Les droits des personnes concernées dans la nouvelle LPD

François Charlet

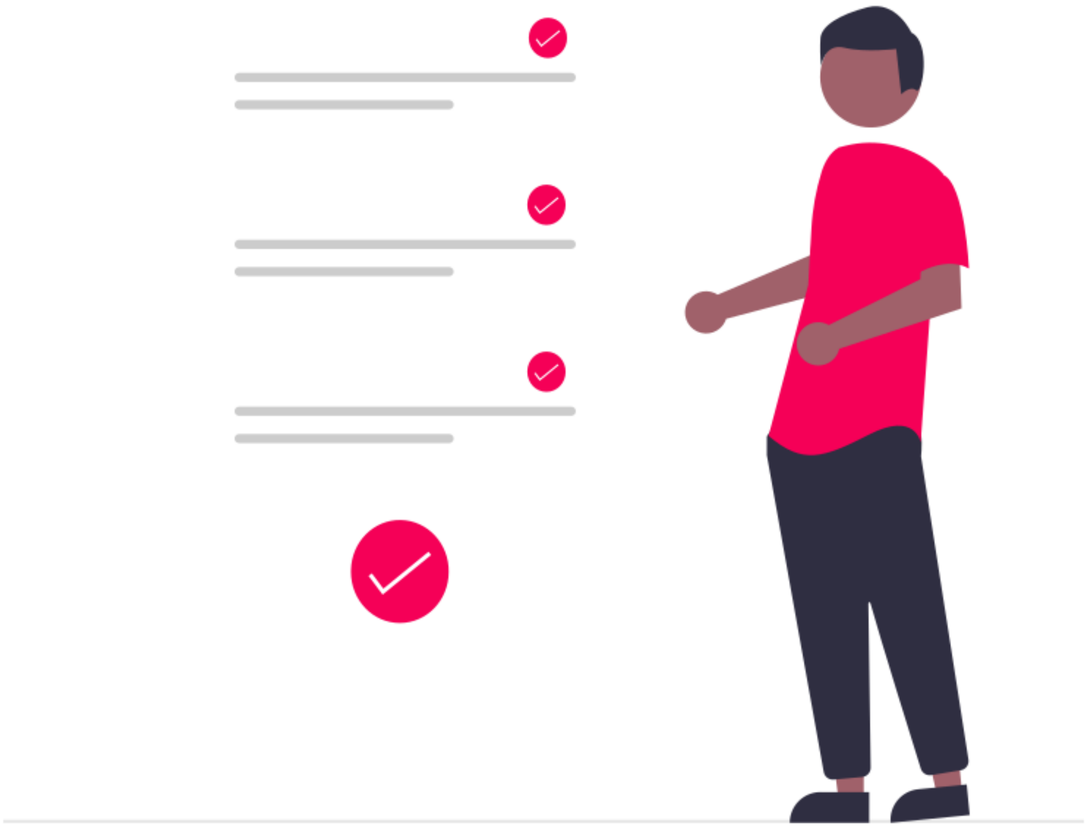
23 novembre 2023

De quoi parle-t-on ?

Les droits

des personnes concernées

- être informé sur les traitements
- ne pas faire l’objet d’une décision automatisée
- être informé en cas de violation de la sécurité des données
- **accéder aux données**
- demander la portabilité
- s’opposer au traitement
- **effacer les données**
- rectifier les données



Faut-il se préparer à recevoir des demandes ?

