RGPD *notions et procédures CNIL*

MODULE 1 : LE RGPD ET SES NOTIONS CLÉS

1. Définition du traitement de données à caractère personnel
2. A qui s'applique le RGPD ?
3. S'évaluer

MODULE 2 : LES PRINCIPES DE LA PROTECTION DES DONNÉES

1. Les 8 règles d'or
2. Finalité du traitement
3. Licéité du traitement
4. Minimisation des données
5. Protection particulière de certaines données
6. Conservation limitée des données
7. Obligation de sécurité
8. Transparence à l'égard des personnes concernées
9. Droits des personnes sur leurs données
10. Encadrement des transferts de données hors de l'UE

MODULE 3 : LES RESPONSABILITES DES ACTEURS

1. Nouvelle logique de responsabilisation : l'*accountability*
2. Partage des responsabilités
3. Responsabilité spécifique des sous-traitants
4. Les sanctions et voies de recours

MODULE 4 : LE DPO ET LES OUTILS DE LA CONFORMITÉ

1. Le délégué à la protection des données
2. Le registre des activités
3. L'analyse d'impact relative à la protection des données (AIPD)
4. La notification des violations de données
5. Code de conduite et certification

Table des matières

LES DONNÉES
À CARACTÈRE PERSONNEL

1 Des données **directement** identifiantes

Les données personnelles sont directement identifiantes **si elles sont associées à un élément indiquant clairement l'identité de la personne**. Il peut s'agir d'un nom, d'un prénom, d'un email nominatif, d'une photo, etc.

Ce type de données figure, par exemple, sur :

- les fiches de paie
- les relevés de compte bancaire
- les devis
- les factures
- les fichiers clients
- etc.

LES DONNÉES
À CARACTÈRE PERSONNEL

2 Des données **indirectement** identifiantes

Dans certains fichiers, les noms et prénoms des personnes sont remplacés par un identifiant : numéro client, numéro de téléphone, etc.

Prises isolément, ces données ne permettent pas de savoir immédiatement à qui correspondent les informations.

En revanche, **lorsqu'elles sont associées à une autre base de données** détenue en interne ou par tout autre tiers, comme le fichier client de l'entreprise ou l'annuaire téléphonique, **il est possible de retrouver l'identité de la personne**.

LES DONNÉES
À CARACTÈRE PERSONNEL

3 Les combinaisons d'informations

Certaines informations ne permettent pas à elles seules ni directement, ni indirectement (en étant associées à une autre base) d'identifier une personne.
En revanche, **la combinaison de plusieurs de ces informations peut parfois permettre d'identifier de manière unique une seule personne**.

LES DONNÉES
À CARACTÈRE PERSONNEL

3 Les combinaisons d'informations

Une enquête ne sera pas rendue anonyme seulement parce qu'elle ne demande pas le nom et le prénom de la personne interrogée. C'est le cas des enquêtes qui concernent peu de personnes, surtout si ces personnes sont sélectionnées selon une caractéristique prédéterminée.
Une seule réponse peut permettre de retrouver l'identité d'une des personnes interrogées.

Même une enquête qui porte sur un grand nombre de personnes interrogées au hasard, dans la rue par exemple, peut contenir des réponses qui combinées les unes aux autres permettent de retrouver l'identité des sondés. C'est le cas lorsque les questions sont très nombreuses ou précises (par ex., "je suis née à Paris, dans le 14ème arrondissement, je travaille à la CNIL et je suis fan d'animaux, de jazz et de jeux vidéo").

LES DONNÉES
À CARACTÈRE PERSONNEL

3 Les combinaisons d'informations

Par exemple en matière d'open data (ouverture et mise à disposition des données produites et collectées par les services publics) donnant la possibilité d'accéder à certaines informations personnelles.

Supposons que la France soit quadrillée, **chaque carreau étant associé à des données socio-démographiques, dont l'imposition moyenne des habitants, la population active, le niveau de diplôme, etc.**

Dans les zones peu peuplées, **les carreaux, selon leur taille, peuvent ne comprendre qu'un nombre limité de foyers, voire un seul, dont il peut être aisé de retrouver l'adresse, l'identité, la physionomie générale**, notamment par un croisement de ces données avec des informations fournies par un moteur de recherche ou un service de cartographie en ligne.

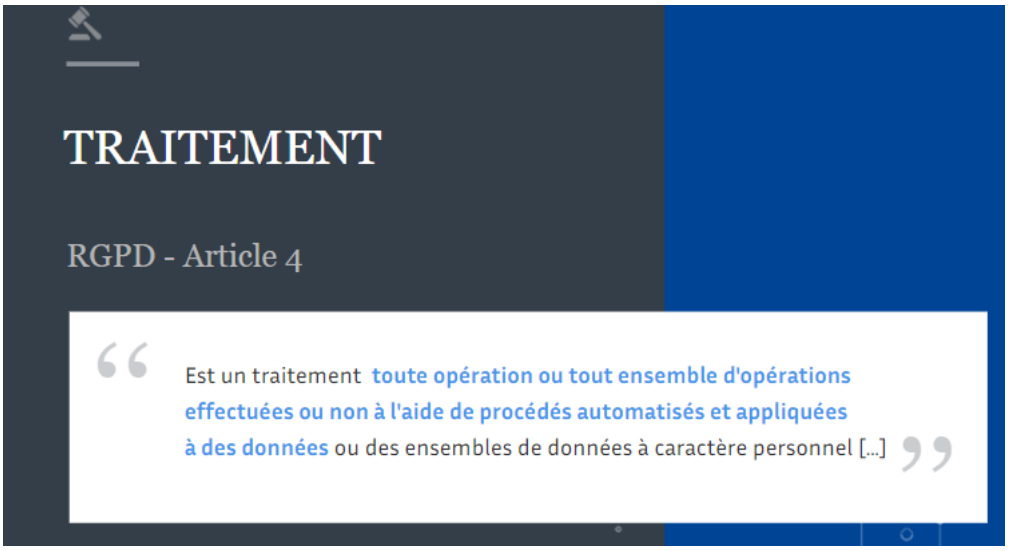
Ainsi, selon la granularité du carreau, **la combinaison d'informations peut se révéler identifiante pour les personnes.**

LES DONNÉES
À CARACTÈRE PERSONNEL

3 Les combinaisons d'informations

L'essor du numérique apporte des possibilités croissantes d'identification ou de ré-identification des personnes sur la base d'informations dépersonnalisées.

De nombreux travaux de recherche portant sur cette question démontrent en effet que **la ré-identification devient de plus en plus facile**, du fait de la multiplicité des données disponibles, de leur degré de précision et des techniques informatiques de recoupement de données.



TRAITEMENT

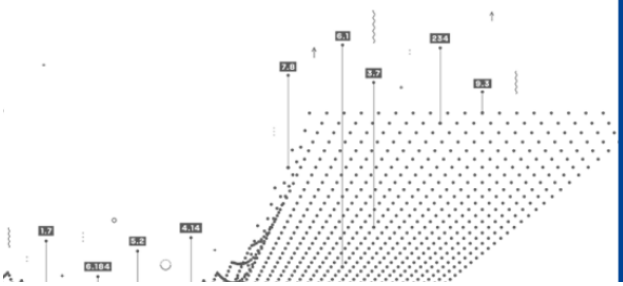
Sont ainsi notamment concernées les opérations suivantes :

- la collecte
- l'enregistrement
- la structuration
- la conservation (l'hébergement)
- la transmission
- la modification
- l'extraction
- la communication
- la mise à disposition
- le rapprochement
- etc.

Le traitement de données personnelles est très vite arrivé !

TRAITEMENT

Tout organisme est amené à traiter des données personnelles pour pouvoir correctement fonctionner et/ou assurer la gestion de ses activités.



Traitements liés au fonctionnement interne

Les organismes mettent en œuvre de nombreux traitements de données personnelles pour permettre à leur structure de fonctionner dans de bonnes conditions : fichiers de gestion RH, de gestion administrative et comptable, dispositifs de sécurisation des locaux (contrôle d'accès par badge, vidéosurveillance), etc.

Traitements liés aux activités

Le traitement de données personnelles est souvent indispensable à l'accomplissement des missions de l'organisme : gestion des fichiers de prospection commerciale, gestion de la liste des donateurs d'une association, gestion de l'état civil d'une commune, etc.

SYNTHÈSE

Les notions de données personnelles et de traitement étant protéiformes, les règles protectrices du RGPD trouvent très largement à s'appliquer.
Les organismes comptables de leur respect doivent faire preuve d'une grande vigilance.

A QUI S'APPLIQUE LE RGPD ?

INTRODUCTION

Les notions de données personnelles et de traitements sont très larges.

De plus, le RGPD s'articule autour d'une logique de responsabilisation de l'ensemble des acteurs traitant des données sur des personnes situées dans l'Union européenne.

Ainsi, de très nombreux organismes doivent prendre en compte les principes posés par cette réglementation protectrice.

ORGANISMES CONCERNÉS

Le RGPD concerne
tous les organismes publics et privés,
quels que soient leur taille ou leur secteur d'activité. Sont ainsi notamment concernées :

- Les entreprises (TPE, PME, ETI et GE)
- Les administrations
- Les collectivités
- Les associations

ORGANISMES CONCERNÉS

Champ d'application territorial

D'après l'article 3 du RGPD,
la règlementation s'applique aux traitements
de données personnelles effectués par :

Un organisme établi sur le territoire de l'Union européenne (critère de l'établissement), que le traitement ait lieu ou non dans l'UE.

Voir un exemple

Un organisme dont l'activité cible des personnes qui se trouvent sur le territoire de l'UE (critère du ciblage). Les organismes sont concernés lorsque le traitement vise à offrir des biens ou services à de telles personnes ou à suivre leur comportement au sein de l'Union.

