Ethique et Sécurité

Focus RGPD

Au Sommaire

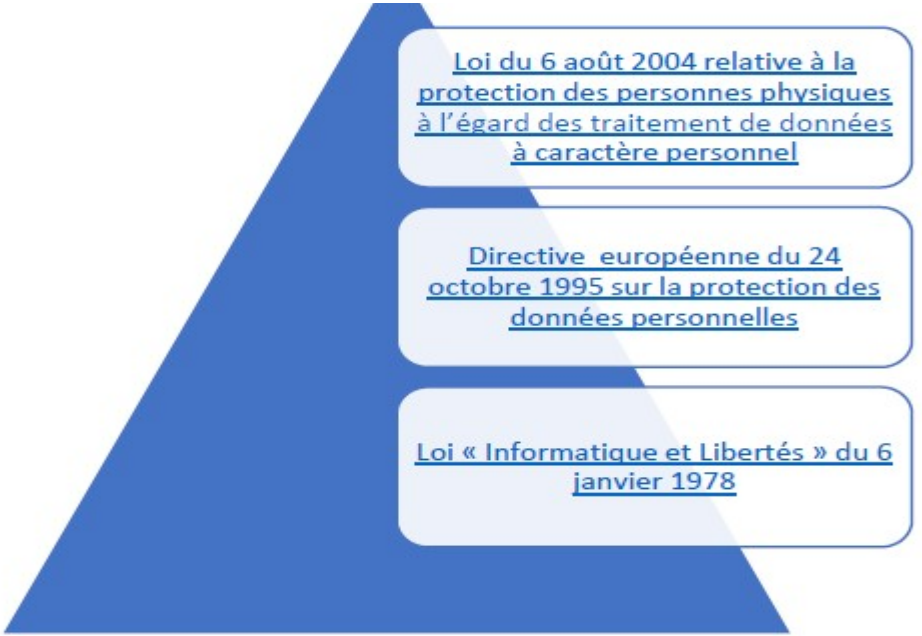
Contexte

Définitions essentielles

Passer à l'action

Impacts et intérêts

Le RGPD, pourquoi maintenant ?

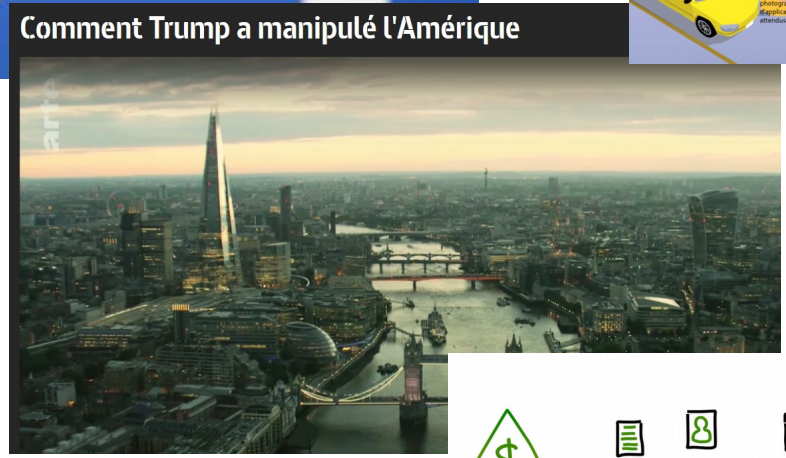


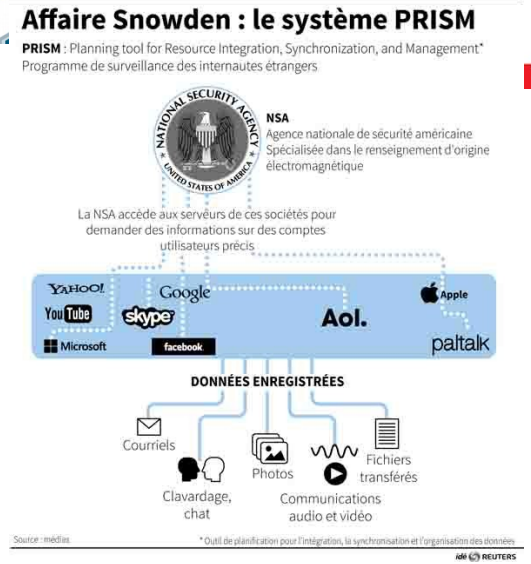
Nouveau Règlement Général sur la Protection des données
(Introduction 2012 -> Adoption 2016 -> Entrée en vigueur 25 mai 2018)

Contexte

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

Le RGPD, pourquoi maintenant ?





