



Niveau 1

Principales notions et principes fondamentaux du RGPD

Mots clés : bases légales - consentement - données personnelles - DPO - finalité - droit d'accès - le droit d'effacement - le droit d'opposition – opt-out - responsable de traitement - RGPD - sous-traitant- traitement de données

Les acteurs du RGPD

La Commission nationale pour la protection des données (CNPD)

Au Luxembourg, la CNPD est chargée de vérifier la légalité des fichiers et de toutes collectes, utilisations et transmissions de données concernant des individus identifiables.

Elle doit assurer dans ce contexte le respect des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée.

Personnes concernées :

- Toute personne physique qui fait l'objet d'un traitement de données à caractère personnel.
- Responsable du traitement
- Tout organisme qui détermine les finalités et les moyens du traitement de données à caractère personnel.
- Il peut s'agir d'une administration, d'une entreprise, d'une association, d'un professionnel ou d'un indépendant.

Sous-traitant

Tout organisme qui traite des données à caractère personnel pour le compte et sur instruction du responsable du traitement.

Délégué à la protection des données

Voir fiche pratique n° 2



Dominique Schummer, Directeur de LuxXport entreprise conforme au RGPD

Maîtrisez les « Basics »

1. Le RGPD, Règlement général sur la protection des données

Date d'entrée en application

25 mai 2018

Objectifs (non exhaustifs) :

- Donner aux individus le contrôle de leurs données à caractère personnel ;
- Demander aux entreprises qui gèrent des données de :
 - » Justifier la collecte, le traitement et la conservation des données personnelles;
 - » Assurer leur intégrité, disponibilité, sécurité et leur confidentialité;
 - » Informer les personnes concernées sur leurs droits (modification, suppression, portabilité des données...);
 - » Nommer un délégué à la protection des données dans certains cas;

Suis-je concerné ?

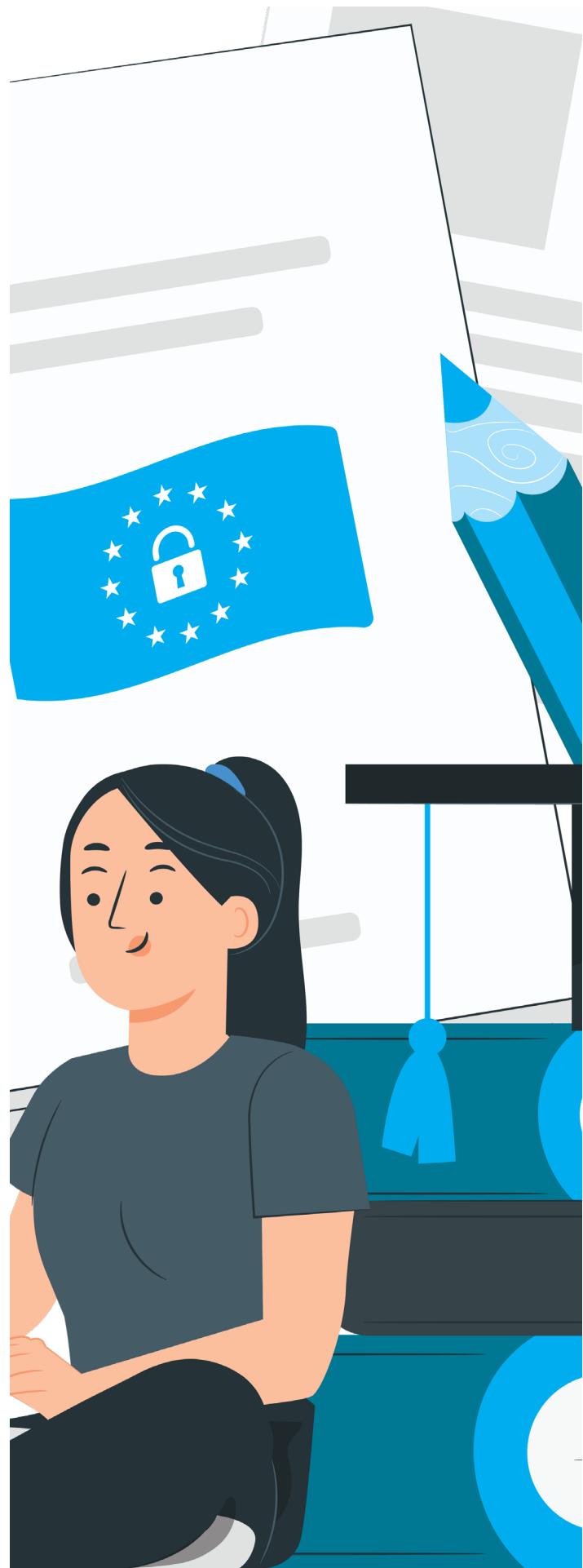
Dès que votre organisme collecte et traite des données à caractère personnel et est établi sur le territoire de l'Union européenne, votre organisme est soumis au RGPD, indépendamment de sa taille, de sa forme juridique, de ses activités ou de son objet social.

