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, ...)*
Cliquez ici.

☐ Autres catégories de données *(précisez)* :
Cliquez ici.

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☐ Non

Si oui, lesquelles ? :
Cliquez ici.

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Cliquez ici. **Jours,** Cliquez ici. **Mois,** Cliquez ici. **Ans, Autre durée :** Cliquez ici.

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).
Cliquez ici.

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

4

Passons à la pratique

Cartographie des traitements de données et Registre

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

Logiciel/application

Catégorie de données personnelles

Sous-traitant

Dossier papier

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-protection

Trier vos données

Archivage

Le cycle de vie des données

1ère phase : La base active.

- durée d'utilisation courante des données ou autrement dit, la durée nécessaire à la réalisation de la finalité du traitement.

2ème phase : L'archivage intermédiaire

obligation légale de conservation de données pendant une durée fixée ;

- intérêt administratif, notamment en cas de contentieux (commerciale, civile et fiscale)
- recherche scientifique ou historique ou à des fins statistiques.
- avec accès restreint et sous réserve de garanties appropriées

Par exemple, Après transaction effectuée, les numéros de carte bancaire : archivage intermédiaire en cas d'éventuelle contestation (13 mois) conformément à l'article L133-24 du Code monétaire et financier.

3ème phase : l'archivage définitif

- intérêt public
- services des archives

https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

Archivage

Passons à la pratique

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

Gérer vos sous-traitants

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

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)

Sécuriser vos données

Passons à la pratique

Sécurité des données

Niveau 1 : le minimum pour démarrer

La confiance passant par la sécurité, il est aujourd'hui impératif de sécuriser ses systèmes. Pour commencer, l'ANSSI et la CPME ont publié douze règles essentielles.

> L'essentiel pour démarrer

Niveau 2 : les mesures d'hygiène pour protéger votre SI

Pour protéger la plupart des systèmes d'informations courants, les mesures d'« hygiène informatique » constituent un socle indispensable. La CNIL et l'ANSSI proposent des guides pour vous aider.

> Protéger les SI les plus courants

Niveau 3 : protéger le plus sensible de façon spécifique

Pour satisfaire à l'obligation de sécurité des données qu'il traite, tout organisme doit déterminer si les mesures qu'il a choisies sont proportionnées aux risques sur les droits et libertés. Comment s'y prendre ?

> Protéger les traitements sensibles

https://www.cnil.fr/fr/securite-des-donnees

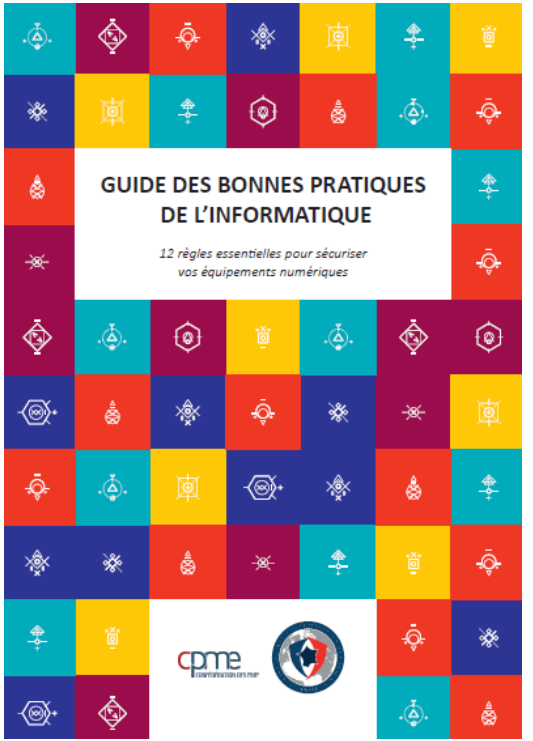
Passons à la pratique

Niveau 1 : le minimum pour démarrer

1. Choisir avec soin ses mots de passe
2. Mettre à jour régulièrement vos logiciels
3. Bien connaître ses utilisateurs et ses prestataires
4. Effectuer des sauvegardes régulières
5. Sécuriser l'accès Wi-Fi de votre entreprise
6. Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur
7. Protéger ses données lors de ses déplacements
8. Être prudent lors de l'utilisation de sa messagerie
9. Télécharger ses programmes sur les sites officiels des éditeurs
10. Être vigilant lors d'un paiement sur Internet
11. Séparer les usages personnels des usages professionnels
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

https://www.educnum.fr/

https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/



Passons à la pratique

Sensibiliser les utilisateurs

https://www.pearltrees.com/j6c29/sensibiliser-les-utilisateurs/id24040825/item249912834

Sécuriser les sites web

https://www.cnil.fr/fr/securite-securiser-les-sites-web

Utiliser des outils « privacy »

https://framindmap.org/c/maps/438273/public

Chiffrer ses documents

https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

Choisir un bon mot de passe

https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

Passons à la pratique

Notifier une violation de données personnelles

24 mai 2018

Le règlement général sur la protection des données (RGPD) impose aux responsables de traitement de documenter, en interne, les violations de données personnelles et de notifier les violations présentant un risque pour les droits et libertés des personnes à la CNIL et, dans certains cas, lorsque le risque est élevé, aux personnes concernées.