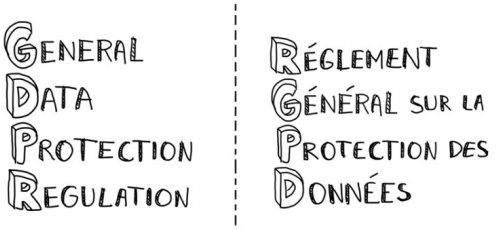
Contexte

Le RGPD, de quoi parle-t-on ?

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)



Law shopping

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.

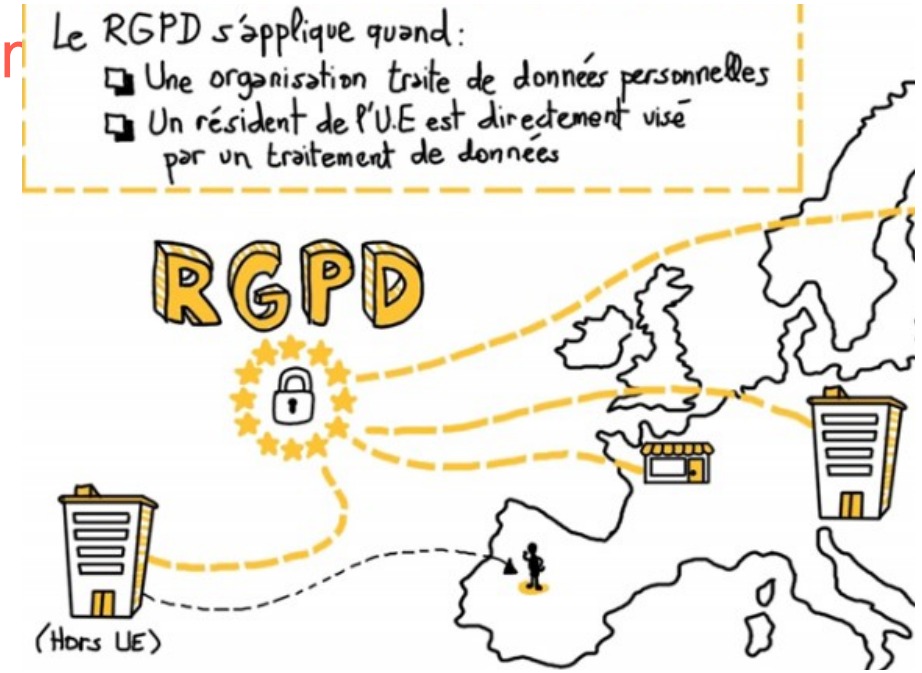
Règlements

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

Le RGPD, de quoi parle-t-on ?



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.).

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

Contexte

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

Loi nationale

MARGES DE MANOEUVRE NATIONALES

https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article1

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

https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=C2684DE6B0D372D975B936C152205424.tplgfr43s_1?cidTexte=LEGITEXT000006068624&dateTexte=20190601#LEGIART

Un peu de théorie

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://scinfolex.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
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://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 ensemble d'opérations, portant sur des données personnelles de la collecte à la destruction

Exemples :

- Gestion du personnel
- Maintenance du parc informatique
- Liste de diffusion
- Gestion des événements
- Procès verbaux des assemblées /commissions

...

Responsable de traitement

La personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.
Quel que soit la taille, le nombre de salariés, le nombre d'adhérents

Exemples :

Président de l'association
Gérant d'une entreprise
Maire d'une commune

...