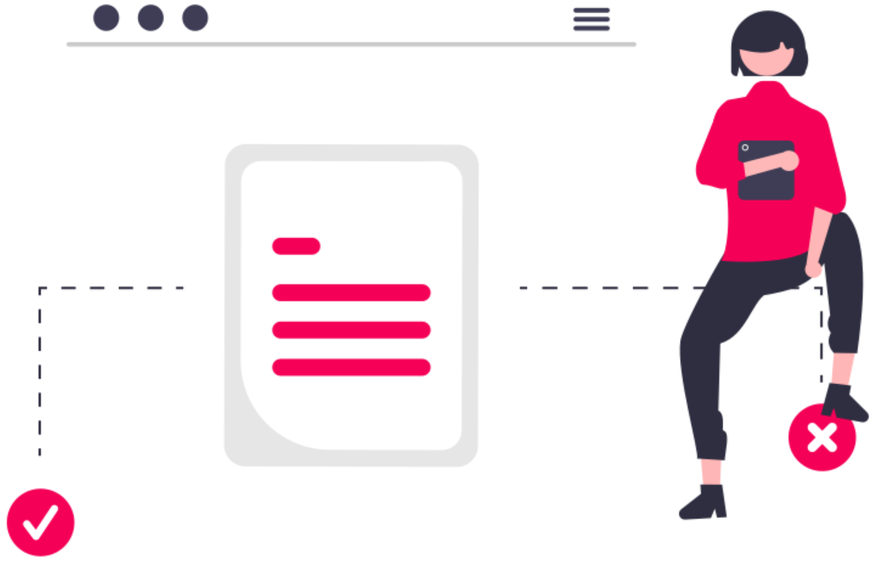
Oui, mais cela dépend de vos activités…

Les gens sont de plus en plus conscients de leurs droits et de l'utilisation (abusive ?) qui est faite de leurs données.

Un client ou collaborateur mécontent tentera souvent d'accéder à ses données pour « savoir ce qu'on lui cache ». Ou juste pour embêter.

Les médias évoquent le sujet de la protection des données et de la sécurité de l'information de plus en plus souvent.

Traiter les demandes prend du temps et coûte de l'argent.



Faut-il se préparer à recevoir des demandes ?

Coûts d'une demande d'accès : exemple

Poste de coût	Temps estimé
Réception et analyse de la demande	15 minutes
Vérification de l'identité	15 minutes
Vérification de la validité de la demande	60 minutes
Analyse de l'effort pour traiter la demande	60 minutes
Recherche et extraction des données et documents	30 heures (15 personnes, 2h/pers.)
Vérification des données et caviardage	5 heures
Transmission des données et informations	30 minutes
Clôture de la demande	15 minutes
Total	38 heures 15 minutes (ou env. 5 j/h)

Qui peut les exercer et comment ?

Qui peut les exercer et comment ?

Toute personne physique (vivante) peut faire une demande pour ses propres données ou une autre personne (vivante) qu'elle représente.

La demande peut être simple (« merci de me remettre une copie de toutes mes données », « arrêtez de m'envoyer de la publicité »), on ne doit pas se montrer formaliste.

Elle n'a normalement pas à être justifiée.

La demande peut se faire par écrit ou oralement.

Un mineur capable de discernement peut exercer ses droits seul.

Faut-il vérifier l’identité ?

Faut-il vérifier l’identité ?

La vérification de l’identité au moyen d’une ID ou d’autres données n’est pas toujours nécessaire et dépendra de la manière dont la demande est déposée, des données (sensibles) concernées, etc.

Si vous disposez d’un espace client/collaborateur en ligne avec une authentification forte, une demande déposée par ce biais ne nécessite normalement aucune autre mesure de vérification d’identité.