Le RGPD s'applique :

- Aux organismes établis sur le territoire de l'Union européenne, que le traitement ait lieu ou non dans l'UE ;
- aux organismes situés hors UE, dont l'activité cible des personnes qui se trouvent sur le territoire de l'UE.

Pour en savoir plus :

[Art. 2 et Art. 3 du RGPD](#)



2. Les données à caractère personnel

Par « données à caractère personnel », on entend toute information concernant une personne physique identifiée ou identifiable.

Une « personne physique identifiable » est définie comme 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, une opinion politique ou un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychologique, économique, culturelle ou sociale.

Pour en savoir plus :

[Art. 4.1 du RGPD](#)

3. Le traitement de données

« Est un traitement, toute opération ou 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 ».

Quelques exemples de traitements:

- Les traitements RH
- Les traitements des salaires
- La prospection commerciale
- Les traitements des clients
- Les traitements Fournisseurs et Prestataires et SAV



4. Le délégué à la protection des données

Le délégué à la protection des données (DPD ou en anglais DPO pour “Data Protection Officer”) a comme missions principales :

- D'informer et conseiller l'organisme concernant la mise en œuvre du RGPD;
- De contrôler la conformité au RGPD;
- D'être un point de contact entre l'organisme, la CNPD et les personnes concernées.

Pour en savoir plus :

[Article 39 du RGPD et page dédiée sur la notion de DPO du site de la CNPD](#)

Avez-vous besoin d'un DPO ?

La désignation d'un DPO est obligatoire si:

- Vous êtes un organisme public;
- Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations

pénales et infractions.

- Dans tous les autres cas, la désignation est facultative.

Dans quel cas dois-je désigner un DPO ?

Quelques illustrations :