Fermer l'exemple

RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT

Un traitement de données peut être mis en œuvre par un organisme soit pour son propre compte, soit pour le compte et sur instruction d'un autre organisme.

Cette question joue un rôle central dans le partage des responsabilités entre les acteurs et impacte significativement leurs obligations respectives.

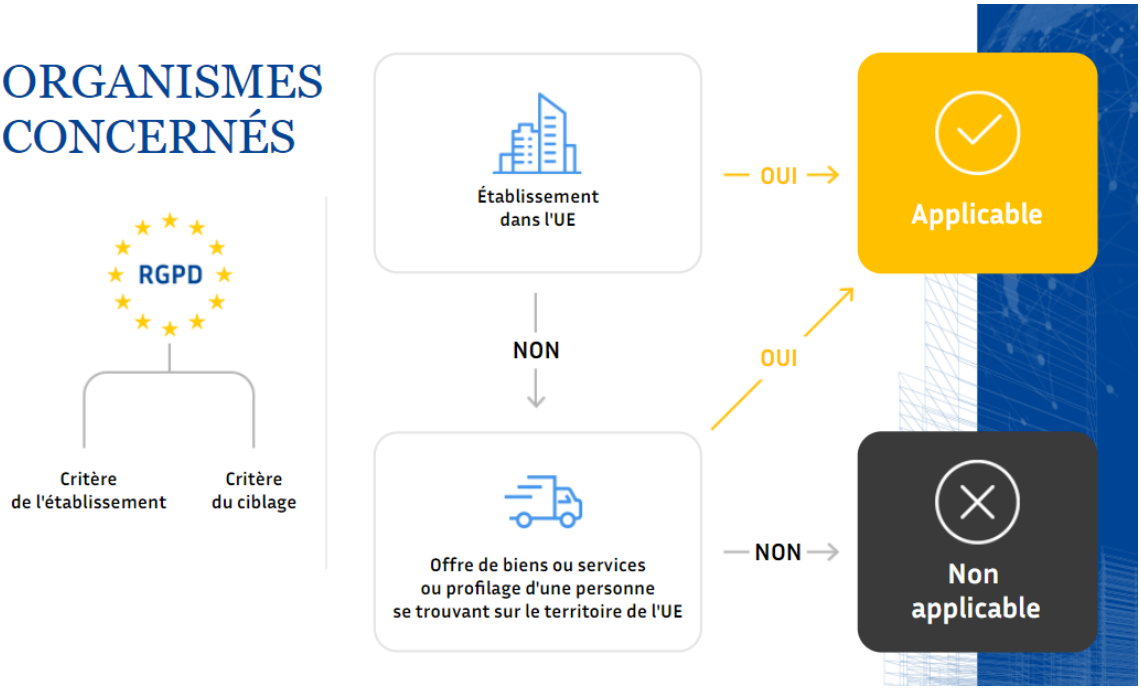
Un organisme peut donc être :

- **Responsable de traitement (RT)** s'il détermine le "pourquoi" et le "comment" du traitement de données, c'est-à-dire sa finalité (objectifs poursuivis) et ses moyens (conditions de mise en œuvre, notamment sur le plan technique, matériel et organisationnel)

OU

- **Sous-traitant (ST)** s'il traite des données personnelles pour le compte et sur instruction d'un autre organisme.

ORGANISMES CONCERNÉS



RESPONSABLE DE TRAITEMENT

De façon générale, le responsable de traitement, qui doit être porté à la connaissance des personnes concernées, est considéré comme étant **l'organisme pour lequel le traitement est mis en œuvre** :
c'est donc sur lui que pèsera la responsabilité du respect des obligations.

Dans certains cas, la loi peut déterminer le responsable du traitement. Par exemple, dans le cadre de la gestion des vaccinations contre la grippe aviaire, la CNAMTS est expressément désignée comme responsable de ce traitement.

En pratique, ce sera au représentant légal de veiller à la bonne prise en compte par l'organisme des principes "Informatique et Libertés" :

- **Pour le secteur privé,** il s'agira ainsi de son dirigeant (président, directeur général, PDG, gérant...)

- **Pour le secteur public,** il s'agira, selon l'organisme, du ministre, du maire, du président de l'EPCI, du conseil départemental...

SOUS-TRAITANT

Un organisme est sous-traitant lorsqu'il **traite des données personnelles pour le compte et sur instruction d'un autre organisme** ayant la qualité de responsable de traitement.

Ces activités de sous-traitant peuvent concerner une tâche bien précise (sous-traitance d'envoi de courriers de prospection commerciale) ou être plus générales et étendues (gestion de l'ensemble d'un service pour le compte d'un autre organisme telle que la gestion de la paie des salariés ou des agents par exemple).

SOUS-TRAITANT

Une très grande variété de prestataires peut donc avoir la qualité de sous-traitant au sens « protection des données » tels que :

- les prestataires de services informatiques (hébergement, maintenance,...), les intégrateurs de logiciels, les entreprises de services numérique (ESN) et celles de sécurité informatique
- les agences de marketing ou de communication qui traitent des données personnelles pour le compte de clients
- plus généralement, tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme.

SOUS-TRAITANT

Ne sont pas considérés comme sous-traitant, dans la mesure où ils n'ont pas accès et ne traitent pas de données personnelles, les éditeurs de logiciels ou les fabricants de matériels (badgeuse, matériel biométrique, matériel médical) qui ne font que fournir un **outil « vide » de données**.

De nombreux prestataires de service auront une double casquette : "responsable de traitement" pour les opérations effectuées pour leur propre compte (ex. : gestion RH, gestion clients, etc.) et "sous-traitant" pour les opérations effectuées pour le compte de leurs clients (ex. : hébergement de données, envoi de courriels, etc.)

Le sous-traitant est soumis à un certain nombre d'obligations précisées dans le **contrat de sous-traitance** qui doit être conclu avec le responsable de traitement.

L'EXCEPTION DOMESTIQUE

En revanche, le responsable de traitement ou le sous-traitant qui fournit la solution ou le dispositif utilisé dans ce cadre privé, est soumis au RGPD.

Exemple:
le fabricant d'une enceinte connectée utilisée dans un cadre familial doit respecter les obligations imposées par le RGPD : respect du principe du *privacy by design* (protection dès la conception), information des personnes, etc.

SYNTHÈSE

Tout organisme est concerné par le RGPD dès lors qu'il se trouve sur le territoire de l'UE ou qu'il traite des données personnelles d'individus se trouvant sur le territoire de l'UE.

INTRODUCTION

Le RGPD encadre la collecte, l'utilisation et la conservation des données personnelles par 8 règles d'or auxquelles tout organisme privé ou public doit se conformer.

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

1

Un traitement ne peut être mis en oeuvre que s'il est **fondé sur une des 6 conditions de licéité**

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

2

Les données personnelles collectées ne peuvent être **traitées que pour une finalité définie précisement et légitime**

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

Seules les **données strictement nécessaires pour atteindre la finalité** peuvent être collectées et traitées

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

Les données sensibles ne peuvent être **collectées et traitées que dans certaines conditions**

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

Les données doivent être **archivées, supprimées ou anonymisées** dès que la finalité pour laquelle elles ont été collectées est atteinte

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

Au regard des risques, **des mesures** doivent être mises en oeuvre pour **s'assurer de la sécurité des données traitées**

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

Les personnes doivent être **informées de l'utilisation des données les concernant et de la manière d'exercer leurs droits**

Les 8 règles d'or

- Licéité du traitement
- Finalité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

Les personnes bénéficient de **nombreux droits qui leur permettent de garder la maîtrise de leurs données**

Fianlité des traitements :

INTRODUCTION

C'est à partir de la finalité que découlent notamment la durée de conservation, la pertinence des données collectées et la liste des personnes habilitées à y accéder.

LA FINALITÉ

La raison d'être du traitement

C'est l'objectif en vue duquel les données sont collectées, enregistrées, exploitées, transmises, conservées, etc. par l'organisme.

Par exemple, la finalité d'un traitement peut être la gestion des recrutements, la gestion de la clientèle ou des usagers d'un service public, la protection des biens et des personnes, etc.

LA FINALITÉ

Tout traitement de données doit venir satisfaire un objectif précisément déterminé et légitime.

Il n'est pas possible de collecter et de traiter des données personnelles "à toutes fins utiles" ou dans l'éventualité où elles pourraient, un jour, servir à quelque chose.

Tout traitement de données doit être nécessaire à la poursuite d'un objectif déterminé, au préalable, par l'organisme.
En plus d'être légal, cet objectif doit être légitime par rapport à la nature et aux activités de l'organisme.

DÉFINITION

La finalité doit être déterminée et explicite

Le RGPD prévoit que toute finalité soit déterminée, c'est-à-dire qu'un objectif précis à atteindre doit avoir été arrêté avant la mise en œuvre d'un traitement.

Son caractère explicite est vérifié lorsque la finalité est énoncée (en interne et à l'égard des personnes concernées) de manières compréhensible et suffisamment claire.

DÉFINITION

La finalité doit être légitime

La légitimité de la finalité s'apprécie au regard des dispositions de l'article 1er de la loi Informatique et Libertés, de l'article 6 du RGPD mais également de l'ensemble de la législation applicable au traitement.

La légitimité pourra être remise en cause si la finalité est jugée peu justifiée ou trop intrusive pour les personnes concernées.

Le principe de finalité permet de délimiter le champ des usages des données.

L'objectif est d'éviter qu'elles fassent l'objet, par l'organisme qui les a collectées ou un tiers, d'une utilisation qui n'aurait pas été initialement prévue par lui, ni portée à la connaissance de la personne concernée lors du recueil de ses données.