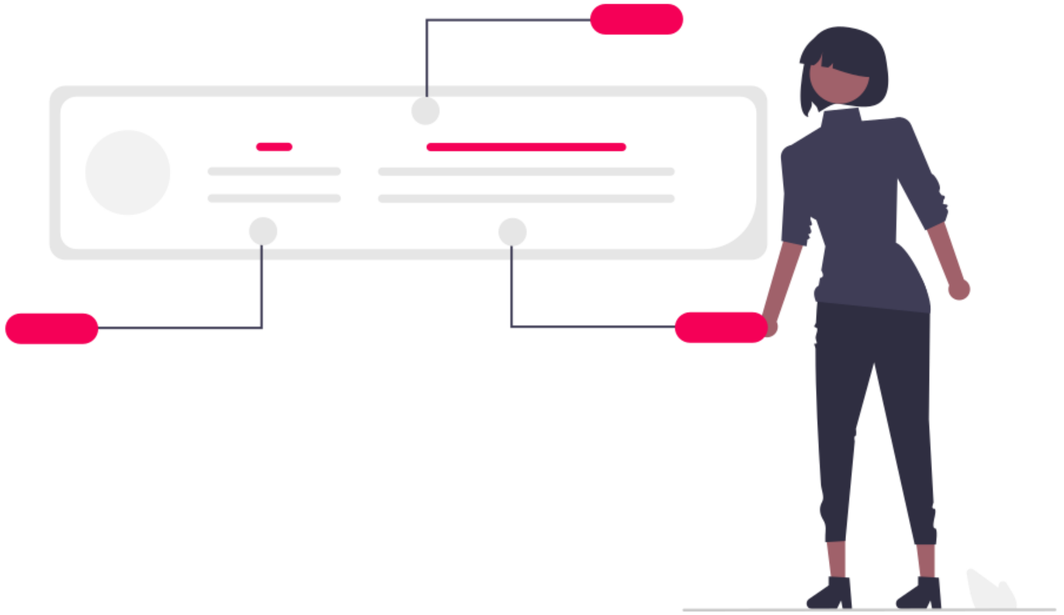
Demande d’accès

Demande d’accès

Quelles données ?

Uniquement

- les données auxquelles la LPD s’applique (art. 2 LPD)
- les données en tant que telles et non l’intégralité d’un document contenant lesdites données



Demande d’accès

Quelles données ?

Y compris

- les données qui n’existaient pas au moment du dépôt de la demande, mais qui ont été collectées avant la remise des données
- les données personnelles qui auraient dû être supprimées, mais qui ne l’ont pas été
- les données sur un lien de parenté ou une quelconque autre relation entre la personne concernée et un autre individu (mais rien d’autre sur ce dernier)

Demande d’accès

Quelles données ?

Y compris

- les faits et les jugements de valeur
- les données figurant dans les e-mails de tout collaborateur ou mandataire de l’entreprise qui contiennent des données personnelles
- les données qui figurent dans d’autres bases de données, dans les archives, sur l’ordinateur ou le smartphone professionnel (ou privé, mais utilisé à des fins professionnelles) d’un collaborateur, chez un sous-traitant, un responsable conjoint du traitement ou au siège d’une autre société d’un même groupe

Demande d’accès

Quelles données ?

Y compris

- les données personnelles dérivées (créées sur la base des données personnelles déjà à disposition)
- les données personnelles figurant dans les notes internes et les documents cachés ou non officiels

Demande d’accès

Quelles données ?

Mais pas

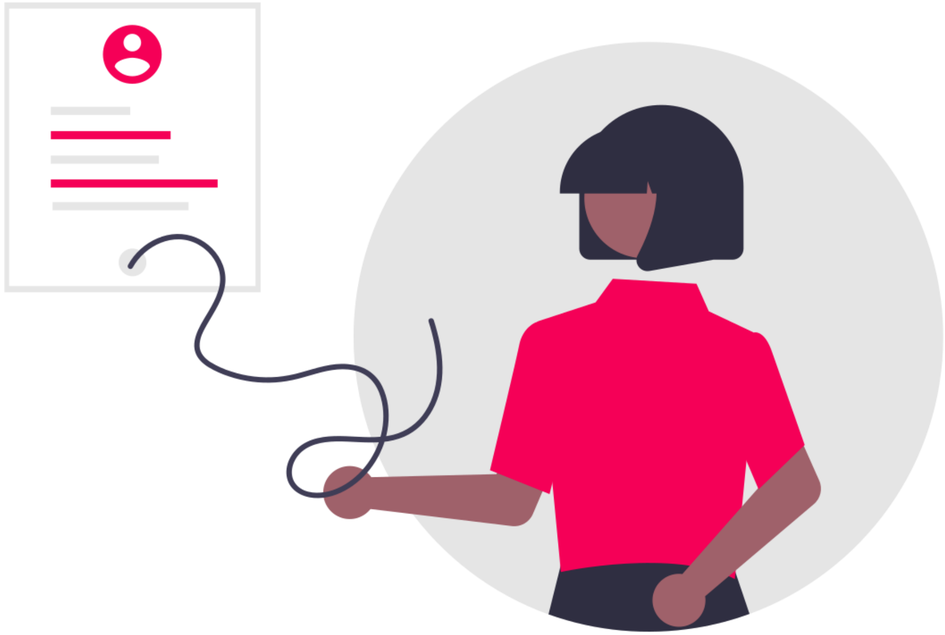
- des données qui n’existaient pas et qui devraient être générées spécialement pour répondre à la demande
- les données qui ont été détruites après la réception de la demande, mais avant la réponse du responsable du traitement, en raison de l’expiration d’un délai de conservation (controversé ?)
- les données qui ont été effacées ou détruites, physiquement ou logiquement, avant la réception de la demande, et qui ne peuvent plus être récupérées (quid des backups ?)