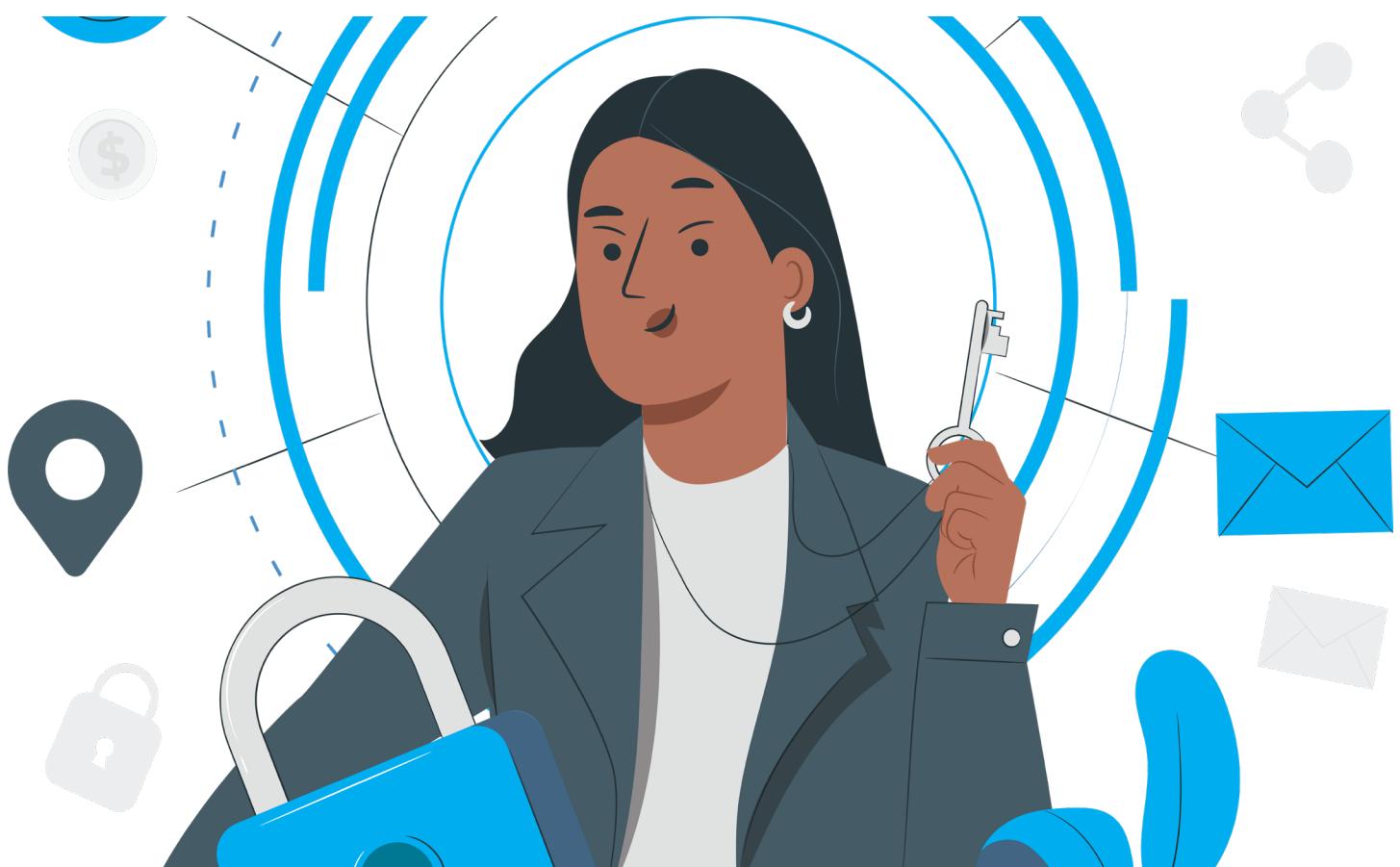
Oui, vous traitez des données à caractère personnel pour diffuser des publicités ciblées sur les moteurs de recherche en fonction du comportement en ligne des personnes concernées.

Oui, vous êtes une banque qui doit régulièrement et systématiquement suivre l'évolution des comptes et des transactions de ses clients notamment dans le cas de ses obligations liées à la prévention de la fraude, du blanchiment d'argent ou du financement du terrorisme.

Non, vous envoyez une publicité à vos clients une fois par an pour promouvoir votre entreprise locale de denrées alimentaires.

Non, vous êtes un médecin généraliste et vous collectez des données sur la santé de vos patients.

Oui, vous traitez des données à caractère personnel portant sur la génétique et la santé pour le compte d'un établissement hospitalier.





Veillez au respect des grands principes

Quand vous traitez des données à caractère personnel, vous devez respecter les principes suivants:

1. Collectez les données personnelles de façon licite, loyale et transparente

La collecte, l'enregistrement, l'utilisation et la transmission de données personnelles doivent se faire en conformité au RGPD, de bonne foi et non pas à l'insu de la personne concernée.

2. Ne collectez et traitez pas des données personnelles sans finalité bien déterminée

Les données personnelles doivent être collectées pour des finalités (objectifs) déterminées, explicites et légitimes et ne peuvent pas être traitées d'une manière incompatible avec ces finalités (p.ex. une utilisation ultérieure pour une autre finalité).

3. Appliquez le principe de minimisation des données

Il faut traiter uniquement les données qui sont nécessaires à la réalisation des finalités définies.

4. Veillez à ce que les données soient exactes et tenues à jour

Vous devez prendre toutes les mesures raisonnables afin de garantir que les données personnelles inexactes soient rectifiées ou supprimées sans tarder.

5. Déterminez une durée de conservation proportionnée

Les données ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des

finalités pour lesquelles elles sont collectées et traitées.

Au-delà, les données doivent être supprimées ou anonymisées.

6. Assurez l'intégrité et la confidentialité des données

Il faut garantir une sécurité suffisante des données à l'aide de mesures techniques et organisationnelles appropriées, notamment contre un traitement non autorisé ou illégal et contre la perte, destruction ou altération accidentelle des données.

7. Démontrez votre conformité (« accountability »)

Vous devez prendre les mesures appropriées pour garantir et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du RGPD.

Qu'est-ce que le conflit d'intérêt ?