Ce dernier point est particulièrement important car la connaissance de cette seconde utilisation aurait pu conduire la personne concernée à ne pas accepter le recueil de ses données.

Le non-respect de la délimitation des usages initialement définis (et communiqués à la personne concernée) est considéré comme un **détournement de finalité**.

Exemple de détournements de finalité

Fichiers de caisse de sécurité sociale
constitués par l'administration afin de calculer le montant des aides aux personnes.
Détournement de finalité :
transmission des adresses emails à une entreprise qui va les utiliser pour faire de la prospection commerciale.

Dispositif de géolocalisation
installé dans les véhicules du personnel pour assurer le suivi des livraisons.
Détournement de finalité :
l'employeur utilise le dispositif de géolocalisation pour contrôler le temps de travail des salariés.

Exemple de détournements de finalité

Fiches des inscriptions scolaires
établies afin de prévenir les parents/élèves en cas de modification des emplois du temps.
Détournement de finalité :
le maire utilise des données contenues dans les fiches d'inscriptions scolaires pour faire de la communication politique.

Il existe des fichiers dont la finalité est adaptée à la communication politique : les listes électorales, en particulier.

Fichiers du personnel
établis afin d'organiser la paie des salariés.
Détournement de finalité :
le service commercial utilise les adresses emails contenues dans les fichiers du personnel pour leur adresser de la prospection.

Seuls les fichiers clients et prospects peuvent être utilisés à de telles fins, sous réserve de respecter les droits des personnes.

SANCTION PÉNALE

CODE PÉNAL - ARTICLE 226-21

Le détournement de finalité est sanctionné d'une peine pouvant s'élever à 300.000 € d'amende et 5 ans d'emprisonnement.

SANCTION ADMINISTRATIVE

RGPD - ARTICLE 83-5

Le détournement de finalité fait l'objet d'une sanction administrative pouvant s'élever à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

ÉVOLUTION DES USAGES SANS DÉTOURNEMENT DE FINALITÉ :

La finalité compatible

Le principe de finalité n'interdit pas toute évolution dans les usages qui sont faits des données par l'organisme qui les traite ou par un tiers destinataire : un traitement ultérieur des données pour une finalité différente peut en effet être envisagé.

La détermination d'une nouvelle « finalité compatible » avec la finalité initiale est l'un des cas possibles.

Le RGPD prévoit expressément (article 5-1, alinéa b) 3 finalités qui, par principe, pourront être jugées comme compatibles avec la finalité initiale de la collecte de données :

- traitement à des fins archivistiques dans l'intérêt public
- traitement à des fins de recherche scientifique ou historique
- traitement à des fins statistiques.

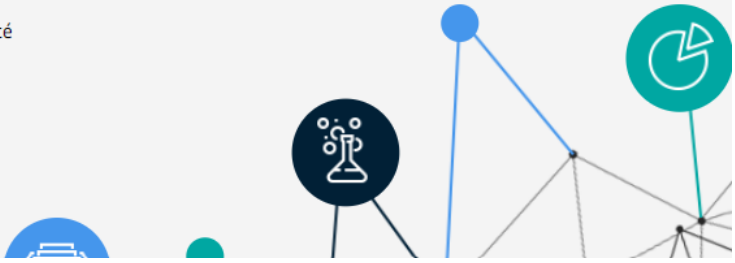
ÉVOLUTION DES USAGES SANS DÉTOURNEMENT DE FINALITÉ :

La finalité compatible

D'autres finalités pourront le cas échéant être considérées comme compatibles par l'organisme au moyen de la méthode du faisceau d'indices prévue par le RGPD (article 6-4) qui s'intéresse à :

- l'existence d'un lien entre la finalité initiale et la finalité ultérieure
- la nature des données
- les conséquences pour les personnes concernées
- l'existence de garanties appropriées (ex: chiffrement).

Attention,
l'évolution de la finalité devra s'effectuer en toute transparence et dans le respect des droits des personnes concernées et tout particulièrement leur droit de s'y opposer.



ÉVOLUTION DES USAGES SANS DÉTOURNEMENT DE FINALITÉ :

Le consentement ou le texte juridique

En dehors de la possibilité de définir une « finalité compatible », il reste possible de définir un nouvel usage (une nouvelle finalité) si l'une de ces deux conditions est réunie :

- le responsable de traitement obtient le consentement des personnes pour définir un nouvel usage des données
- le nouvel usage des données se fonde sur une disposition du droit de l'Union ou du droit de l'État membre.

SYNTHÈSE

La finalité définit le lien entre les données, les traitements et les organismes qui les mettent en œuvre.

Elle délimite le périmètre de leur exploitation.

Le principe de finalité n'interdit pas l'exploitation ultérieure des données à des fins différentes de celles pour lesquelles les données ont été collectées, sous réserve du respect de certaines conditions.

La réutilisation à d'autres fins devra être réalisée dans le respect des différents principes de protection des données personnelles, et en particulier dans le respect des droits des personnes.

Unité 3 : Licéité du traitement

INTRODUCTION

Lorsqu'un organisme souhaite collecter des données à caractère personnel, il doit avant toute chose identifier la licéité (dite aussi « la base légale ») de cette démarche.

LICÉITÉ DU TRAITEMENT

RGPD - Article 6-1

Le traitement n'est licite et ne peut être mis en œuvre que si au moins l'une de ces **6 conditions** suivantes est remplie :

1. La personne concernée a **consenti au traitement** de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.
2. 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.
3. Le traitement **est nécessaire au respect d'une obligation légale** à laquelle le responsable de traitement est soumis.
4. Le traitement **est nécessaire à la sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique.
5. 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 de traitement.
6. Le traitement **est nécessaire aux fins des intérêts légitimes** poursuivis par le responsable de 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.

1 LE CONSENTEMENT

RGPD - Article 4-11

Le RGPD définit le consentement comme « toute manifestation de volonté **libre, spécifique, éclairée et univoque** par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

1 LE CONSENTEMENT

Le consentement n'est pas un concept nouveau, puisqu'il était déjà **inscrit dans la loi Informatique et Libertés**.

Le RGPD complète néanmoins sa définition et précise cette notion sur certains aspects, afin de permettre aux personnes concernées d'exercer un **contrôle réel et effectif sur le traitement de leurs données**.

Il leur permet ainsi de :

- choisir sans contrainte d'accepter ou de refuser un traitement
- pouvoir retirer à tout moment son consentement (ce qui mettra fin au traitement).

1 LE CONSENTEMENT

Attardons-nous plus précisément
sur **les caractéristiques du consentement** :

LIBRE - SPÉCIFIQUE - ÉCLAIRÉ - UNIVOQUE

Le consentement
ne doit être ni contraint ni influencé.

La personne doit se voir offrir un choix réel.
Le caractère libre du consentement doit faire l'objet d'une attention particulière dans le cas de l'exécution d'un contrat, y compris pour la fourniture d'un service.

La personne doit pouvoir refuser de consentir à un traitement qui n'est pas nécessaire à l'exécution du contrat sans subir aucune conséquence négative en cas de refus.

1 LE CONSENTEMENT

Prenez connaissance de l'exemple à droite, puis répondez à la question ci-dessous :

Le consentement concernant l'utilisation des données personnelles demandé dans le cadre de la souscription à un contrat d'abonnement de service est-il libre ?

Oui | Non

Le consentement est considéré comme libre car il n'est pas **lié aux conditions générales de vente**.

La personne peut donc refuser que ses données soient transmises à un partenaire **sans que cela n'impacte la fourniture du service**.

1 LE CONSENTEMENT

LIBRE - **SPÉCIFIQUE** - ÉCLAIRÉ - UNIVOQUE

Un consentement doit correspondre à un seul traitement, pour une finalité déterminée.

Lorsqu'un traitement comporte plusieurs finalités, la personne doit pouvoir consentir indépendamment pour chacune de ces finalités. Elle doit pouvoir choisir librement les finalités pour lesquelles elle donne son accord.

1 LE CONSENTEMENT

Prenez connaissance de la situation ci-contre, puis répondez à la question ci-dessous :

Ce consentement est-il valide ?

Oui | Non

Le consentement aurait été valide si la personne avait pu consentir librement et séparément à chacun de ces deux traitements :

- la conservation de la carte bancaire afin de faciliter les prochains paiements
- la conservation de l'adresse courriel afin de communiquer sur les prochaines promotions.

1 LE CONSENTEMENT

LIBRE - SPÉCIFIQUE - **ÉCLAIRÉ** - UNIVOQUE

Pour qu'un consentement soit valide, certaines informations doivent être distinctement affichées avant que la personne ne donne son accord.

Le responsable de traitement doit mettre en avant certaines informations. Celles-ci ne devront pas être "noyées" dans les conditions générales.
Enfin, la personne concernée doit avoir un moyen de consulter l'intégralité des informations requises si elle le souhaite (au moyen d'un lien permettant d'accéder à une page dédiée par exemple).

