DEVOIR DE TRANSPARENCE, GESTION DU CONSENTEMENT ET DES DROITS DES PERSONNES CONCERNÉES

François Charlet

27 avril 2023

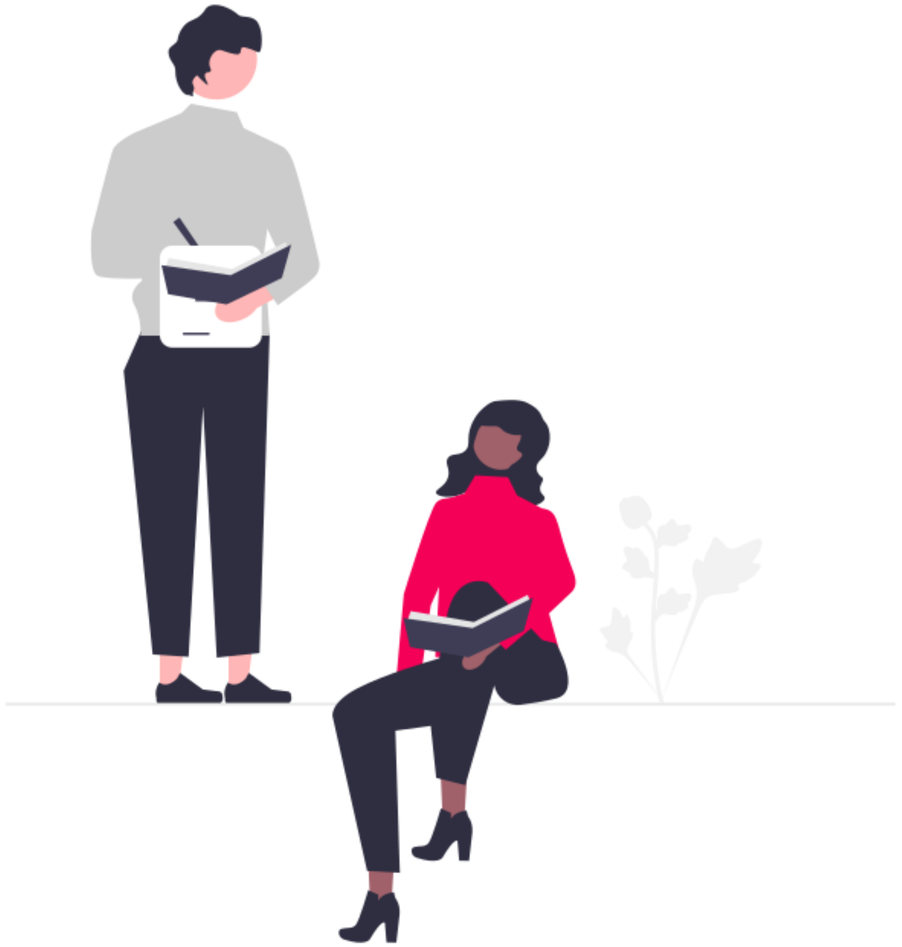
Comment rédiger une déclaration de protection des données ?

Comment rédiger une déclaration de protection des données ?

D’abord, réfléchir…

Les informations à fournir vont dépendre principalement des **activités** et traitements pour lesquels vous collectez les données.

Les informations doivent permettre à la personne concernée de faire valoir ses droits et pour assurer la **transparence** des traitements (art. 19 LPD).



Comment rédiger une déclaration de protection des données ?

Puis préparer…

- qui traite les données personnelles ?
- quelles données sont collectées ?
- comment sont-elles collectées ?
- comment sont-elles utilisées et dans quels buts ?
- quelle est la base juridique qui permet l'utilisation des données ?
- avec qui sont-elles partagées ?
- vers quels pays sont-elles transférées et avec quelles garanties ?
- comment sont-elles sécurisées ?
- combien de temps sont-elles conservées ?
- quels sont les droits de chaque personne concernée ?
- qui est la personne de contact et comment la contacter ?

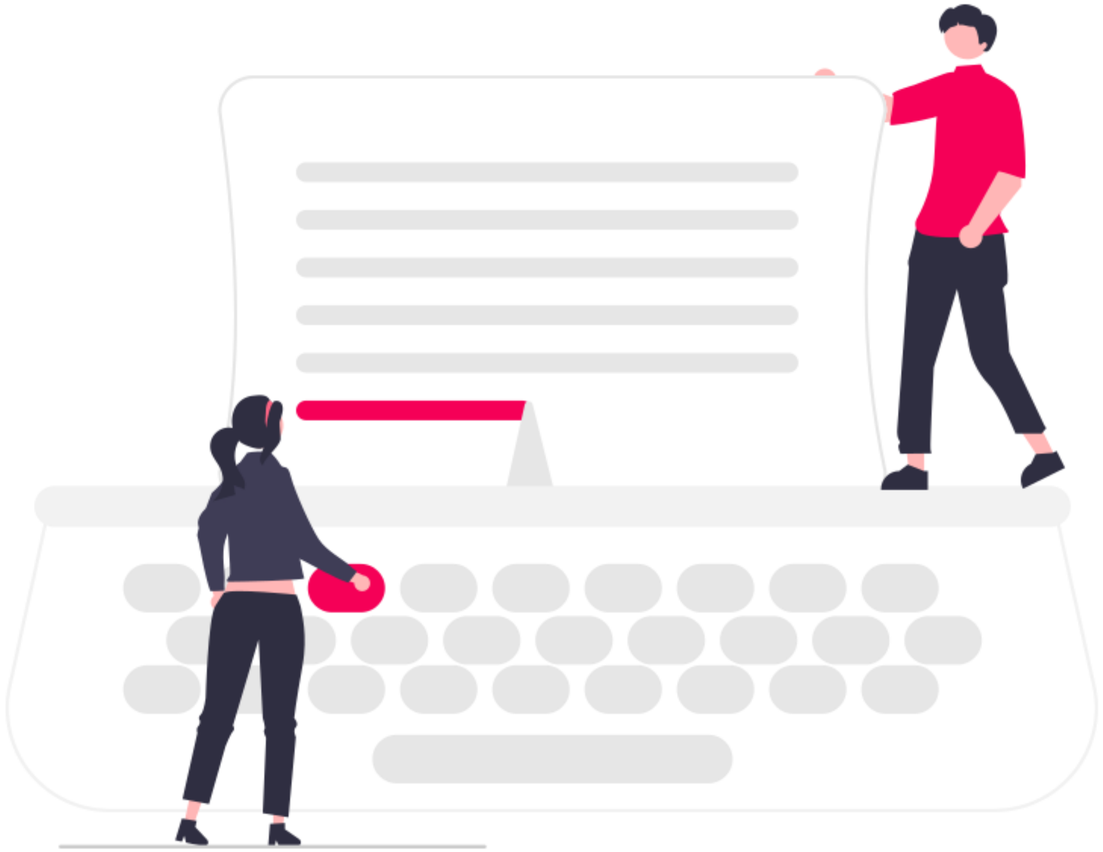
Comment rédiger une déclaration de protection des données ?