Demande d’accès

Quelles données ?

Mais pas

- les données personnelles qui ont déjà été transmises à la personne concernée par le passé (en principe et sauf si elles sont requises)
- les données concernant des tiers qui doivent être retirées, voire caviardées
- les données qui ne figurent pas sur un support (p. ex. celles qui se trouvent dans la mémoire d’un être humain)



Demande d’accès

Quel format pour les données ?

Les données sont fournies par écrit ou sous la forme dans laquelle elles se présentent. Le format numérique doit être standard. Il n’est pas requis de transcrire par écrit des enregistrements audios.

La personne concernée doit comprendre les données et leur signification, si nécessaire des explications doivent être fournies.

On ne peut pas renoncer à fournir les données brutes et ne communiquer qu’un résumé explicatif.

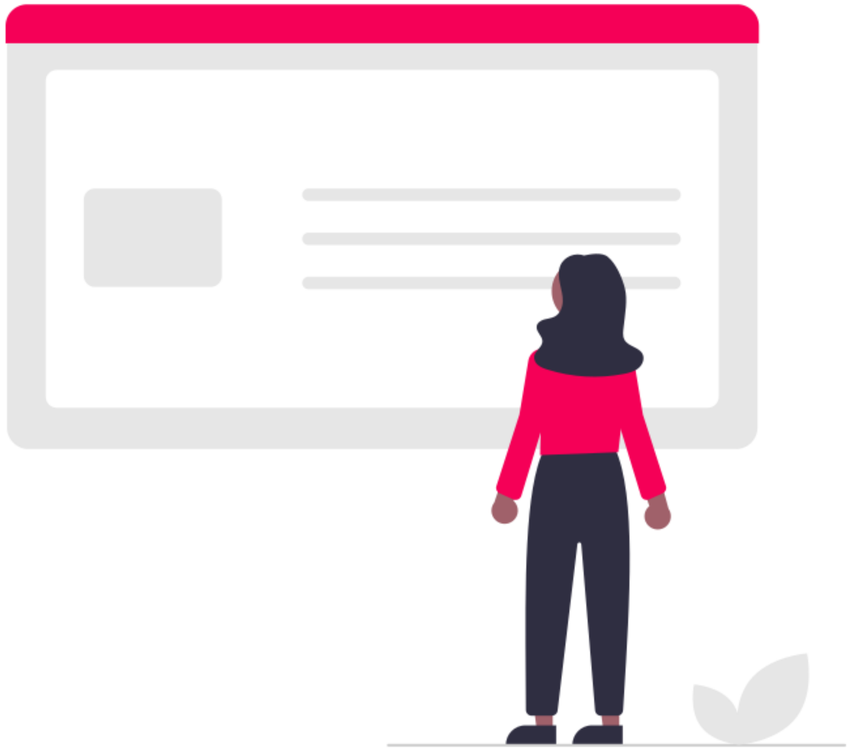
Les notes manuscrites illisibles doivent être déchiffrées avant d’être transmises. Il n’y a en principe pas besoin de traduire les données.