1 LE CONSENTEMENT

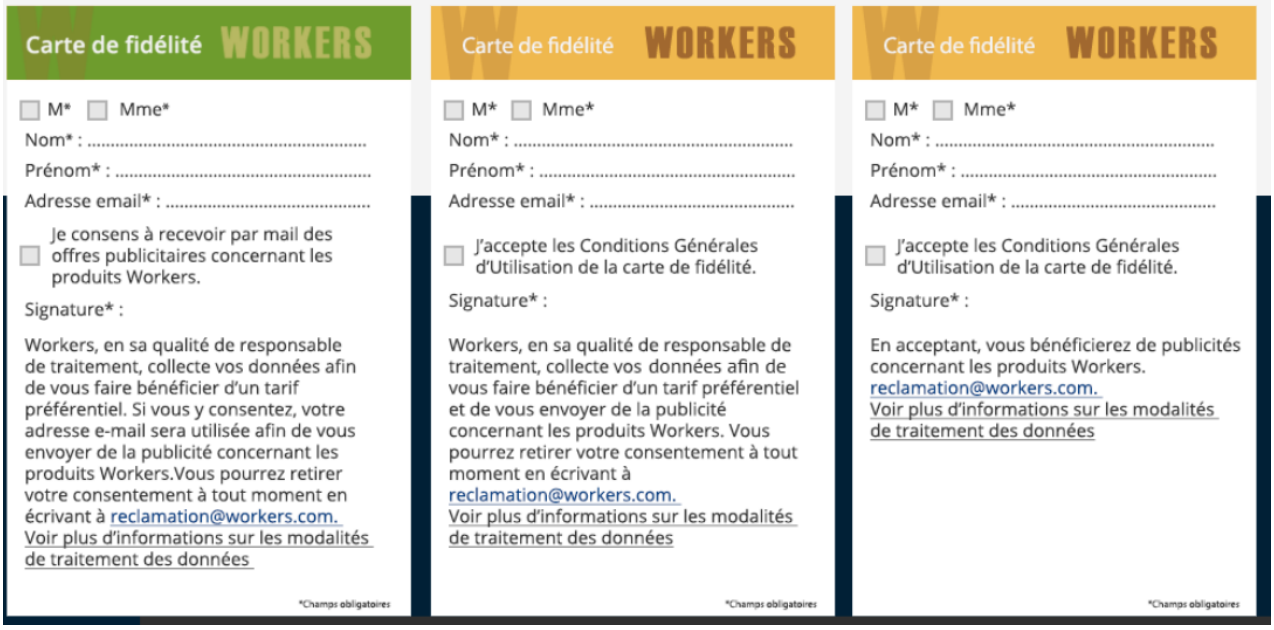
LIBRE - SPÉCIFIQUE - **ÉCLAIRÉ** - UNIVOQUE

Informations que le responsable de traitement doit particulièrement mettre en avant :

- **l'identité** du responsable du traitement
- **les finalités** du traitement
- **les catégories** de données collectées
- l'existence d'un **droit de retrait du consentement**
- selon les cas : le fait que les données seront utilisées **dans le cadre de décisions individuelles automatisées** ou qu'elles feront l'objet d'un **transfert vers un pays hors de l'UE**.

1 LE CONSENTEMENT

Seule la première carte de fidélité permet de recueillir valablement un consentement. Les deux autres cartes ne permettent pas de recueillir un consentement valable en raison, notamment, du caractère lié des finalités (carte n°2) et de l'insuffisance des informations affichées (carte n°3).



1 LE CONSENTEMENT

LIBRE - SPÉCIFIQUE - ÉCLAIRÉ - **UNIVOQUE**

Le consentement doit être donné sans ambiguïté par une déclaration ou un acte positif clair.

Le consentement n'est pas considéré comme univoque si :

- les cases sont pré-cochées ou pré-activées
- il résulte de l'acceptation globale d'un contrat ou de conditions d'utilisation d'un service
- il résulte d'une inaction de la personne concernée.

1 LE CONSENTEMENT

Prenez connaissance de l'exemple à droite, puis répondez à la question ci-dessous :

Cette méthode de recueil du consentement est-elle valide ?

Oui Non

L'absence de réponse à un email ne peut en aucun cas valider le consentement d'une personne :

une action positive est nécessaire !

1 LE CONSENTEMENT DES MINEURS

Le RGPD prévoit des conditions particulières de consentement pour certaines situations et notamment pour les mineurs **dans le cadre des services de la société de l'information** (réseaux sociaux, plateformes de vidéos à la demande, newsletters, etc.).

En France,
les enfants de 15 ans ou plus peuvent consentir eux-mêmes au traitement de leurs données fondé sur le consentement dans le cadre des services de la société d'information.

En-dessous de 15 ans, la loi « Informatique et Libertés » impose le recueil du consentement conjoint de l'enfant et du titulaire de l'autorité parentale.

1 LA PREUVE DU CONSENTEMENT

RGPD - ARTICLE 7-1

> Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en **mesure de démontrer que la personne concernée a donné son consentement** au traitement de données à caractère personnel la concernant.

1 LA PREUVE DU CONSENTEMENT

RGPD - ARTICLE 7-1

Pour ce faire, les responsables de traitement doivent documenter les conditions de recueil du consentement.
La documentation doit permettre de démontrer :

- la mise en place de mécanismes de consentement non contraints ou non liés à la réalisation d'une autre finalité ou d'un contrat (consentement « libre »)
- la séparation claire et intelligible des différentes finalités de traitement (consentement « spécifique »)
- la bonne information des personnes (consentement « éclairé »)
- le caractère positif de l'expression du choix de la personne (consentement « univoque »).

Pour conserver ces preuves, les responsables de traitement peuvent tenir un registre des consentements.

1 CONSENTEMENT RECUEILLI AVANT LE RGPD

Un consentement obtenu et recueilli avant le 25 mai 2018 peut demeurer valide, à la condition qu'il soit conforme aux nouvelles dispositions et conditions posées 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 de traitement doivent « rafraîchir » ou compléter le consentement recueilli auprès des personnes afin d'être considéré comme valide et conforme aux exigences du RGPD.

RGPD

LICÉITÉ DU TRAITEMENT

RGPD - Article 6-1

Découvrons maintenant en détail le fondement suivant :
LA NÉCESSITÉ CONTRACTUELLE

1. La personne concernée a **consenti au traitement** de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.
2. 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.

2 LA NÉCESSITÉ CONTRACTUELLE

Ce fondement correspond à deux cas de figure bien précis :

- l'exécution d'un contrat auquel la personne concernée est partie
- l'exécution de mesures précontractuelles prises à la demande de la personne concernée

Par exemple, dans le cadre de la souscription d'une **assurance auto**, un devis préalable doit être établi. L'assureur doit donc traiter, dans le cadre de mesures précontractuelles, un certain nombre de données relatives au véhicule et à son utilisation.

De même dans le cadre de l'**achat d'un bien sur internet**, le commerçant doit traiter pour l'exécution de ce contrat, des données relatives aux coordonnées de l'acheteur pour pouvoir organiser la livraison du bien.

LICÉITÉ DU TRAITEMENT

RGPD - Article 6-1

Découvrons maintenant en détail le fondement suivant :
L'OBLIGATION LÉGALE

1. La personne concernée a **consenti au traitement** de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.
2. 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.
3. Le traitement **est nécessaire au respect d'une obligation légale** à laquelle le responsable de traitement est soumis.

3 L'OBLIGATION LÉGALE

Le respect d'une obligation légale imposée au responsable de traitement.

« L'obligation légale » définie par le règlement européen doit être un texte du droit de l'Union ou du droit d'un État membre. Cette obligation n'est pas nécessairement de niveau législatif et peut donc être un texte de valeur règlementaire (décret, arrêté, etc.).

Par exemple, **les institutions financières sont tenues de signaler certaines opérations suspectes aux autorités compétentes** en vertu de règles visant à lutter contre le blanchiment d'argent.

De la même manière, **un employeur doit mettre en œuvre certains traitements de données** en raison d'obligations déclaratives pesant sur lui en matière fiscale et sociale.

4 LA SAUVEGARDE DES INTÉRÊTS VITAUX

Ce fondement doit être interprété strictement : il peut être utilisé uniquement lorsqu'il est impossible de recourir à un autre fondement.

Il est ainsi retenu en cas de menace pour la vie de la personne, lorsqu'elle est par exemple en incapacité physique d'exprimer son consentement quant à l'utilisation de ses données.

Ce fondement pourrait s'appliquer aux traitements nécessaires à la gestion des problématiques humanitaires (suivi des épidémies et catastrophes, rapatriements d'urgence).

5 L'INTÉRÊT PUBLIC

L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

Ce fondement ne pourra être utilisé que lorsque la finalité poursuivie correspond à une mission pour laquelle le responsable de traitement est compétent (par exemple : gestion des missions de la police municipale par le maire).

Autrement dit, les missions menées dans l'intérêt public d'un pays tiers ou relevant de l'exercice d'une autorité publique conférée en vertu d'une législation étrangère à l'UE n'entrent pas dans le champ d'application de cette disposition.

5 L'INTÉRÊT PUBLIC

L'exécution d'une mission d'intérêt public
ou relevant de l'exercice de l'autorité publique.

Par exemple, relèveront de ce fondement **les traitements liés à la gestion des inscriptions des collégiens et lycéens par les établissements scolaires.**

De la même manière, **la délivrance de subventions dans les domaines sportif et culturel par l'autorité départementale dans le cadre de sa politique budgétaire relève de ce fondement juridique.**

6 INTÉRÊTS LÉGITIMES

La poursuite d'intérêts légitimes par le responsable de traitement.

L'utilisation de cette base légale doit reposer sur une mise en balance entre les intérêts poursuivis par le responsable de traitement et les droits de la personne concernée ainsi que ses propres intérêts.

Il s'agira pour l'organisme de se poser la question suivante : la personne concernée peut-elle raisonnablement s'attendre à ce que ses données fassent l'objet d'un traitement à une fin spécifique ?

Le résultat de cet examen déterminera ainsi dans une large mesure si ce fondement peut servir de base juridique justifiant le traitement.

6 INTÉRÊTS LÉGITIMES

La poursuite d'intérêts légitimes par le responsable de traitement.

Par exemple, **une entreprise aura un intérêt légitime à assurer la sécurité des biens et des personnes au sein de son établissement** au moyen par exemple d'un dispositif de vidéosurveillance.

De la même manière, **une association aura un intérêt légitime à communiquer auprès de ses membres** sur son actualité.