Ensuite rédiger…

Il faut ensuite réaliser la **quadrature du cercle** : être complet, bref et clair.

Conseils :

- Evitez le conditionnel ainsi que les formulations potestatives et générales.
- Dites ce que vous faites réellement, pas ce que vous pourriez faire un jour peut-être selon l'humeur du jour et la météo.
- Si des traitements futurs sont prévus, vous pouvez le dire en avance.

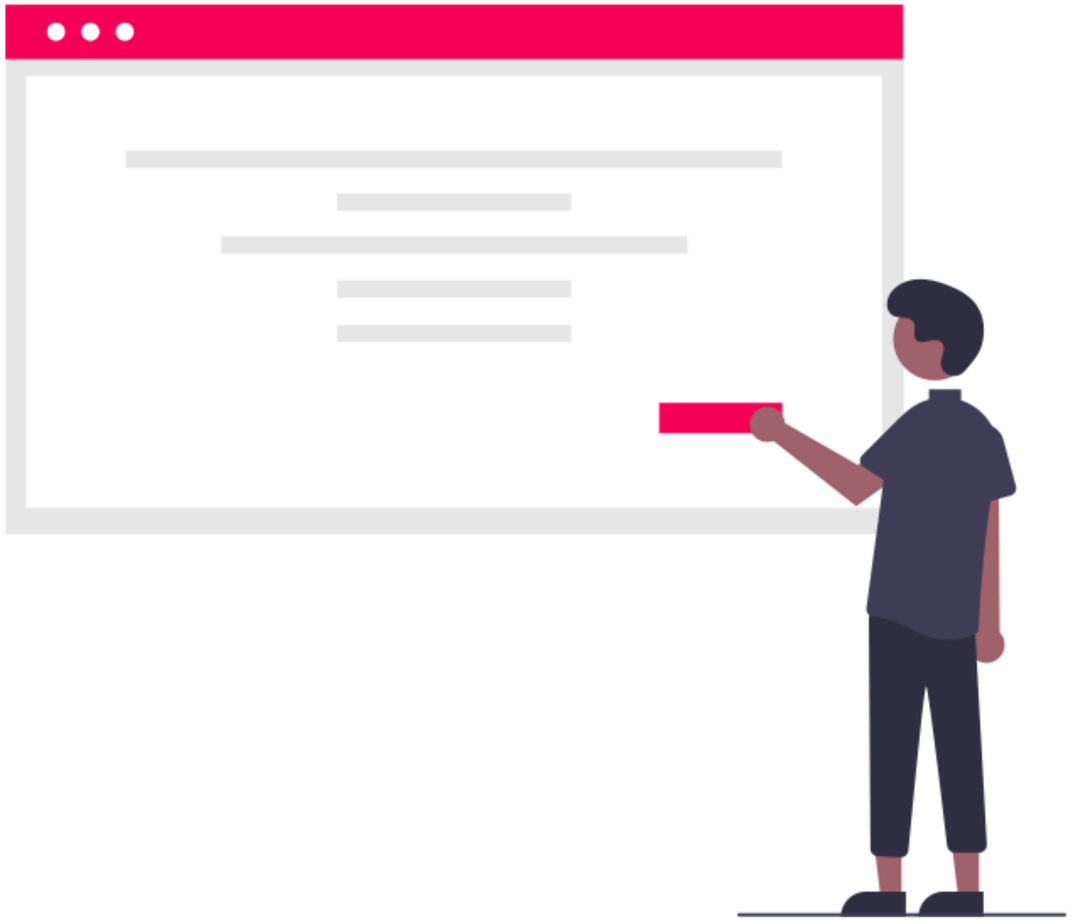


Comment rédiger une déclaration de protection des données ?

Enfin mettre à disposition

Attention, deux situations sont possibles (art. 19 al. 3 à 5 LPD)

- Données collectées auprès de la personne concernée
- Données collectées auprès de quelqu'un d'autre (autorité, broker, voisin, conjoint, médecin, assureur, etc.)



Comment rédiger une déclaration de protection des données ?

Exceptions totales à l'information (exemples)

L'obligation d'informer tombe totalement lorsque (art. 20 al. 1 et 2 LPD)

- la personne concernée dispose déjà de toutes les informations nécessaires
- le traitement de données personnelles est prévu par la loi (p. ex. LPP)
- le responsable du traitement est lié par une obligation légale de garder le secret (p. ex. art. 321 CP)
- les données ne sont pas collectées auprès de la personne concernée et que l'information est impossible à donner ou que le devoir d'informer nécessite des efforts disproportionnés (≠ simples difficultés ou manque d'organisation)

Comment rédiger une déclaration de protection des données ?