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

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

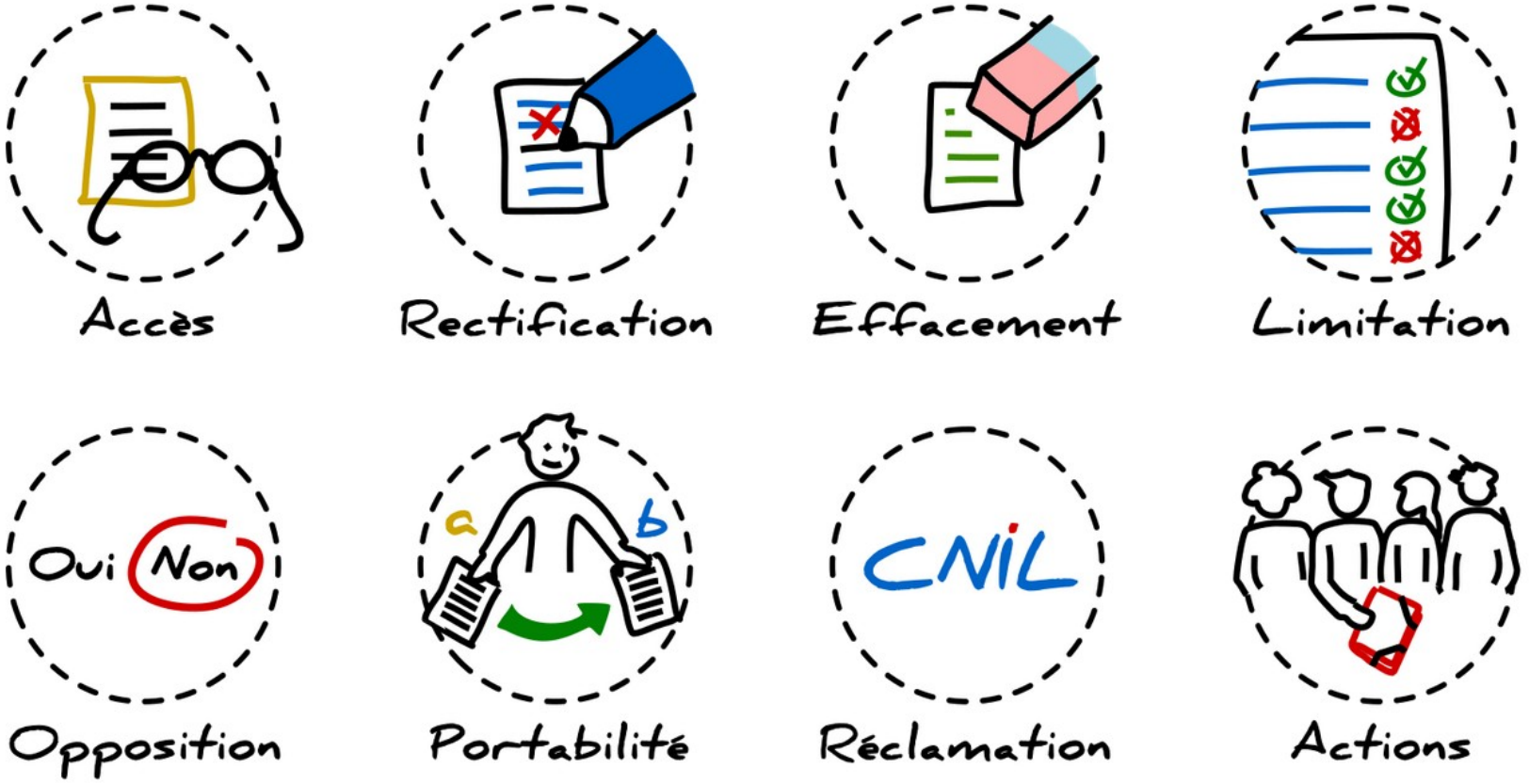
« *Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel* ***qui sont nécessaires*** *au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité 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