L'ex G29 a rendu un avis sur cette notion :
avis 06/2014 sur la notion d'intérêt légitime

SYNTHÈSE

Un traitement est licite s'il est nécessaire :

- à l'exécution d'un contrat
- au respect d'une obligation légale
- à la sauvegarde d'intérêts vitaux
- à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique
- à des intérêts légitimes du responsable de traitement ou d'un tiers, dans le respect des intérêts ou des libertés et droits fondamentaux de la personne
- ou si la personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques

Unité 4 : Minimisation des données

INTRODUCTION

Le principe de minimisation découle du principe de finalité.

Il s'agit de ne collecter que ce dont vous avez strictement besoin pour répondre à l'objectif défini (la finalité).

DÉFINITION

RGPD - Article 5-1

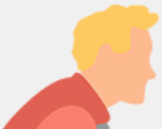
Ce principe signifie que les données collectées doivent être « **adéquates, pertinentes** et **limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

DÉFINITION

Principe de minimisation des données

Une donnée est pertinente si elle a un lien direct avec la finalité du traitement.

Il s'agit de ne collecter que ce dont vous avez strictement besoin pour répondre à l'objectif défini.



Exemple :
Recueillir des informations sur la situation familiale d'un candidat à l'embauche n'apparaît pas pertinent. Ces données ne permettent pas de répondre à la finalité de vérification des compétences d'un candidat.

En revanche, la collecte de données sur l'entourage familial peut être justifiée pour l'attribution d'avantages sociaux à un salarié embauché ou à sa famille.

La minimisation pose aussi la question de la proportionnalité :

certaines données peuvent être jugées pertinentes mais ne sont pas forcément indispensables au traitement.

Le principe de minimisation limite la collecte aux données strictement nécessaires par rapport à la finalité du traitement.

En revanche, des données peuvent être collectées de manière facultative, à la double condition d'en informer les personnes concernées et que celles-ci puissent choisir de les communiquer ou non.

Exemple :
La collecte de la date de naissance doit être facultative lors de la souscription à une carte de fidélité si cette information permet uniquement l'octroi d'avantages supplémentaires à la personne concernée (ex. offre pour l'anniversaire).

DÉFINITION

Principe de minimisation des données

Pour vérifier si vous respectez bien le principe de minimisation, posez vous les bonnes questions :

L'EXACTITUDE DES DONNÉES

RGPD - ARTICLE 5-1.d

Les données personnelles doivent être « **exactes** et, si nécessaire, **tenues à jour** ;

toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ».

Exemple :

Des données inexactes peuvent porter préjudice aux personnes concernées.

Prenons l'exemple d'une banque qui, suite à des incidents de paiement, inscrit le nom, la situation financière et les coordonnées bancaires d'un de ses clients dans le fichier détenu par la Banque de France .

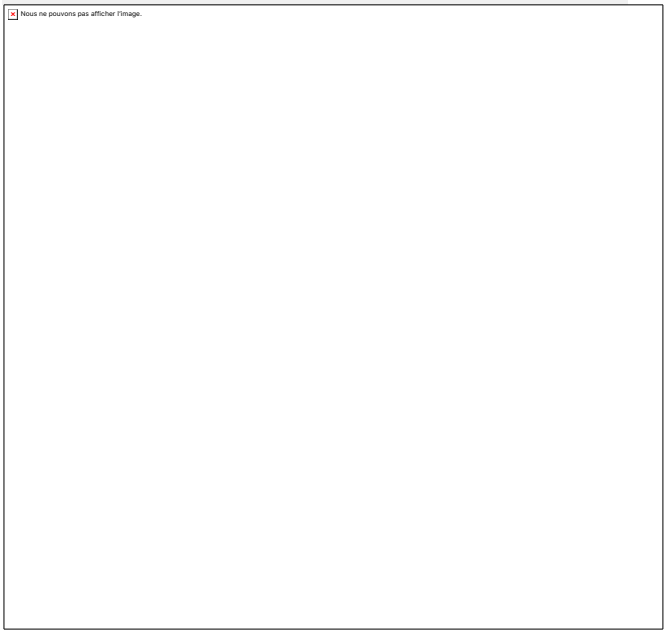
Cette banque est tenue d'effacer les données de ce client dès lors que sa dette est remboursée. L'absence de mise à jour de sa situation serait particulièrement pénalisante pour lui.

PERTINENCE DE LA COLLECTE

Date de naissance

La collecte de la date de naissance d'une personne n'est pas pertinente pour tout type de traitement.

Prenons l'exemple de l'envoi d'une lettre d'information : seules l'identité (nom/prénom) et l'adresse de la personne sont nécessaires pour atteindre le but poursuivi.

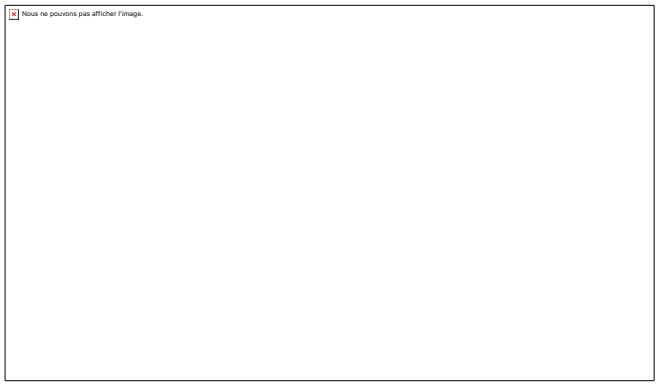


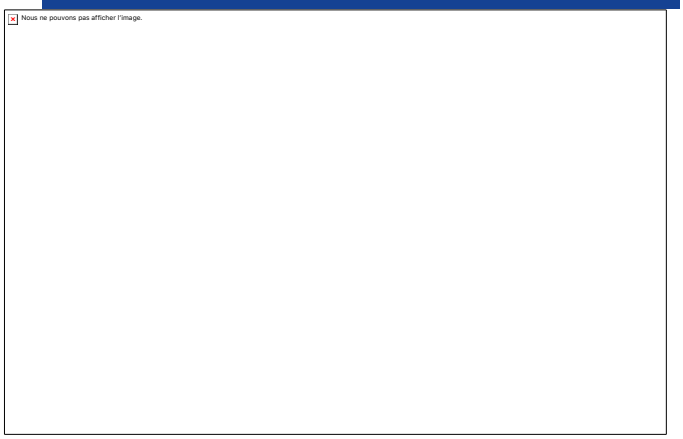
En revanche, elles ne doivent pas filmer les employés sur leur poste de travail, sauf circonstances particulières (employé manipulant de l'argent par exemple, mais la caméra doit davantage filmer la caisse que le caissier).

Les caméras ne doivent pas non plus filmer les zones de pause ou de repos des employés, ni les toilettes.

Si des dégradations sont commises sur les distributeurs alimentaires par exemple, les caméras ne doivent filmer que les distributeurs et non toute la pièce.

Enfin, les caméras ne doivent pas filmer les locaux syndicaux ou des représentants du personnel, ni leur accès lorsqu'il ne mène qu'à ces seuls locaux.





Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

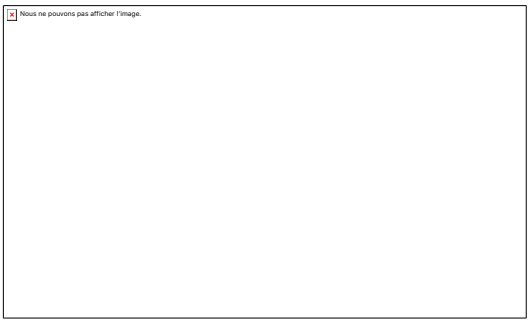
Nous ne pouvons pas afficher l'image.

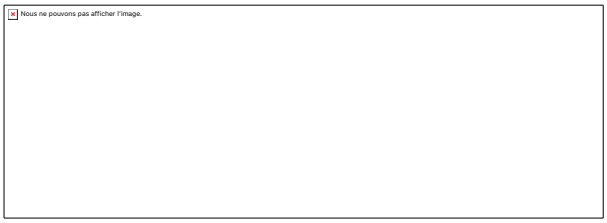
Nous ne pouvons pas afficher l'image.

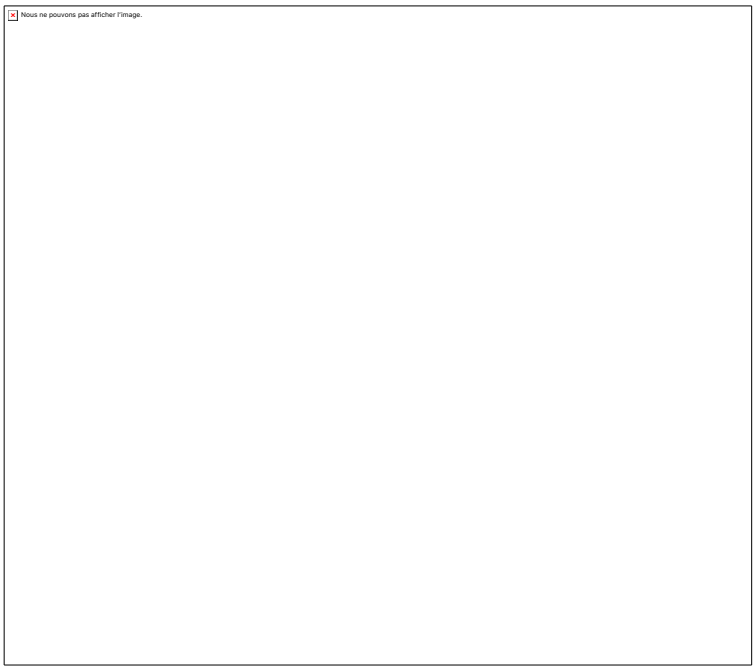
Nous ne pouvons pas afficher l'image.