Demande d’accès

Quelles autres informations ?

Celles de la déclaration de protection des données ainsi que

- les informations disponibles sur l’origine des données personnelles, si elles n’ont pas été collectées auprès de la personne concernée
- l’identité des destinataires (en droit européen ; quid en droit suisse ?)
- et les autres informations mentionnées à l’art. 25 LPD si elles ne figurent pas dans la déclaration.



Demande d’accès

Participation financière ?

Le traitement de la demande est en principe gratuit.

Des exceptions existent, en particulier dans les cas où la communication des données exige des efforts disproportionnés. Ne pas être organisé ne permet pas d’invoquer cette exception.

CHF 300 maximum par demande.

La personne est informée de la demande de participation et doit se déterminer sous 10 jours (refuser, payer, agir devant les tribunaux en exécution du droit d’accès, dénonciation au PFPDT, etc.)

Demande d’accès

Dans quel délai répondre ?

30 jours calendaires à la réception de la demande.

Délai prolongeable plusieurs fois si cela s’avère objectivement nécessaire et que cela ne porte pas atteinte au principe de la bonne foi. Il est obligatoire d’indiquer dans la prolongation dans quel délai parviendra la réponse.

Si une participation aux frais est demandée par le responsable du traitement, le délai de 30 jours est « réinitialisé » et commence à la fin du délai de réflexion de 10 jours (même si la personne concernée s’acquitte immédiatement du montant réclamé).

Demande d’accès

Des limites ?

Il est possible de refuser, restreindre ou différer la remise des données (art. 26 LPD) si :

- Loi fédérale
- Intérêts prépondérants de tiers
- Demande manifestement infondée (p. ex. poursuit un autre but que la protection des données)
- Intérêts prépondérants du responsable du traitement en l’absence de communication à des tiers

Droit à l’effacement

Etapes de mise en oeuvre

Voir p. 20.

Demande d’accès

Quelques conseils

1. Se rappeler que les demandes d’accès peuvent être déposées par tous les moyens et auprès de n’importe quel collaborateur
2. Proposer un formulaire en ligne vers lequel diriger les personnes concernées
3. Définir un processus et une matrice des responsabilités
4. Donner des instructions aux collaborateurs sur la manière de stocker/traiter les données et les lieux pour ce faire
5. Se préparer à devoir fournir de grandes quantités de données personnelles
6. Se préparer à devoir caviarder des documents, e-mails, images, etc.
7. Préparer des modèles de correspondances

Droit à l’effacement

Droit à l’effacement

Pour quel motif ?

Selon l’art. 32 al. 2 let. c LPD, le droit à l’effacement ne semble pouvoir être exercé qu’en cas d’atteinte illicite à la personnalité et sous la forme d’une action au tribunal civil… 😐

L’effacement intervient en réalité dans les cas suivants au moins :