Le DPO peut exercer d'autres missions et tâches, à condition qu'elles n'entraînent pas de conflit d'intérêts. Le DPO ne peut pas exercer au sein de l'organisme une fonction qui l'amènerait à déterminer les moyens (comment ?) et les finalités (pourquoi ?) du traitement de données. Cet aspect doit être étudié au cas par cas.

Identifiez la condition de licéité sur laquelle se fonde votre traitement

Pour être licite, un traitement de données doit se fonder sur une des six conditions suivantes:

1. Le consentement de la personne concernée (distinct pour chaque finalité);
2. Un contrat;
3. Une obligation légale (claire et précise);
4. L'intérêt vital de la personne concernée ou d'une autre personne;
5. Une mission d'intérêt public;
6. L'intérêt légitime du responsable de traitement (p.ex. à des fins de marketing, anti-fraude, traitement des données clients ou salariés, sécurité des traitements, etc.).

Le consentement doit être « libre, spécifique, éclairé et univoque », c'est-à-dire que la personne concernée doit avoir un véritable choix.

Si vous recueillez des données liées à des enfants via votre site web commercial (p.ex. jeux en ligne, réseaux sociaux), il est nécessaire d'obtenir l'accord des parents.

L'information à l'égard des utilisateurs doit être facile à comprendre et formulée en termes simples et clairs.

Pour en savoir plus :

[Articles 5 à 9 du RGPD et voir la fiche pratique n° 3 sur les critères du consentement.](#)

Identifiez les traitements nécessitant une vigilance particulière

Vous traitez certains types de données “sensibles”

- Des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale;
- Des données concernant la santé ou l'orientation sexuelle;
- Des données génétiques ou biométriques;
- Des données d'infraction ou de condamnation pénale;
- Des données concernant des mineurs.

Votre traitement a pour objet ou pour effet

- La surveillance systématique à grande échelle, d'une zone accessible au public;
- L'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

Si vos traitements répondent à l'une des caractéristiques énumérées ci-dessus, des mesures ou des règles particulières peuvent s'appliquer (exemples: analyse d'impact relative à la protection des données, information renforcée, recueil du consentement, clauses contractuelles, etc.).



Respectez les droits individuels

L'objectif majeur du RGPD est de renforcer le contrôle des individus sur leurs données. Pour cela, le règlement prévoit différents droits :

1. Le droit à l'information

Vous devez informer les personnes concernées que leurs données personnelles sont traitées, par qui et pourquoi. Cette information doit se présenter dans un langage simple et clair au moment même de la collecte des données, ou si les données n'ont pas été collectées auprès de la personne elle-même, de manière générale dans un délai raisonnable ne dépassant pas un mois.

2. Le droit d'accès

Si une personne vous demande si vous détenez des informations sur elle, vous devez confirmer que des données personnelles la concernant sont ou ne sont pas traitées, et, le cas échéant, lui communiquer une copie de l'intégralité des données que vous possédez à son sujet.

3. Le droit de rectification

Vous avez l'obligation de veiller à ce que les données que vous collectez soient exactes et, si nécessaire, tenues à jour. À la demande d'une personne concernée, vous devez rectifier les informations inexactes.

4. Le droit à l'oubli

Lorsqu'une personne ne souhaite plus que les données qui la concernent soient traitées, vous avez l'obligation de supprimer ces données à moins qu'un motif légitime ne justifie leur conservation.

Un citoyen peut ainsi, par exemple, exiger le retrait immédiat de données à caractère personnel collectées ou publiées sur un réseau social alors qu'il n'était encore qu'un enfant et n'était pas pleinement conscient des risques inhérents au traitement.

5. Le droit à la portabilité

Lorsqu'une personne concernée souhaite récupérer les données qu'elle vous a com-

muniées, vous devez être en mesure de les restituer dans un format structuré, couramment utilisé et lisible par machine afin de lui permettre de les transmettre à un autre organisme (réseau social, fournisseur d'accès à Internet, site de streaming, etc.).

6. Le droit d'opposition

Lorsqu'une personne concernée exerce le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel nécessaire à la poursuite de vos intérêts légitimes ou à l'exécution d'une mission d'intérêt public, vous devez arrêter le traitement, sauf si vous pouvez démontrer l'existence de motifs légitimes et impérieux pour continuer le traitement. Vous devez aussi respecter le droit de la personne concernée de s'opposer, sans qu'elle doive fournir de justification, à l'utilisation de ses données à des fins de prospection commerciale ou de démarchage à orientation idéologique (partis politiques, syndicats, groupements religieux, etc.).