Exceptions partielles à l'information (exemples)

Le responsable du traitement peut restreindre, différer ou renoncer à fournir les informations lorsque (art. 20 al. 3 let. a, b et c LPD)

- les intérêts prépondérants de tiers l'exigent (p. ex. engagement de confidentialité)
- l'information empêcherait le traitement d'atteindre son but (p. ex. enquête interne)
- le responsable du traitement est une personne privée, ses intérêts prépondérants l'exigent et il ne communique pas les données à un tiers

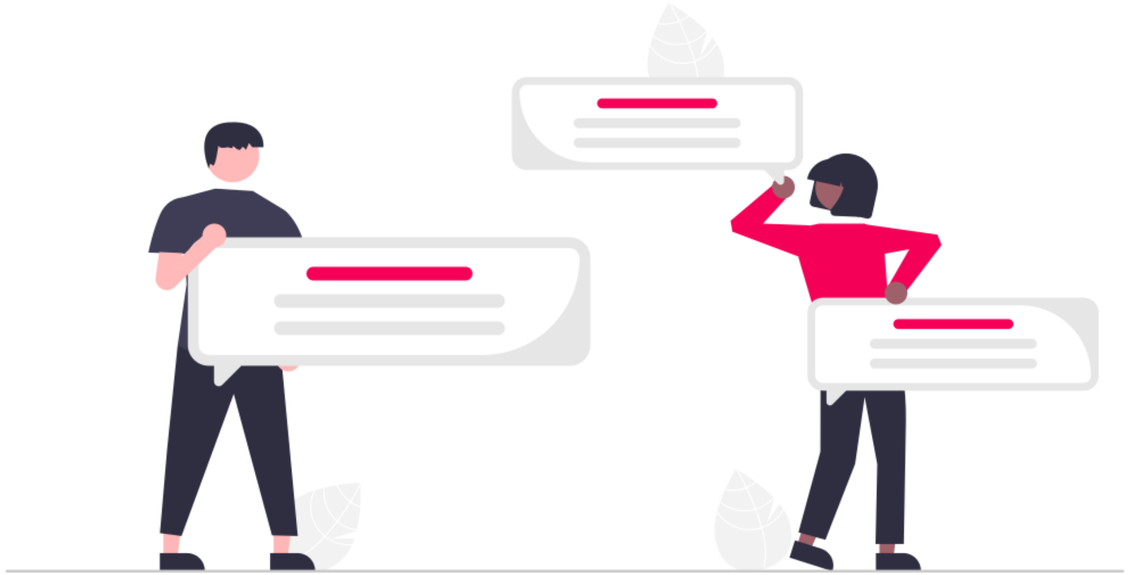
Comment rédiger une déclaration de protection des données ?

Données obtenues de sources publiques librement accessibles

Les règles de la protection des données sont applicables aux données librement accessibles, notamment quant à l'information à donner aux personnes concernées.

L'obligation d'information est d'autant plus importante lorsque le responsable du traitement entend utiliser les données dans un **but différent** de celui pour lequel la personne concernée les a rendues accessibles.

La personne concernée doit avoir rendu ses données accessibles à tout un chacun de façon **volontaire et consciente**.



Comment rédiger une déclaration de protection des données ?

Résumé

1. Fournir aux personnes concernées toutes les informations requises, selon les circonstances (art. 19 LPD)

2. Etre transparent, complet, clair et concis

3. Prévoir une présentation adaptée aux petits écrans et aux mineurs

4. Le cas échéant, déterminer si une exception ou restriction au devoir d'informer entre en ligne de compte (art. 20 LPD)

5. Données librement accessibles ≠ LPD inapplicable (art. 30 al. 3 LPD)

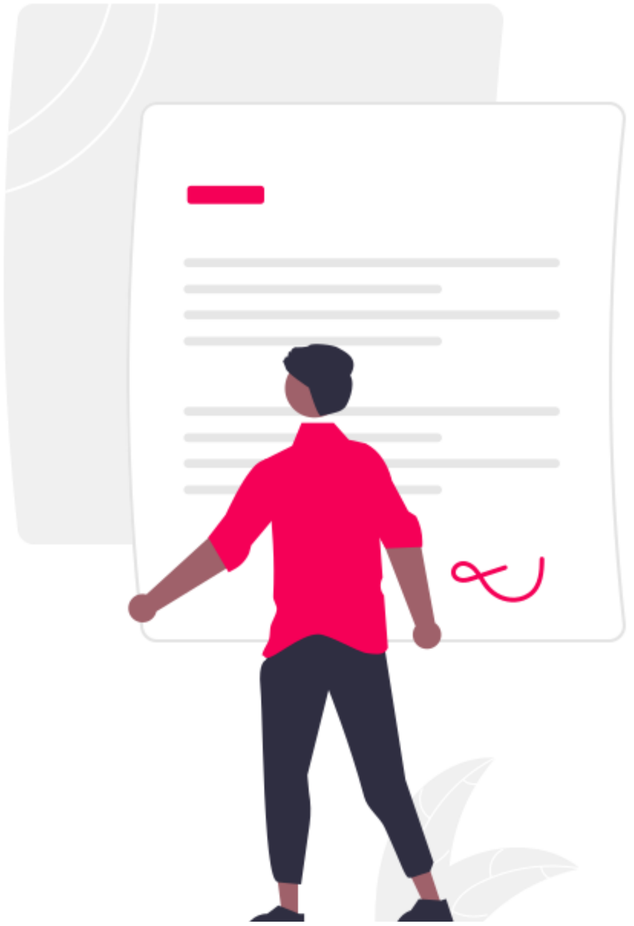
Comment gérer le consentement des personnes concernées lorsqu’il est nécessaire ?

Comment gérer le consentement des personnes concernées

Rappel : consentement ≠ contrat (et vice versa)

Le **consentement** permet à la personne concernée de décider librement si elle accepte que ses données personnelles soient traitées dans le but qui lui est exposé ; en outre, son consentement peut être retiré en tout temps et sans condition, si elle le souhaite.

Le **contrat** ne peut pas être conclu ou exécuté sans le traitement de données indiqué comme nécessaire : la personne concernée n'est donc pas libre d'accepter ou de refuser le traitement de données si elle désire que le contrat soit conclu. D'ailleurs, un contrat (et les traitements de données qui lui sont nécessaires) ne peut souvent être résilié qu'à des conditions particulières.