Qu'est-ce qu'une violation de données à caractère personnel ?

Pour qu'il y ait violation, 2 conditions doivent être réunies :

1. Vous avez mis en œuvre un traitement de données personnelles.
2. Ces données ont fait l'objet d'une violation (perte de **disponibilité**, **d'intégrité** ou de **confidentialité** de données personnelles, de manière **accidentelle** ou **illicite**).

https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

https://notifications.cnil.fr/notifications/index

72 HEURES AU PLUS TARD
APRÈS EN AVOIR PRIS CONNAISSANCE

Notification d'une violation de données personnelles

5 étapes pour finaliser votre notification

Analyser les risques

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/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.

Réaliser un audit

Audit

Définition

Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits (d'après NF ISO 19011 reprise par la CNIL dans son label Audit de traitements)

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

Audit

- Délimiter le champ de l'audit, les questions à poser, les niveaux de risque, la durée des audits (sélection par niveau de risques, par domaine (RH)…)
- Clarifier la méthode :
  - échantillonnage (ex: mentions d'information/ contrats)
  - questionnaires à remplir
  - entretiens
- Auditeurs externes ou internes
- Déroulement
  - Planification et préparation
  - Réalisation de l'audit
  - Rapport d'audit
  - Suivi de l'audit et clôture

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

Et pour la suite ?

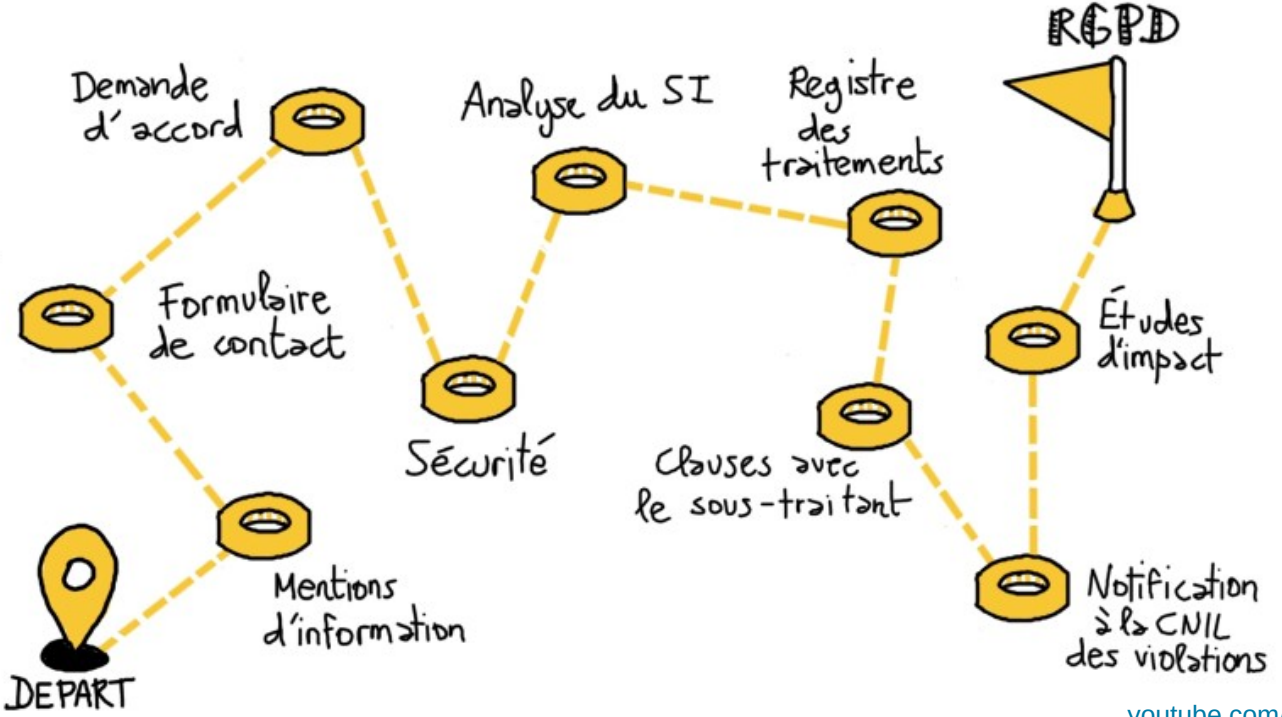
Règlement européen : les associations sont-elles concernées ?

Oui, les associations doivent respecter le Règlement européen sur la protection des données applicable depuis le 25 mai 2018.