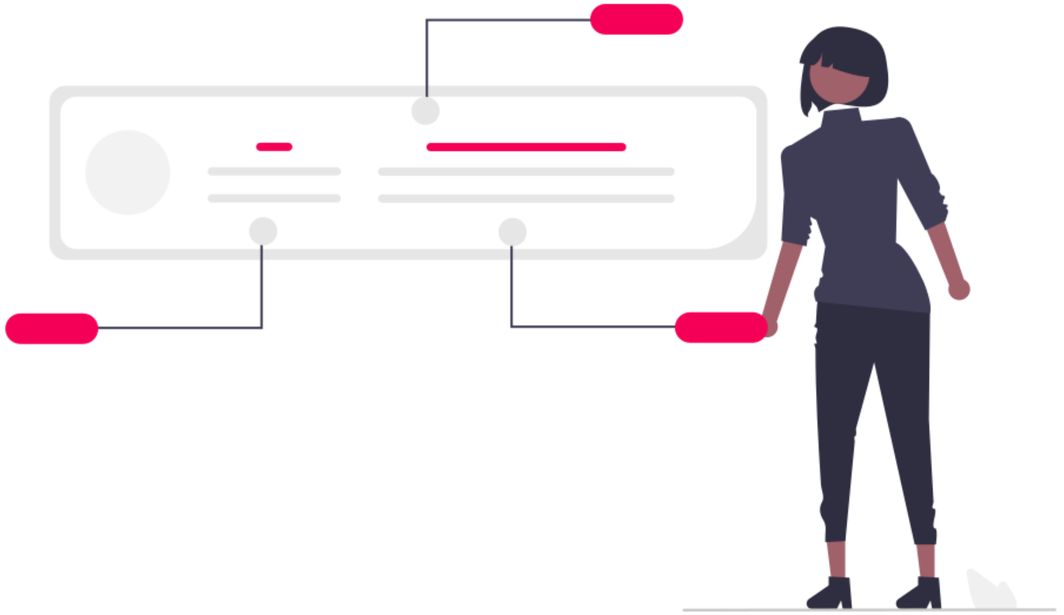
- (Données plus nécessaires aux finalités)
- Retrait du consentement
- Opposition au traitement fondé sur l’intérêt légitime
- Opposition au traitement à des fins marketing
- (Traitement illicite)
- (Obligation légale)

Droit à l’effacement

Quelles données ?

Uniquement

- les données auxquelles la LPD s’applique (art. 2 LPD)
- les données visées par la demande d’effacement

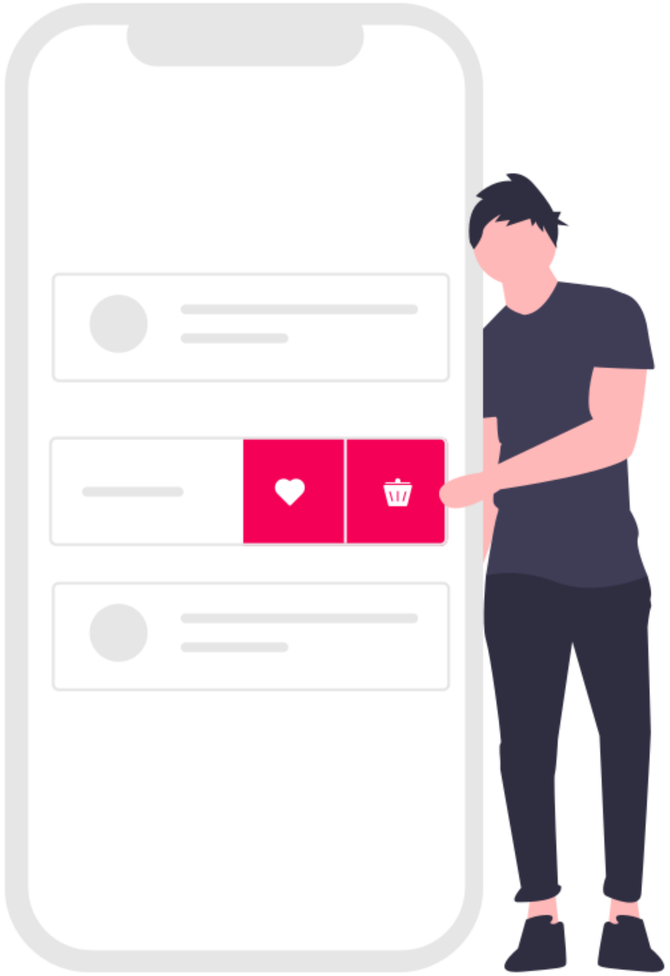


Droit à l’effacement

Quelles données ?