Comment gérer le consentement des personnes concernées

Rappel : règles de validité du consentement

La personne doit exprimer son consentement (art. 6 al. 6 et 7 LPD) :

1. à un ou plusieurs traitements spécifiques (= lien avec les finalités)
2. de manière libre (= sans pression, possibilité concrète de donner ou de retirer le consentement en tout temps)
3. de manière claire (= pas d'ambiguïté, peut se déduire du comportement)
4. après avoir été dûment informée au sujet des traitements
5. de manière explicite lorsque la loi l'exige (= déclaration affirmative orale ou écrite)

Comment gérer le consentement des personnes concernées

Deux étapes

1. **Informer** la personne concernée conformément aux exigences légales, en indiquant également le caractère obligatoire ou facultatif du traitement de données et les éventuelles conséquences en cas de refus ou de retrait du consentement

2. Donner à cette personne la **possibilité d'accepter ou de refuser** librement.

Comment gérer le consentement des personnes concernées

Documenter le consentement

Le principe de **proportionnalité** s'applique, il faut éviter de traiter des données personnelles si possible.

Faut-il absolument **conserver la trace** de chaque (retrait de) consentement ?

Comment gérer le consentement des personnes concernées

Documenter le consentement

Selon les besoins (⚠️ proportionnalité ⚠️), on conservera

- une trace du (retrait du) consentement, le cas échéant associée à une information permettant d'identifier la personne concernée si cela s'avère nécessaire à certaines finalités (e-mail, n° de client…)
- l'ampleur du (retrait du) consentement
- les informations qui ont été fournies pour l'obtention du consentement
- la date du (retrait du) consentement
- la manière dont la personne concernée a donné ou retiré son consentement.

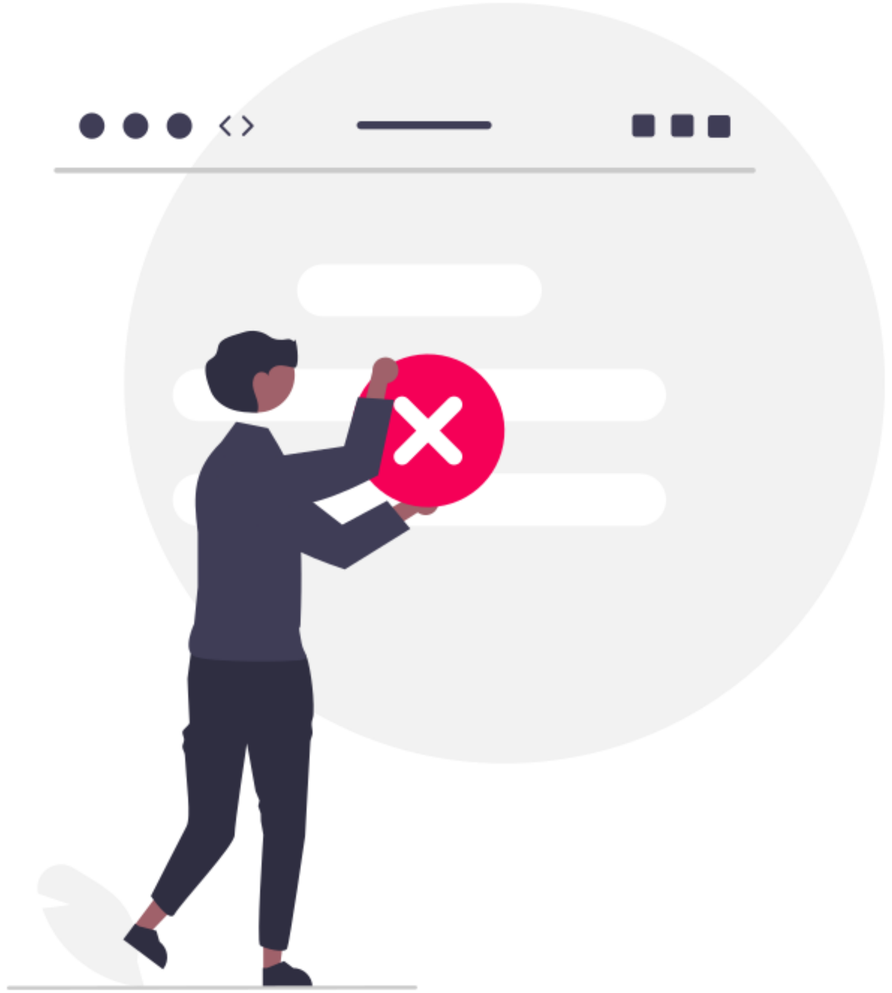
Comment gérer le consentement des personnes concernées

Retrait du consentement

La personne peut changer d'avis en tout temps.

Ce changement d'avis doit pouvoir être réalisé **facilement**, **à n'importe quel moment**.

Le retrait du consentement doit être aussi facile qu'il a été donné (pas de formalisme « excessif »).



Comment gérer le consentement des personnes concernées

Conséquences du retrait du consentement

Le traitement visé doit s’arrêter immédiatement.

Les données doivent être supprimées immédiatement (sauf délai légal ou délai propre de conservation, autre traitement).

Faut-il « blacklister » la personne qui retire son consentement afin d’être en mesure de respecter sa volonté à l’avenir ?

Comment gérer le consentement des personnes concernées

Consentement dans les rapports de travail (par exemple)

Quid de la liberté de choix lorsqu'il y a un rapport hiérarchique ou une dépendance ?

La manière dont l'employeur cherche à obtenir le consentement, les informations présentées, leur complétude, l'ampleur et le but du traitement sont notamment des éléments à considérer pour déterminer si le consentement des travailleurs a été donné librement.

Un employeur peut faire reposer un traitement sur le consentement de ses travailleurs, mais il doit être capable de démontrer que les travailleurs ne subissent **aucun désavantage d'aucune sorte en cas de refus**.