7. Le droit à la limitation

En qualité de responsable de traitement, vous devez suspendre le traitement de données personnelles, lorsqu'une personne concernée revendique la limitation du traitement de ses données, soit que:

- Elle conteste l'exactitude d'une donnée, le temps que vous puissiez vérifier celle-ci;
- Le traitement est illicite et qu'elle s'oppose néanmoins à leur effacement, préférant une telle limitation;
- N'étant plus nécessaire, la personne concernée en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice.

La limitation peut être effectuée selon diverses modalités (déplacement temporaire vers un autre fichier, verrouillage des données, retrait temporaire d'un site Internet, etc.).



Pour en savoir plus :

Articles 13 à 22 du RGPD et la page dédiée du site internet de la CNPD

Point plus approfondi: **Le traitement du droit d'accès**

1. Contenu de la réponse à une demande de droit d'accès

Lorsqu'une personne exerce son droit d'accès, le responsable de traitement doit lui fournir une copie des données la concernant ainsi que les informations suivantes :

- Les finalités du traitement;
- Les catégories de données à caractère personnel concernées;
- Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales;
- Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
- L'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement;
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle;

- Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source;
- L'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4 du RGPD, et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

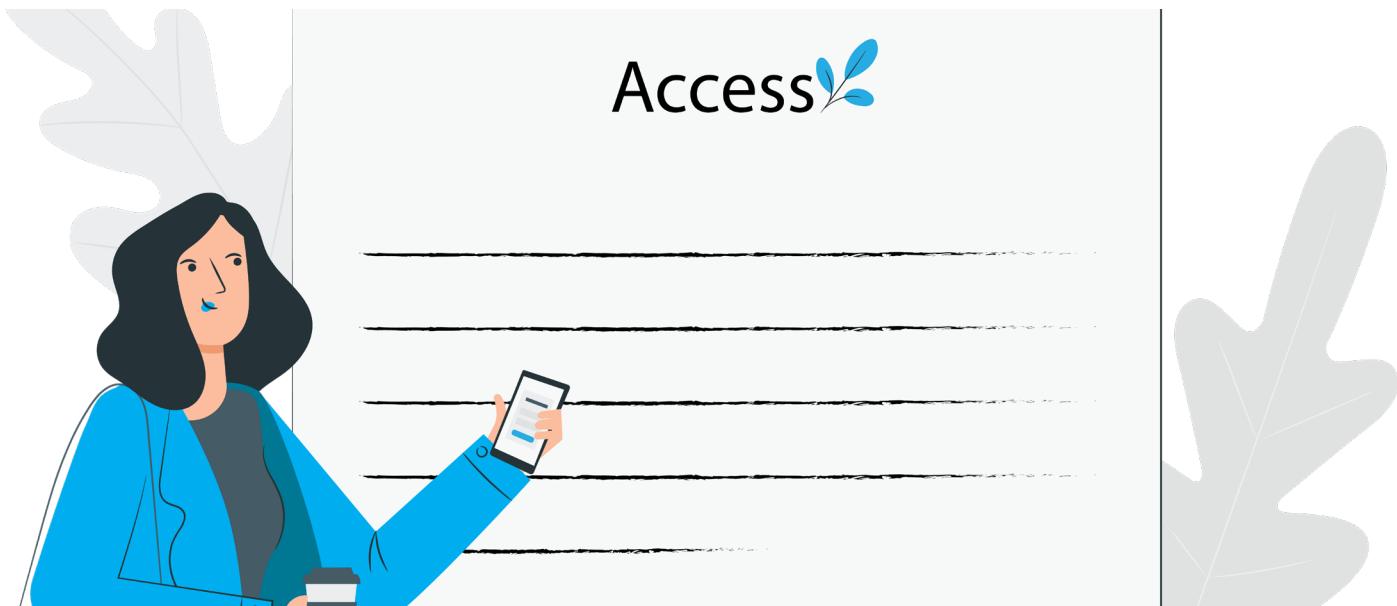
Enfin, lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée doit également être informée des garanties appropriées, en vertu de l'article 46 du RGPD, en ce qui concerne ce transfert.