Unité 5 : Protection particulière de certaines données

Introduction

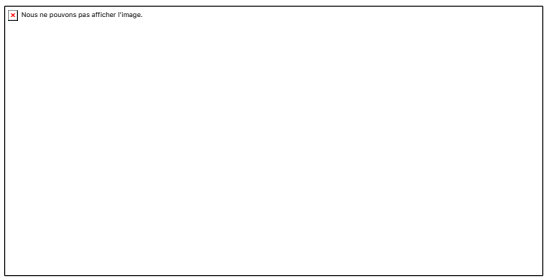




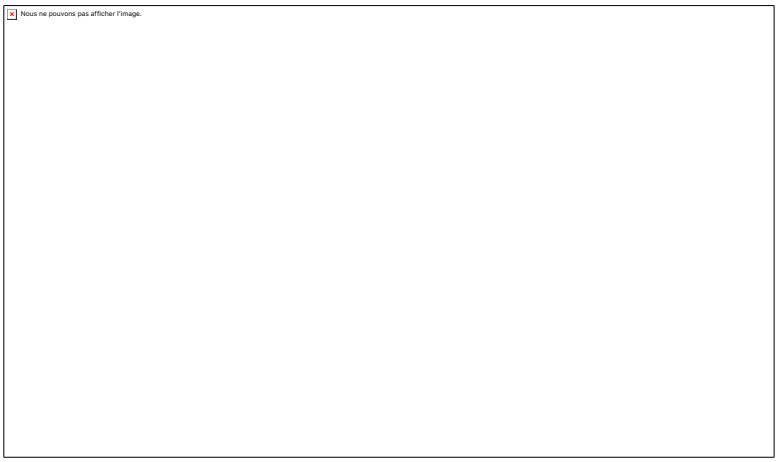


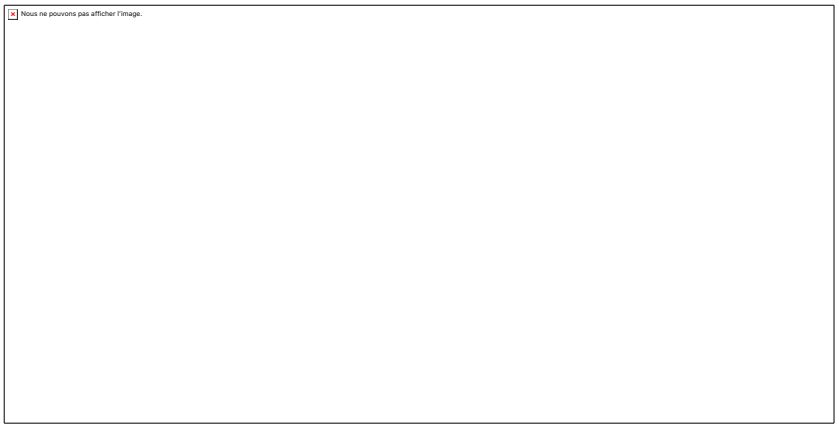
Définition

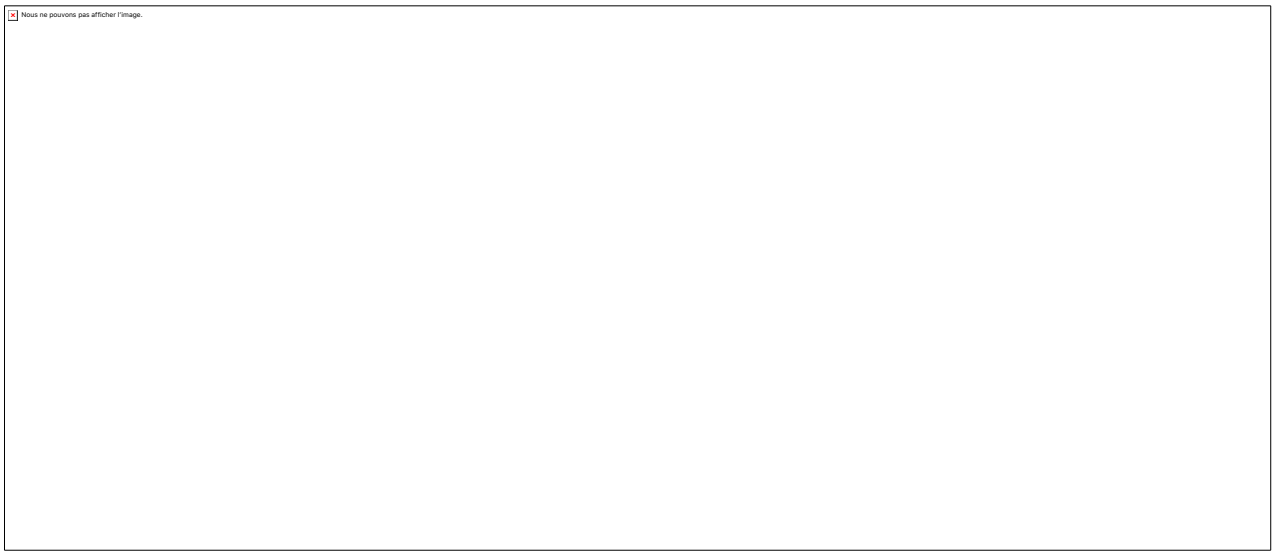
Données sensibles



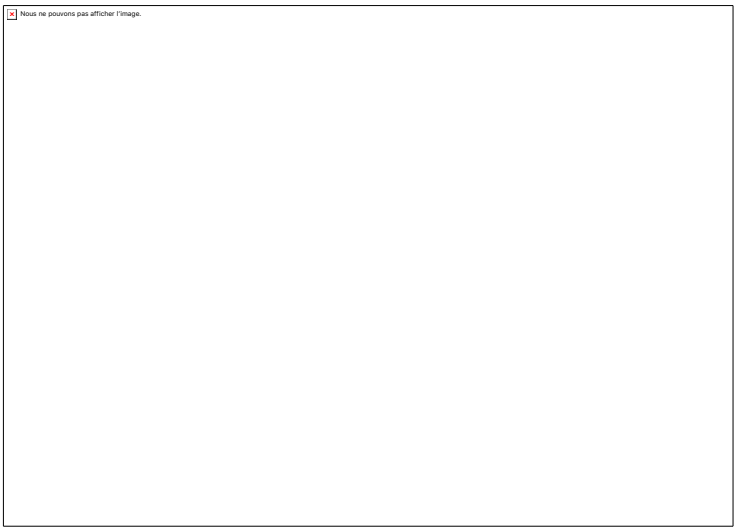
Exceptions

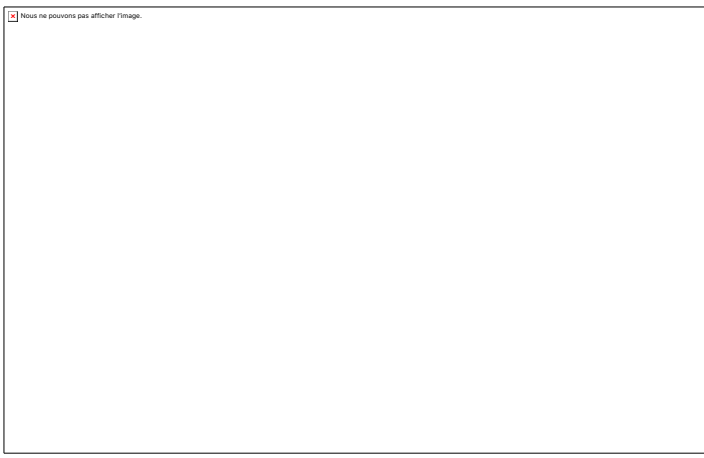




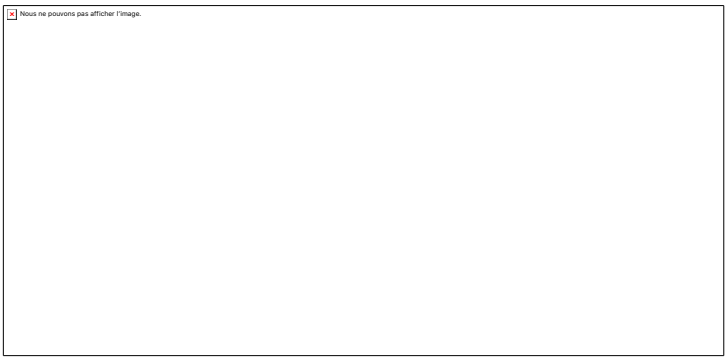


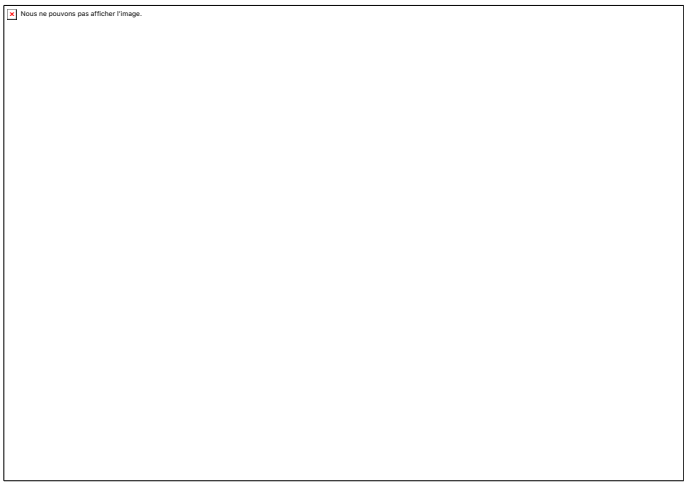
Consentement explicite





Données relatives aux condamnations pénales et aux infractions

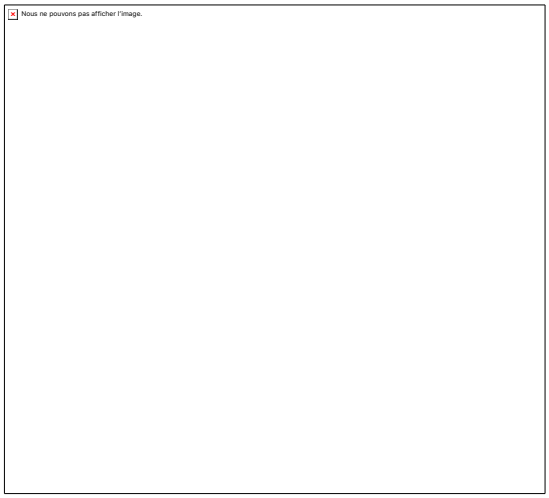


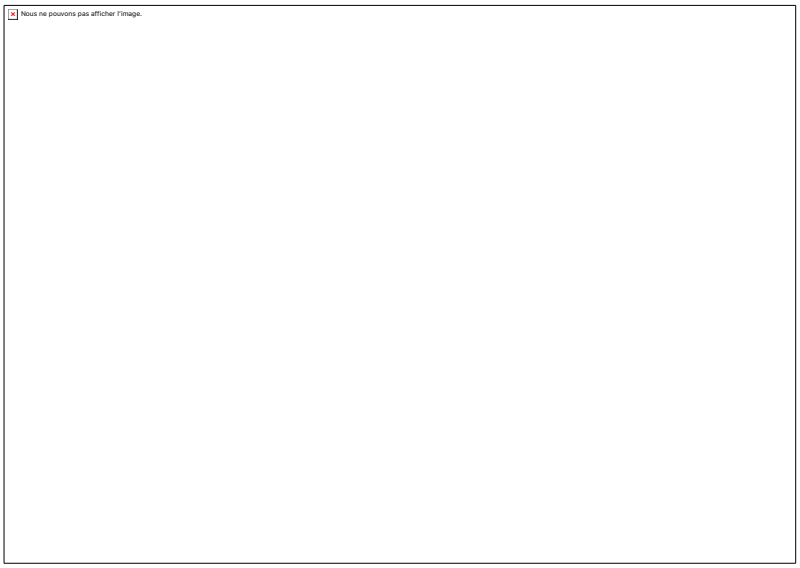