- Si elles collectent, stockent, utilisent des données à caractère personnel. Dans ce cas, les associations sont "responsable de traitement".
- Si elles traitent des données à caractère personnel pour le compte d'autres personnes morales. Dans ce cas, les associations sont "sous-traitantes".

https://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-les-associations-sont-elles-concernees

Vers la mise en conformité…



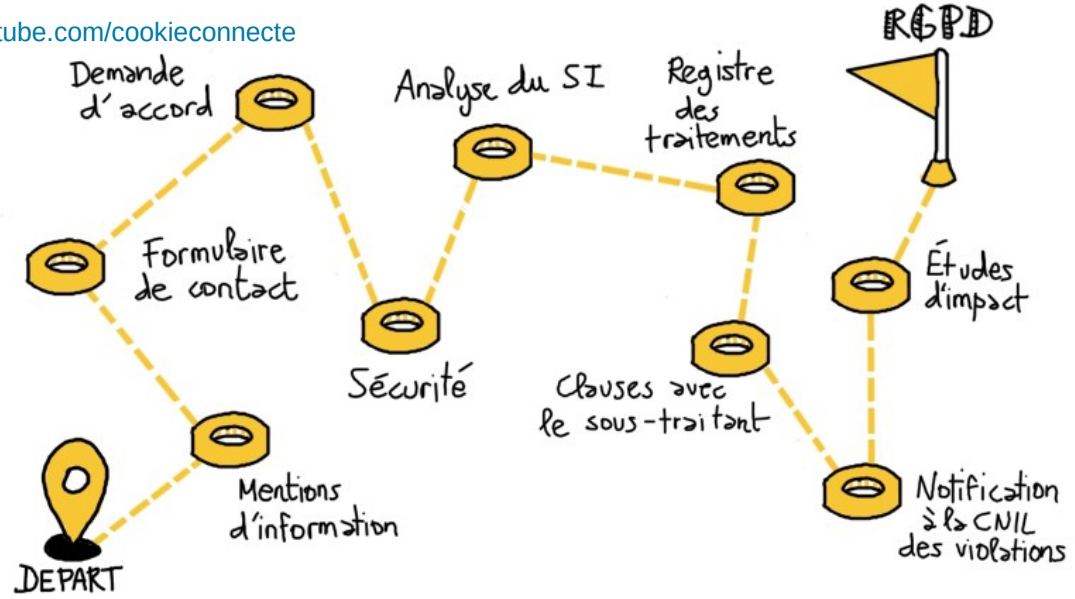
youtube.com/cookieconnecte

https://www.youtube.com/watch?v=OUMGp3HHel4

Vers la mise en conformité...

Délégué à la protection des données (DPD/DPO)

youtube.com/cookieconnecte



https://www.youtube.com/watch?v=OUMGp3HHeI4

https://www.youtube.com/watch?v=u4M5IVYv3UI

Délégué à la protection des données (DPD)

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données (DPD) est principalement chargé :

- 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'organisme sur la réalisation d'une analyse d'impact relative à 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 DPD détient les compétences requises : juridiques, techniques, organisationnelles et « métier »

Le DPO dispose de moyens suffisants

Le DPO a la capacité d'agir en toute indépendance

https://www.cnil.fr/fr/designer-un-pilote

Délégué à la protection des données (DPD)

La désignation d'un délégué est obligatoire pour :

- Les autorités ou les organismes publics,
- Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
- Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

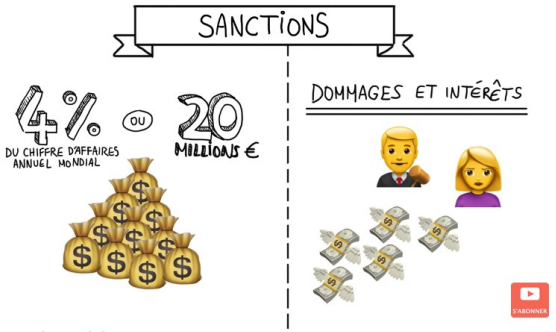
https://www.cnil.fr/fr/designation-dpo

https://www.cnil.fr/fr/designer-un-pilote

Obligations

Sanctions

Prise de conscience



youtube.com/cookieconnecte

Le RGDP, une opportunité pour …

1 - Renforcer la confiance, rassurer les adhérents, les clients, les partenaires…

2 - Améliorer la gestion et l'efficacité de l'organisation

3 - Développer votre activité et créer de nouveaux services

https://www.youtube.com/watch?v=u4M5lVYv3UI

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

- Faire l'inventaire des traitements internes et externes : registre, AIPD
- Vérifier le respect des droits des personnes : mentions d'informations, recu du consentement...
- Revoir les contrats de sous-traitance
- Intégrer la sécurité : gestion des accès, protection du réseau, violations de données personnelles ...

...

https://www.cnil.fr/professionnel

Data Terra
Données
Acteurs
& Territoires
Collaboratifs

www.dataterra.fr
Hébergée par Chrysalide – Quimper
Siret : 44390356200041
Membre du collectif Tiriad

19 Février 2019