Comment gérer le consentement des personnes concernées

Résumé

1. Déterminer si on souhaite donner à la personne concernée la possibilité d'accepter ou de refuser un ou plusieurs traitements de données

2. Vérifier si le consentement peut être obtenu de manière valide (⚠️ situations de dépendance/rapport hiérarchique)

3. Informer la personne concernée (information usuelle + information spécifique liée au consentement)

4. Documenter le consentement, si nécessaire

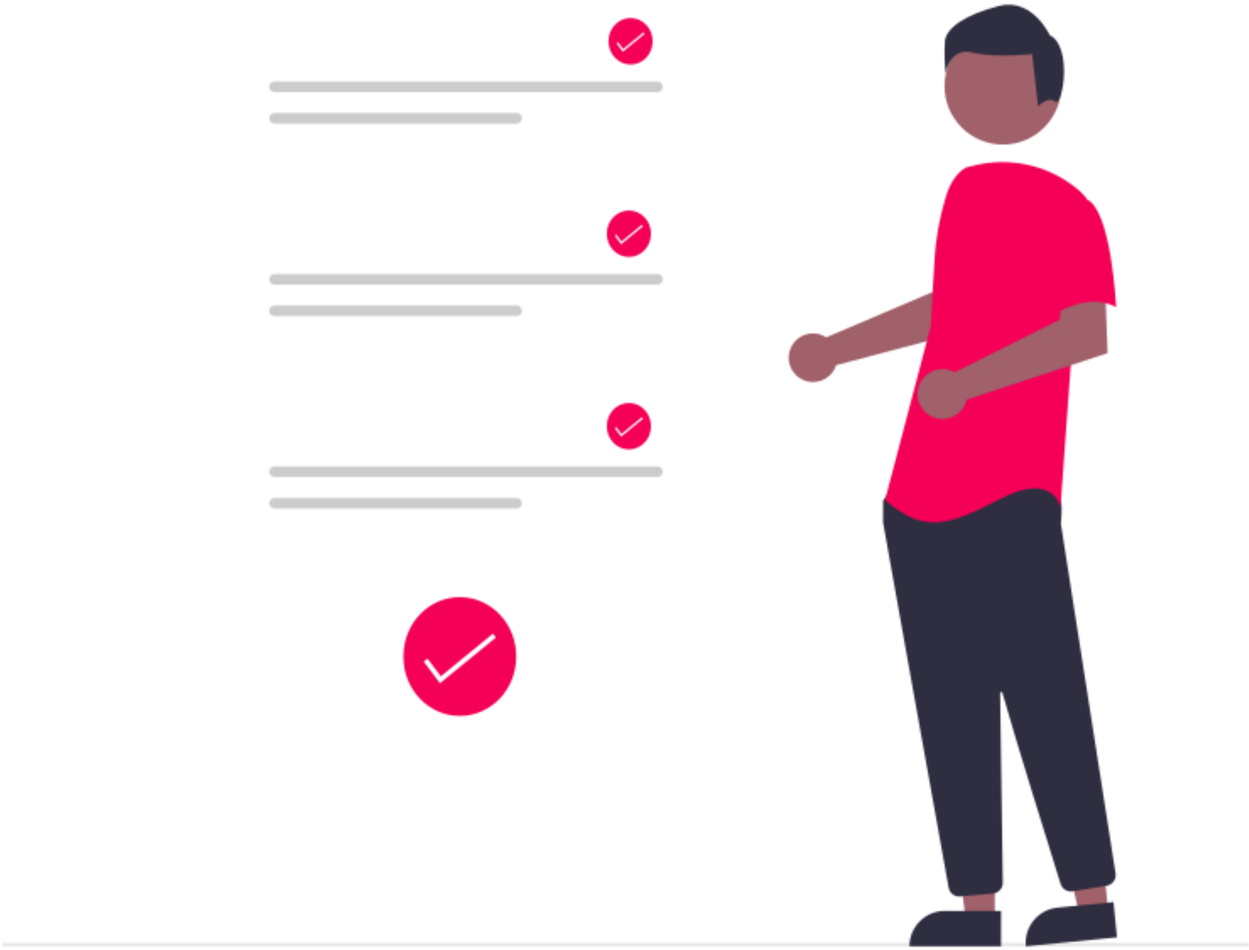
5. Se préparer au retrait du consentement et à ses conséquences

Comment préparer et gérer les demandes des personnes ?

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



Comment préparer et gérer les demandes des personnes ?

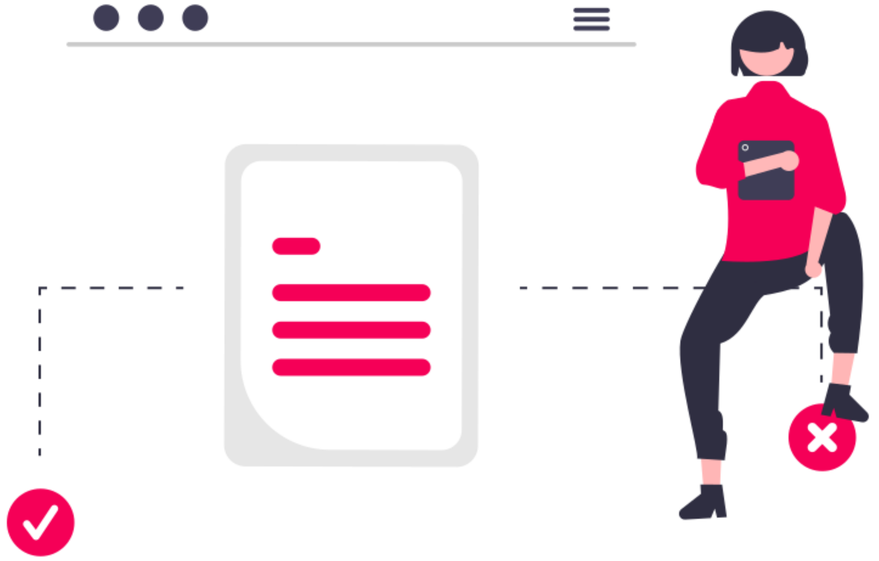
Pourquoi se préparer à recevoir des demandes ?

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 ».

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.



Comment préparer et gérer les demandes des personnes ?

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)

Demande d’accès aux données

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : généralités

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 »), on ne doit pas se montrer formaliste. Elle n’a pas à être justifiée.

La demande doit se faire par écrit (ou oralement).