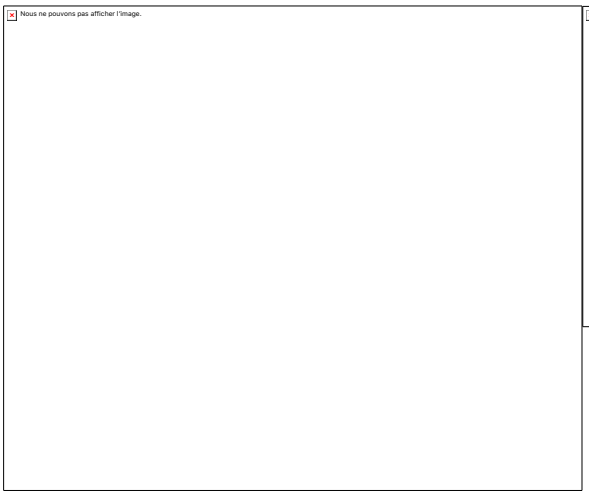
Synthèse

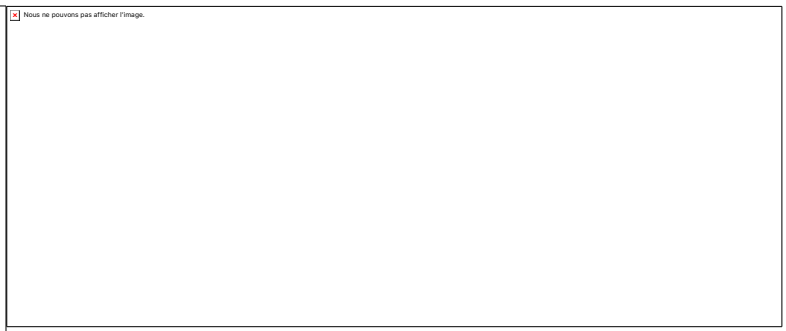
Unité 6 : Conservation limitée des données

Introduction

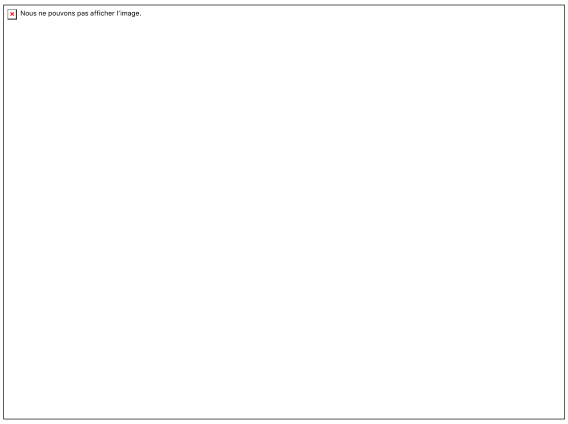


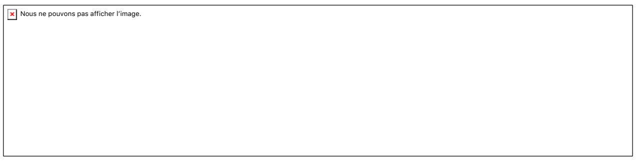


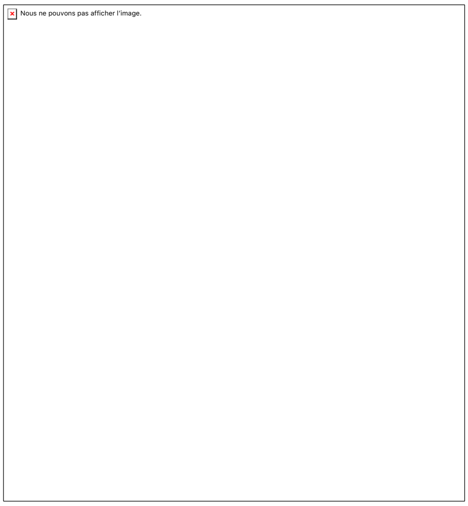


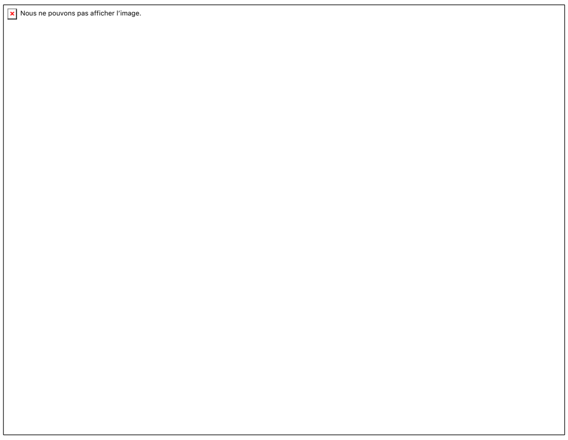


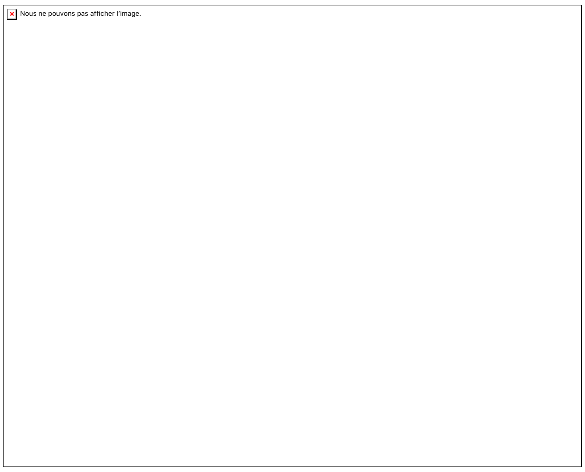
1. Durée de conservation











1. Le cycle de vie des données

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

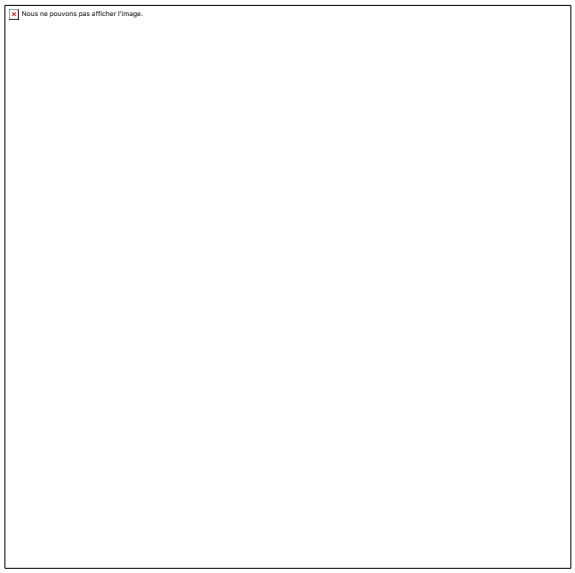
Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

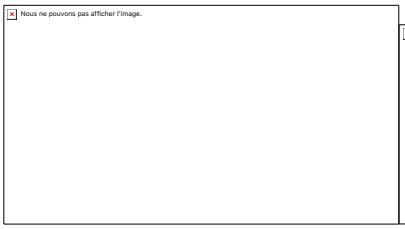
Nous ne pouvons pas afficher l'image.