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

Passer à l'action

1-Constituez un registre de vos traitements de données

2-Faites le tri dans vos données

3-Respectez les droits des personnes

4-Sécurisez vos données

https://www.cnil.fr/fr/rgpd-passer-a-laction

1-Constituez un registre de vos traitements de données

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

Passer à l'action

2-Faites le tri dans vos données

REFERENTIEL DUREE DE CONSERVATION

2012
En attente
d'un nouveau référentiel

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

Une cartographie des outils et pratiques de protection de la vie privée

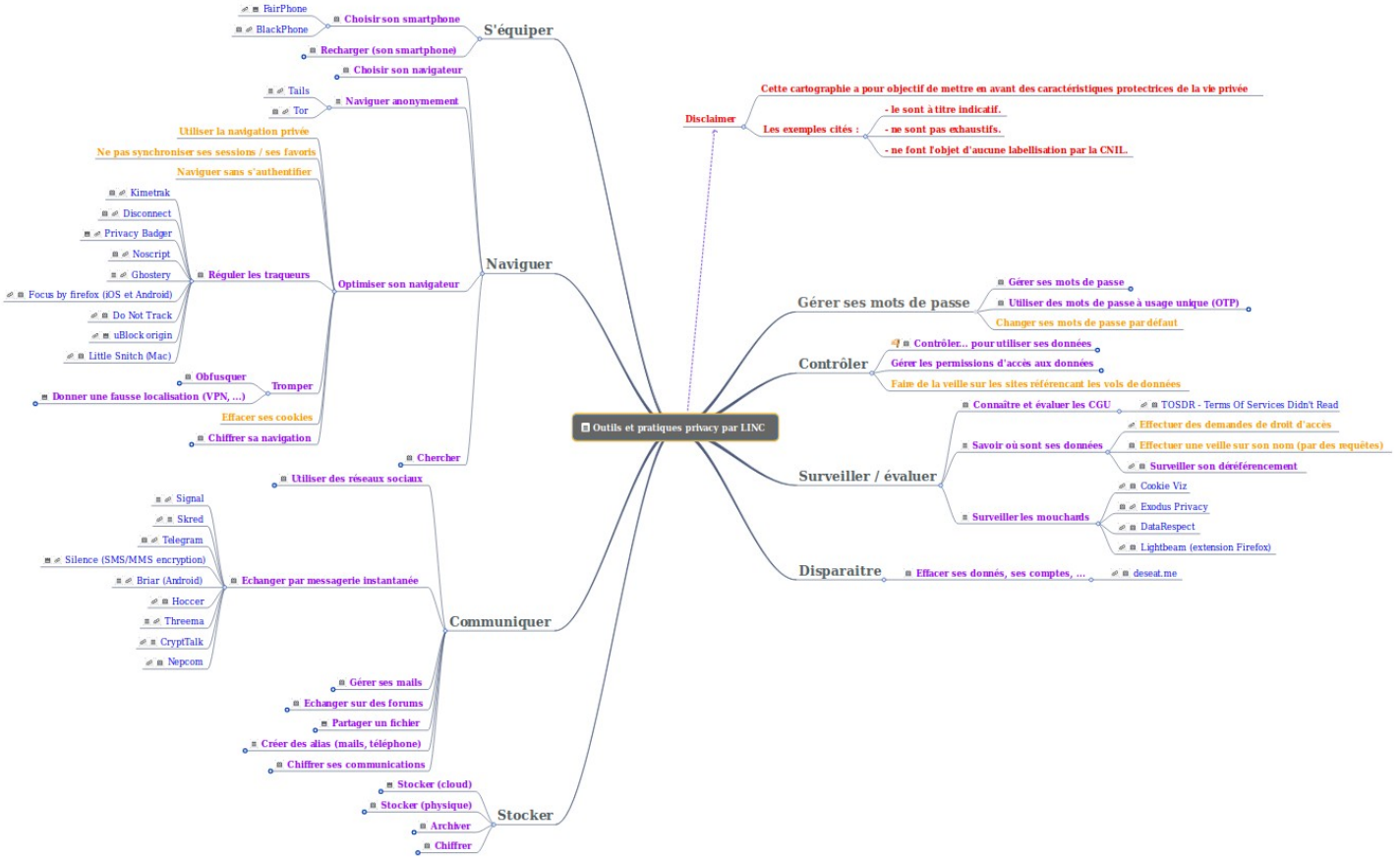
11 avril 2018

LINC publie sa cartographie d'exploration des outils et pratiques de protection de la vie privée, classées selon les usages et actions que chacun pouvons effectuer en ligne. Un outil pour donner à voir différentes caractéristiques ou technologies mises en œuvre par des porteurs de services, pour la protection des données.

https://linc.cnil.fr/fr/une-cartographie-des-outils-et-pratiques-de-protection-de-la-vie-privee

2-Faites le tri dans vos données

Passer à l'action



https://linc.cnil.fr/fr/une-cartographie-des-outils-et-pratiques-de-protection-de-la-vie-privee

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

3-Respectez les droits des personnes

.

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.