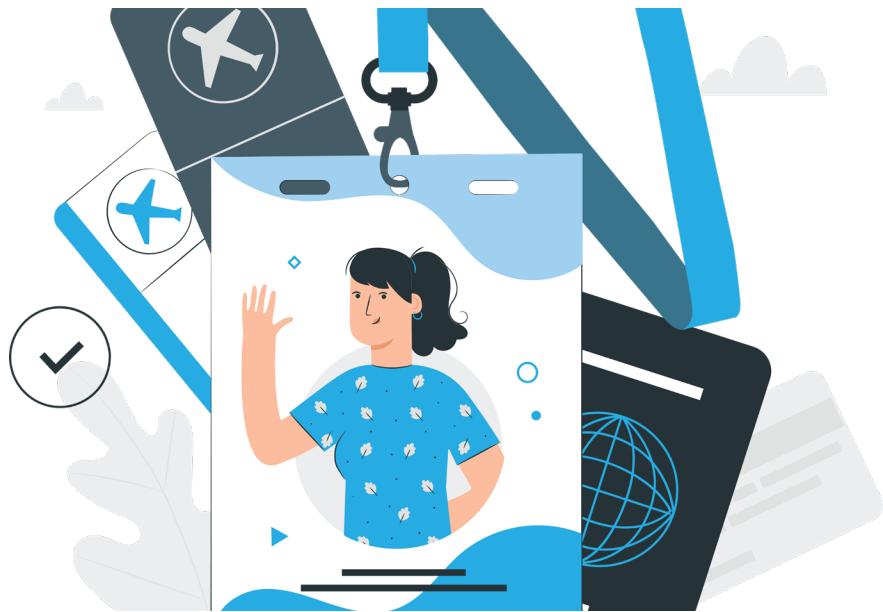
2. Délai de réponse

Une réponse à une demande d'accès doit être communiquée dans les meilleurs délais et en tout état de cause dans un délai d'un mois maximum à compter de la réception de la demande.

Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Dans ce cas, le responsable du traitement doit informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

Ce délai est identique pour l'ensemble des droits individuels.





3. La vérification de l'identité, en cas de doute

Lorsque vous êtes confrontés à la demande d'une personne souhaitant exercer ses droits, la vérification de son identité est essentielle.

Le niveau de vérification requis peut varier en fonction de la nature de la demande, de l'importance des informations communiquées et du contexte spécifique de la demande.

Par principe, il faut éviter de demander une copie de la carte d'identité de la personne car cette vérification d'identité peut être effectuée « par tout moyen ».

Par exemple, la personne concernée peut vous fournir des informations complémentaires telles qu'un numéro de client ou d'adhérent, afin de confirmer son identité. La personne peut également justifier de son identité en exerçant ses droits depuis un espace où elle s'est préalablement authentifiée.

Toutefois, en cas de « doute raisonnable » concernant l'identité d'une personne, vous pouvez lui demander de fournir d'autres documents permettant de confirmer son identité dont une copie de la carte d'identité.

4. Un droit non-absolu, en principe gratuit

L'exercice du droit d'accès est en principe gratuit.

L'organisme doit faciliter l'exercice des droits des individus concernés par le traitement des données. Il ne peut pas refuser de donner suite à une demande sans le justifier

auprès de la personne.

L'organisme peut ne pas donner suite à une demande si :

- Sa mise en œuvre porte atteinte aux droits ou libertés d'autrui (notamment en ce qui concerne le secret des affaires, la propriété intellectuelle et les droits d'auteur protégeant un logiciel);
- Les demandes d'une personne sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif : dans ce cas, le responsable pourra alternativement choisir de répondre en exigeant le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées;
- Si l'organisme choisit de ne pas donner suite à la demande, il doit alors informer la personne concernée dans un délai d'un mois, en motivant son choix et en l'informant de la possibilité d'introduire une réclamation auprès de la CNPD et/ou de former un recours juridictionnel.

Clause de non responsabilité:

Le présent document est une fiche récapitulative des explications fournies dans le cadre de l'outil DAAZ pour illustrer les réponses. Le contenu est fourni à des fins d'information seulement et ne devrait pas être interprété comme constituant un exposé complet et exhaustif des sujets évoqués. Le contenu n'engage nullement la responsabilité de la CNPD. En cas de contradiction entre le présent document et les lignes directrices publiées sur le site de la CNPD, seules les lignes directrices prévalent.