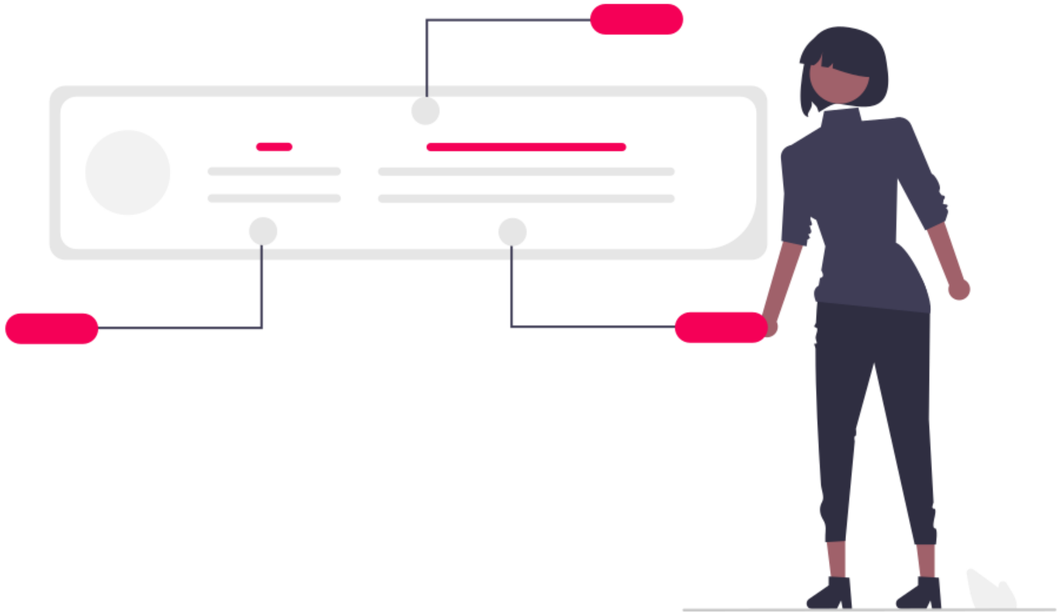
La vérification de l’identité au moyen d’une ID ou d’autres données n’est pas toujours nécessaire et dépendra de la manière dont la demande est déposée, des données (sensibles) à remettre, etc.

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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



Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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)

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : quelles données ?

Y compris

- les faits et les jugements de valeur
- 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
- les données figurant dans les e-mails de tout collaborateur ou mandataire de l’entreprise qui contiennent des données personnelles

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : quelles données ?

Mais pas

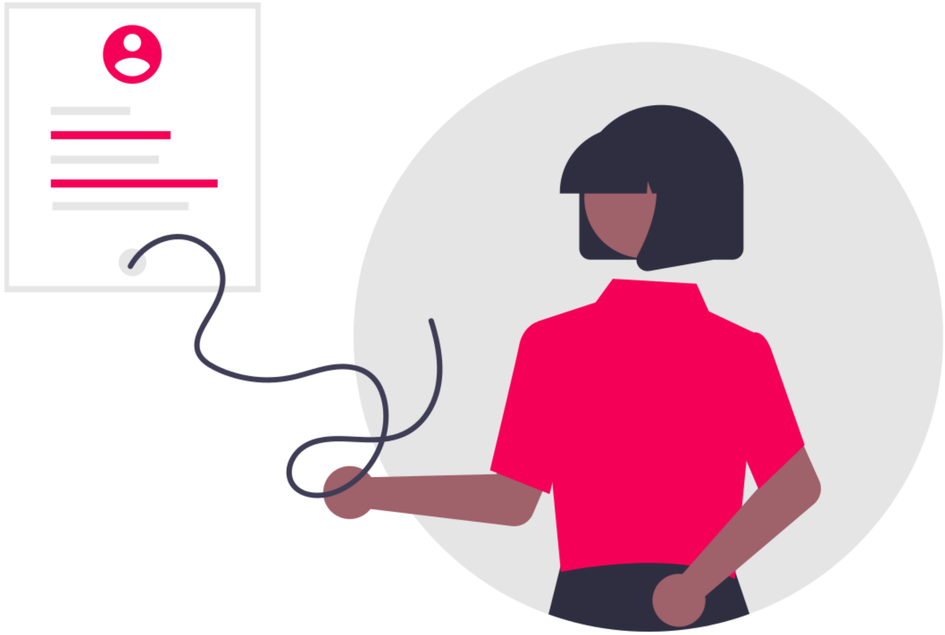
- des données qui n’existaient pas et qui devraient être générées spécialement pour répondre à la demande
- les données qui ont été détruites après la réception de la demande, mais avant la réponse du responsable du traitement, en raison de l’expiration d’un délai de conservation (controversé ?)
- les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

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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)



Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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.

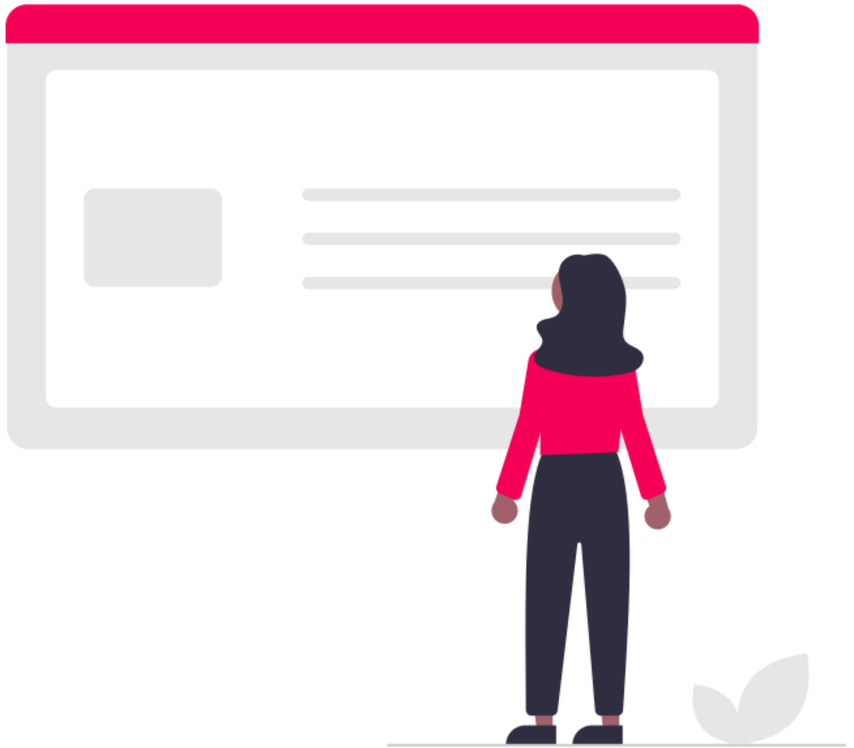
Les notes manuscrites illisibles doivent être déchiffrées avant d’être transmises. Il n’y a en principe pas besoin de traduire les données.