3-Respectez les droits des personnes

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

Informer

3-Respectez les droits des personnes

Exemples de mentions d'informations

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).

https://afcdp.net/
https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation
https://www.cnil.fr/fr/donnees-personnelles
https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche-1_que-faire-quand-votre-entreprise-communique-vend-en-ligne.pdf

3-Respectez les droits des personnes

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

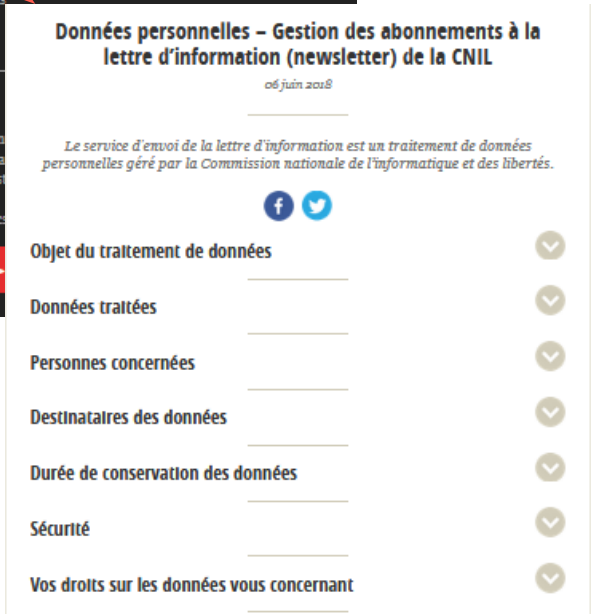
https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