Y compris

- les données qui sont traitées chez un sous-traitant ou responsable conjoint du traitement ;
- les données qui se trouvent dans les systèmes de sauvegardes (backup), dans les archives, dans le cloud ;

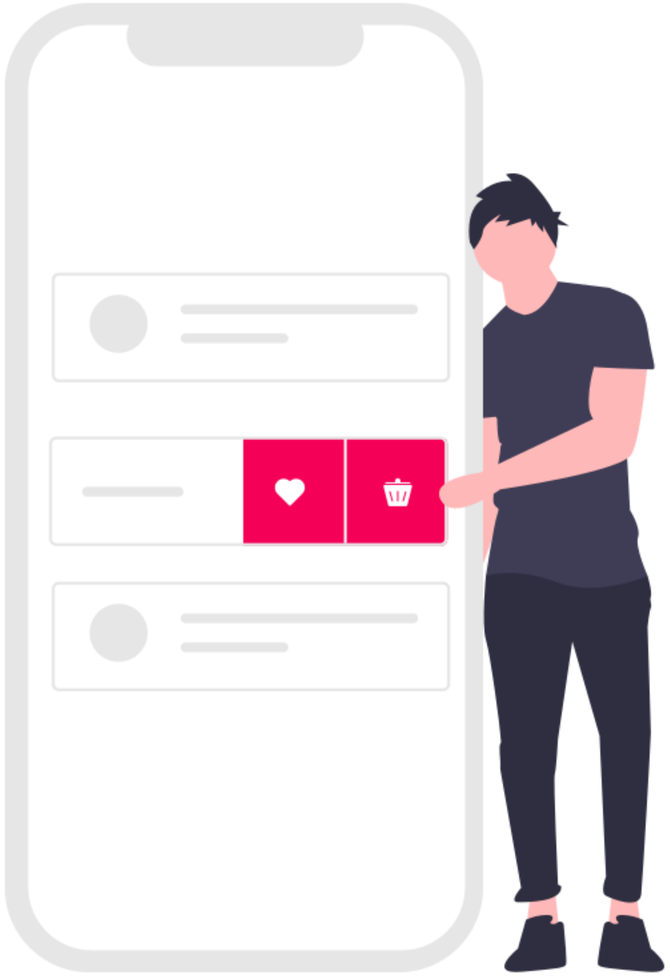


Droit à l’effacement

Quelles données ?

Y compris

- les données au format numérique, au format papier et celles conservées sur un autre support ;
- les données structurées de même que les données non structurées (p. ex. fichiers textes, e-mails, etc.) ;
- les copies des données.



Droit à l’effacement

Des limites ?

Pas spécialement codifiées mais on peut appliquer par analogie celles du droit d’accès

Quid des données librement accessibles ?

Il est possible de refuser, restreindre ou différer la suppression si :

- une loi fédérale impose la conservation (pendant une certaine durée) ;
- les intérêts – prépondérants – du responsable du traitement l’exigent (p. ex. délais de prescription, autres besoins internes objectifs)

Droit à l’effacement

Dans quel délai répondre ? Participation aux frais ?

Pas de délai prévu dans la LPD.

Par analogie au droit d’accès : 30 jours calendaires à la réception de la demande.

Par analogie au droit d’accès : délai prolongeable si cela s’avère objectivement nécessaire et que cela ne porte pas atteinte au principe de la bonne foi.

Pas de possibilité légale de facturer une participation aux frais.

Droit à l’effacement

Etapes de mise en oeuvre

1. Vérifier si les données dont l’effacement est demandé existent

2. Déterminer si elles peuvent être effacées (délai légal de conservation ? autre délai de conservation ? autre motif justifiant la conservation ?)

3. Répondre à la personne concernée en indiquant quelles données ont été supprimées, quelles données doivent être conservées (pourquoi et pour combien de temps), à quels destinataires les données ont été communiquées

Droit à l’effacement

Quelques conseils

1. Rappel : interdiction de conserver les données plus longtemps que nécessaire aux finalités.
2. Collecter le moins de données possible de manière générale
3. Ne pas paniquer lorsqu’on reçoit une demande de ce type (facile à dire 🙄)
4. Ne pas oublier les données traitées par les sous-traitants
5. Ne pas oublier les données publiées sur un site web (public ou non)
6. Ne pas oublier les données dans les archives et sauvegardes
7. Réfléchir avant d’appuyer sur *delete*