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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.



Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : une 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.)

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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).

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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

Comment préparer et gérer les demandes des personnes ?

Demande d’accès aux données : 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

Demande d’effacement des données

Comment préparer et gérer les demandes des personnes ?

Demande d’effacement : généralités

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 supprimer tout ou partie de mes données »), on ne peut pas se montrer formaliste.

La demande doit se faire par écrit ou oralement.

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) à supprimer, etc.

Comment préparer et gérer les demandes des personnes ?

Demande d'effacement : généralités

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 :

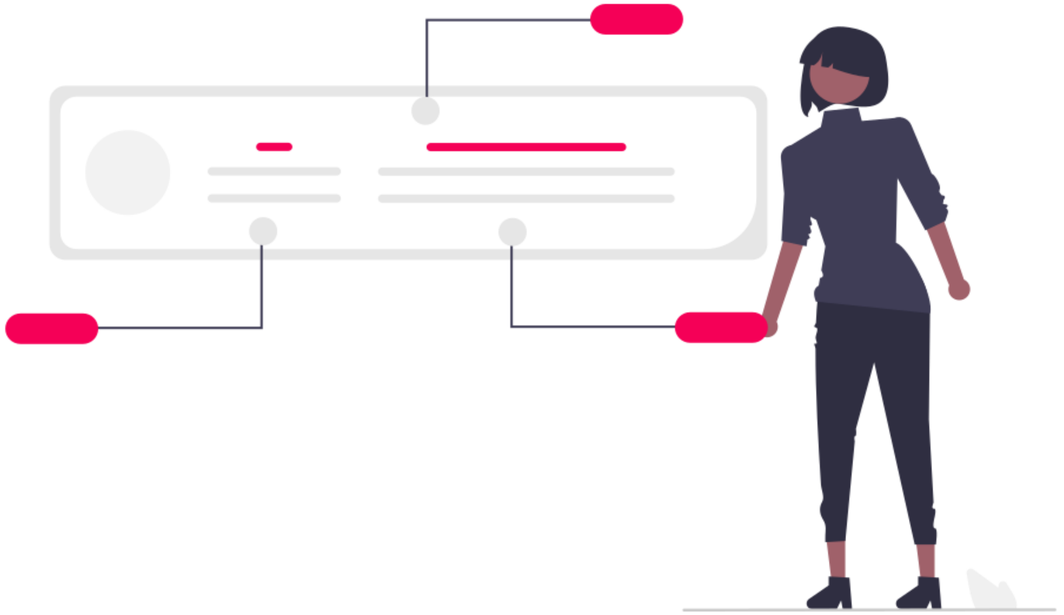
- (Données plus nécessaires aux finalités)
- Retrait du consentement
- Opposition au traitement fondé sur l'intérêt légitime
- Opposition au traitement à des fins marketing
- (Traitement illicite)
- (Obligation légale)

Comment préparer et gérer les demandes des personnes ?

Demande d’effacement : quelle données ?

Uniquement

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

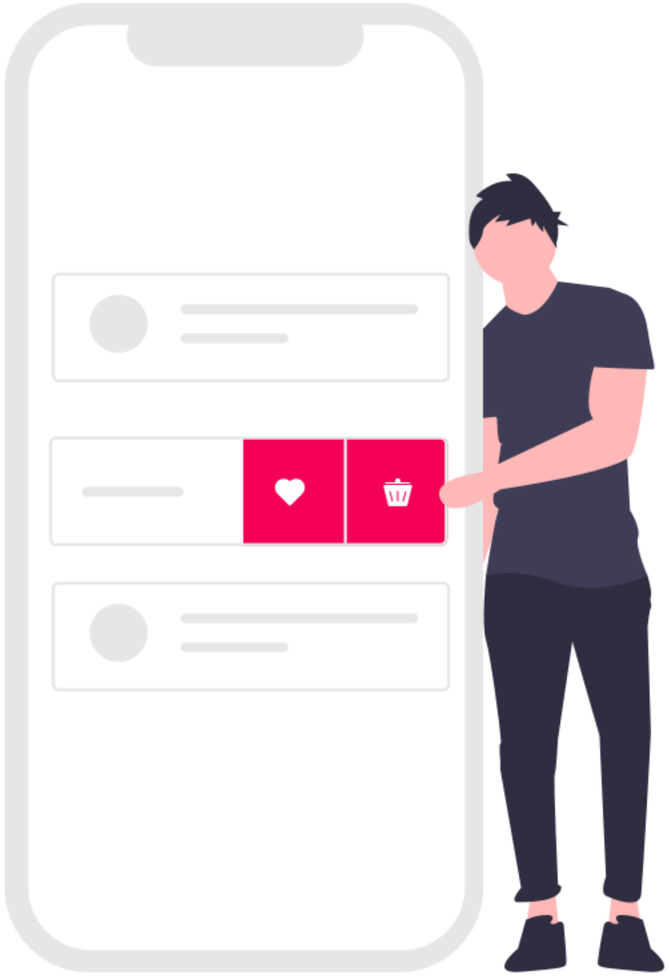


Comment préparer et gérer les demandes des personnes ?

Demande d’effacement : quelles données ?