Exemple de recueil du consentement

☐ J'accepte que ces données fassent l'objet de ce traitement

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

3-Respectez les droits des personnes



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

4-Sécurisez vos données

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

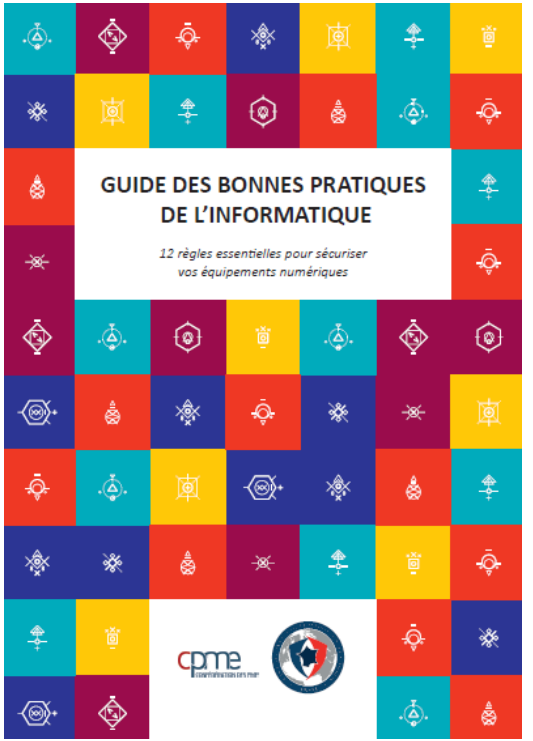
Passer à l'action

4-Sécurisez vos données

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



Passer à l'action

4-Sécurisez vos données

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

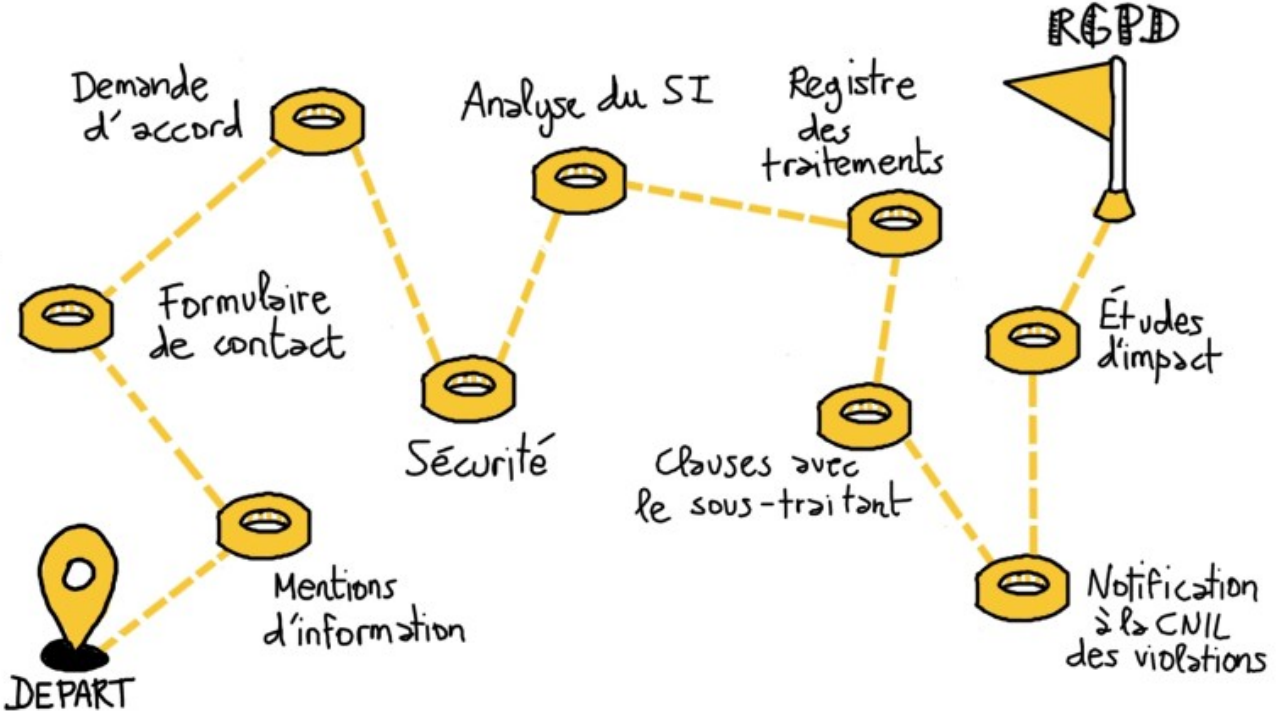
https://notifications.cnil.fr/notifications/index

Notification d'une violation de données personnelles

5 étapes pour finaliser votre notification

Passer à l'action

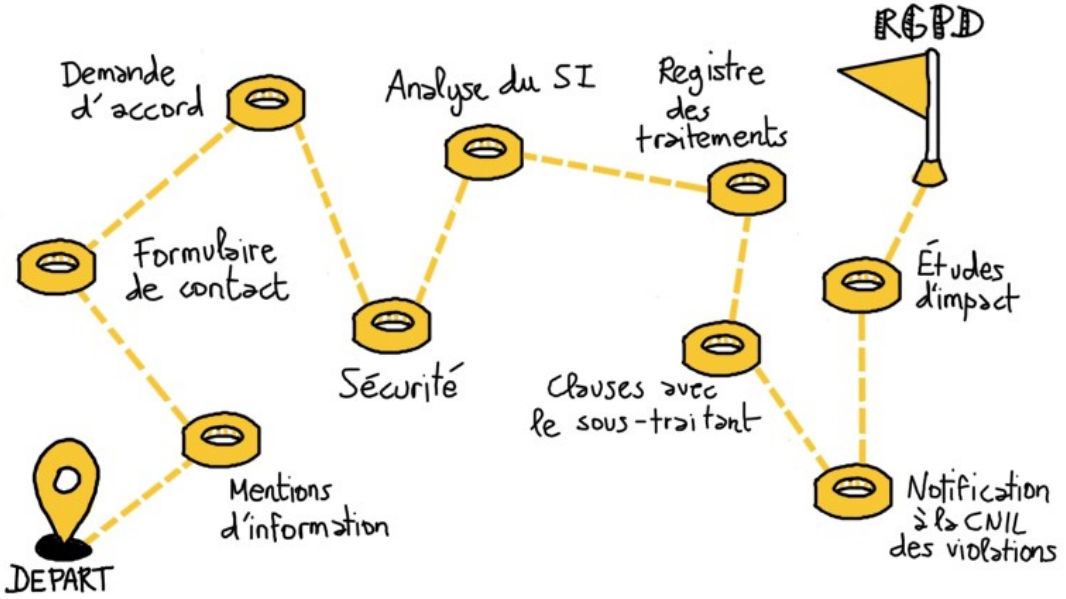
Vers la mise en conformité...



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

Vers la mise en conformité...

Délégué à la protection des données (DPD/DPO)



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

Impacts et intérêts

Obligations

Sanctions

Prise de conscience

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