Y compris

- les données chez les sous-traitants
- les données dans les backups, les archives, le cloud
- les données au format papier ou sur d’autres supports
- les données (non-)structurées



Comment préparer et gérer les demandes des personnes ?

Demande d’effacement : étapes

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

Comment préparer et gérer les demandes des personnes ?

Demande d’effacement : des limites ?

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

Quid des données librement accessibles ?

Comment préparer et gérer les demandes des personnes ?

Demande d’effacement : quelques conseils

1. collecter le moins de données possible de manière générale
2. ne pas paniquer lorsqu’on reçoit une demande de ce type (facile à dire 🙄)
3. ne pas oublier les données traitées par les sous-traitants
4. ne pas oublier les données publiées sur un site web (public ou non)
5. ne pas oublier les données dans les archives et sauvegardes
6. réfléchir avant d’appuyer sur *delete*

Opposition au traitement

Comment préparer et gérer les demandes des personnes ?

Opposition au traitement : généralités

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

La personne doit exprimer l'opposition par un acte qui ne laisse pas de doute. Une opposition tacite n'est pas admissible. On ne doit pas se montrer trop formaliste non plus…

La demande doit se faire par écrit, oralement ou tout autre moyen approprié.

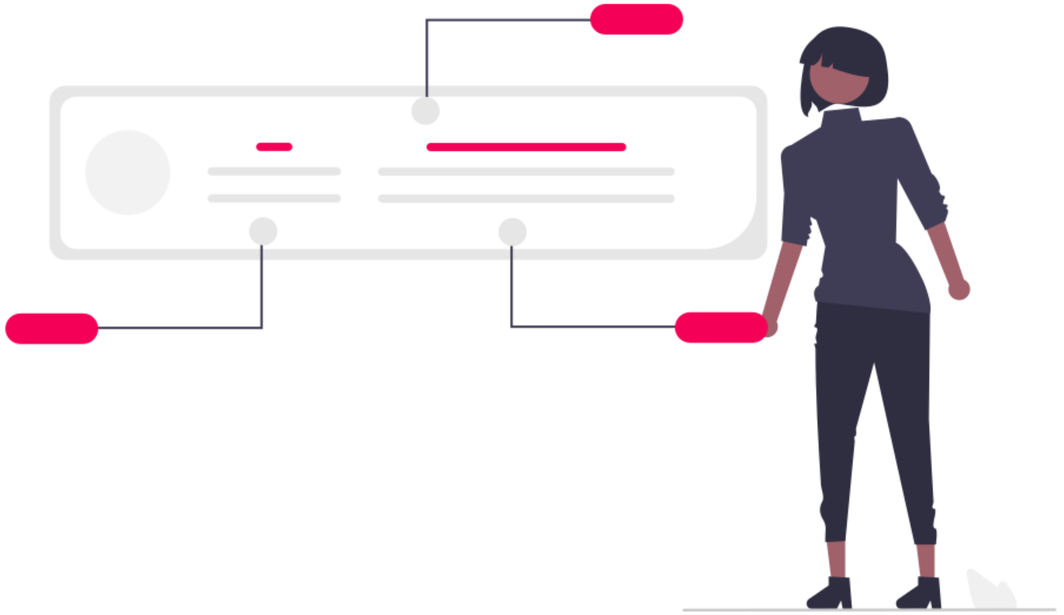
La vérification de l'identité au moyen d'une ID ou d'autres données n'est pas toujours nécessaire et dépendra des circonstances.

Comment préparer et gérer les demandes des personnes ?

Opposition au traitement : quelle données ?

Uniquement

- les données auxquelles la LPD s’applique (art. 2 LPD)
- les traitements visés par la demande d’opposition (spécifiquement ou généralement)



Comment préparer et gérer les demandes des personnes ?

Opposition au traitement : que faire ?

Selon l'art. 30 LPD, la personne concernée a en tout temps et dans n'importe quelle situation le droit (d'essayer) de s'opposer à un traitement spécifique, à plusieurs traitements ou à tous les traitements mis en œuvre par un responsable du traitement, et ce, sans avoir à se justifier ou à remplir d'autres conditions. Une opposition à un traitement implique que celui-ci constitue une atteinte à la personnalité de la personne concernée, l'atteinte étant présumée illicite. Il revient au responsable du traitement de démontrer qu'elle est licite en invoquant un motif justificatif.

En pratique, il s'agit essentiellement de justifier la base juridique utilisée, ainsi que l'éventuel résultat de la balance des intérêts et celui de l'analyse de risques.

Comment préparer et gérer les demandes des personnes ?

Opposition au traitement : quid du marketing ?

Lorsque le traitement de données aux fins de marketing direct se fonde sur le consentement de la personne concernée, celle-ci peut le retirer à tout moment et sans justification. Il en va de même lorsque le responsable du traitement traite les données dans le même but grâce à son intérêt légitime (art. 3 al. 1 let. o LCD).

Le responsable du traitement ne **peut pas refuser** le retrait du consentement ou l'opposition au traitement à des fins marketing.

Comment préparer et gérer les demandes des personnes ?

Opposition au traitement : quid du marketing ?

Conséquences

- l'envoi de publicités doit cesser immédiatement
- les données utilisées pour le marketing ne peuvent plus l'être dans ce but (tout traitement ayant pour but le marketing, y compris le profilage à cette fin, doit cesser)
- les données doivent être retirées des listes d'adresses, des systèmes informatiques et applications servant au marketing
- les données ne peuvent plus être analysées dans un but marketing, même si aucun envoi de publicité n'est réalisé
- si les données ne servent pas un autre but, leur archivage et leur destruction sont soumis aux conditions usuelles

Comment préparer et gérer les demandes des personnes ?

Opposition au traitement : quelques conseils

1. plus de transparence = moins d'opposition ?
2. sensibiliser et former les collaborateurs à reconnaître ce genre de demandes et à les transmettre aux personnes compétentes
3. préparer des modèles de correspondances
4. anticiper les demandes d'oppositions en identifiant à l'avance des motifs de refus, en particulier lorsque le traitement repose sur l'intérêt légitime

Merci

de votre
attention
patience
endurance