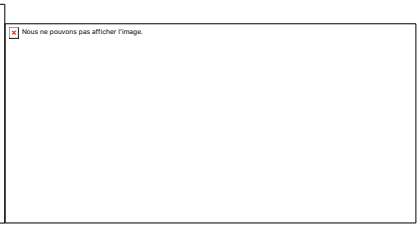
Synthèse



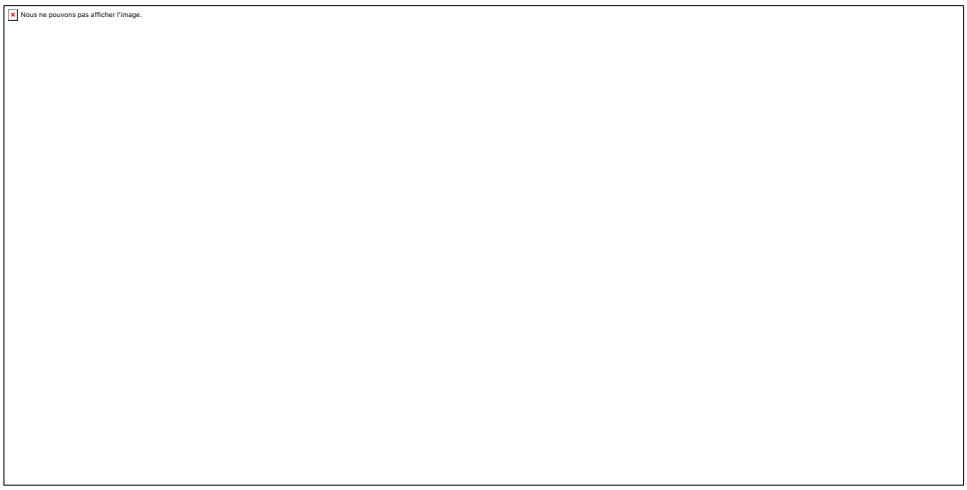
Unité 7 : Obligation de sécurité

Introduction

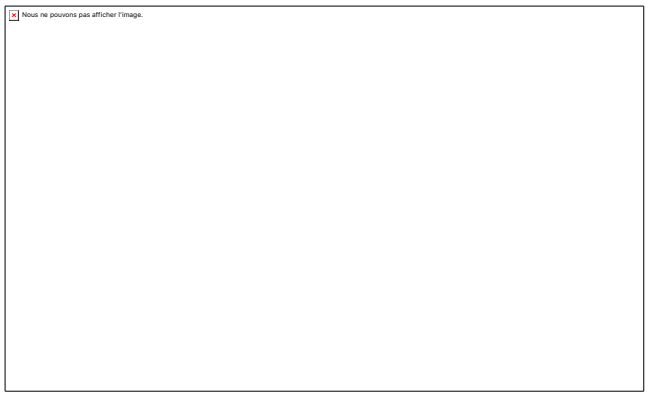




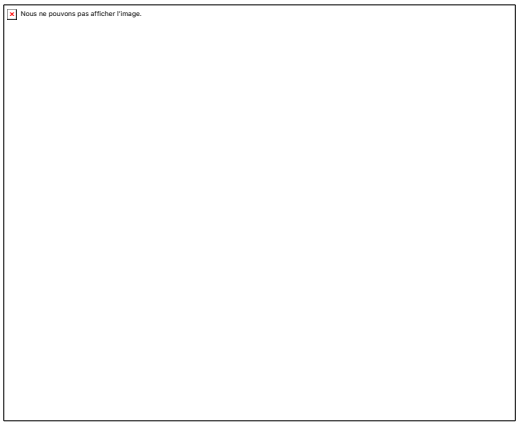
1. Définition



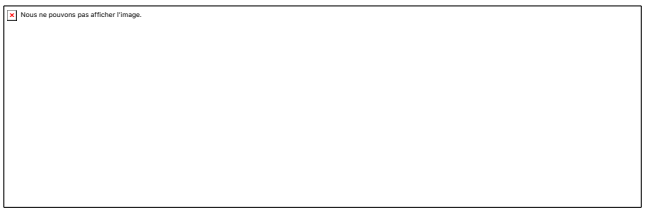
2. Les 3 principes de la sécurité

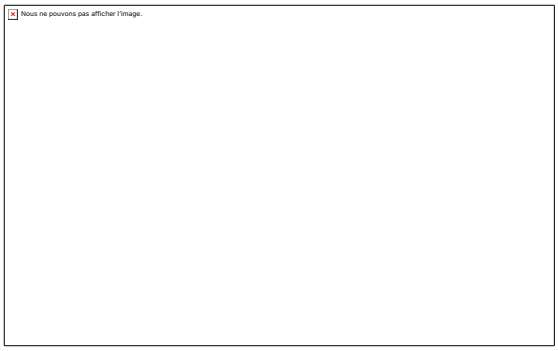


3. Les risques



4. Les mesures de sécurité





Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

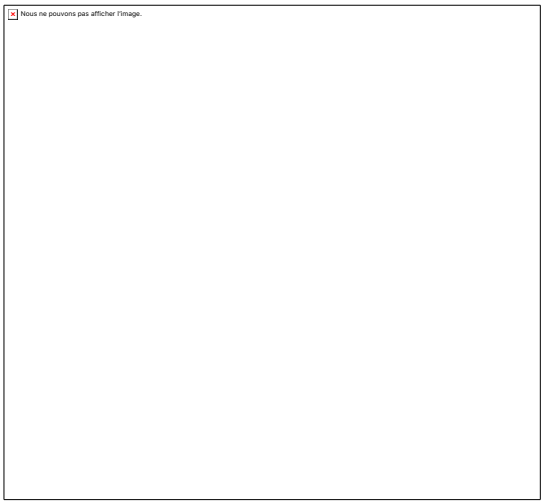
Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

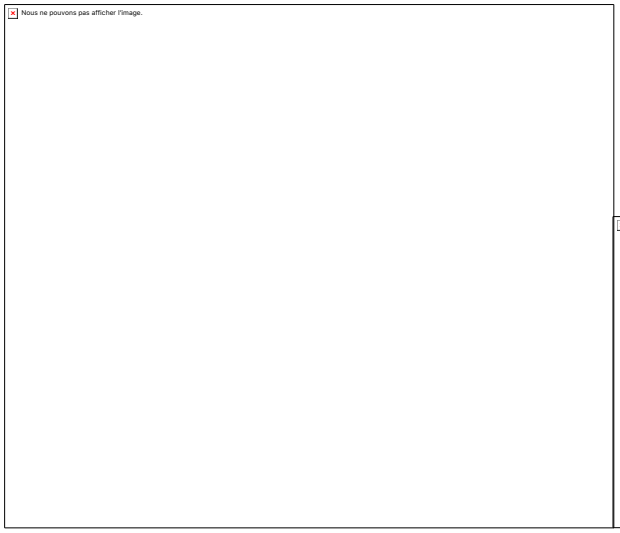
Nous ne pouvons pas afficher l'image.

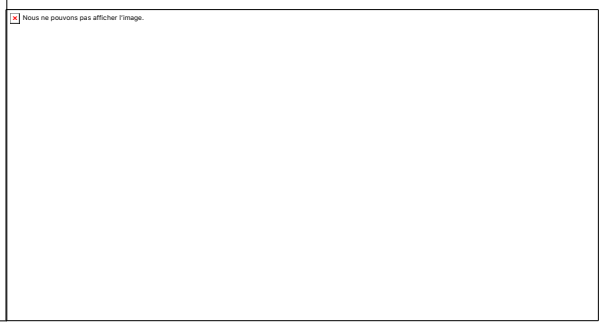
Synthèse



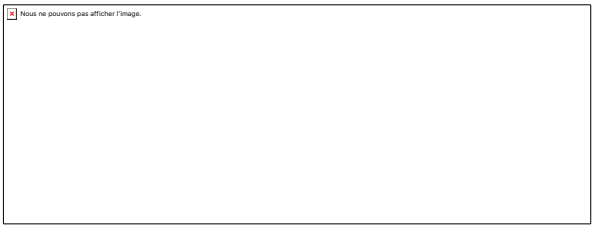
Unité 8 : transparence à l'égard des personnes concernées

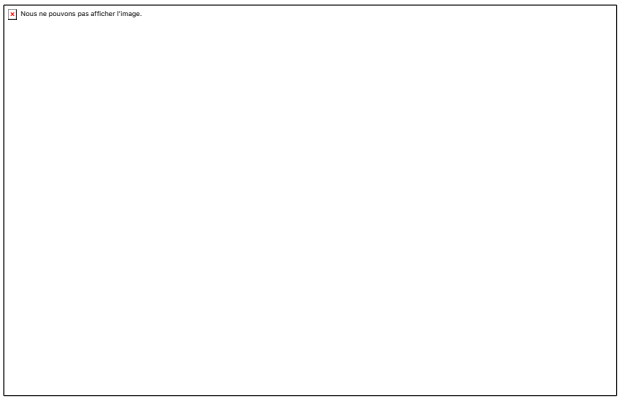
Introduction

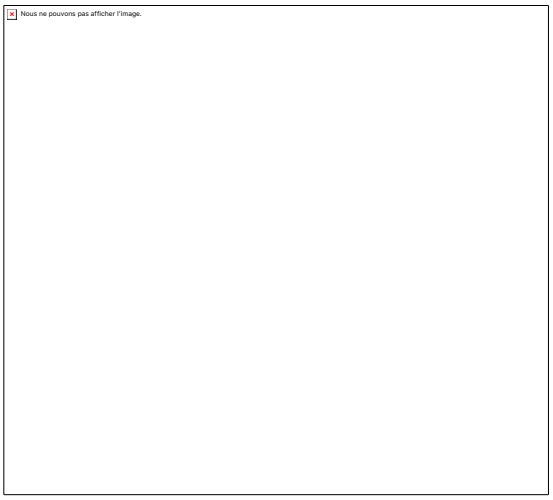


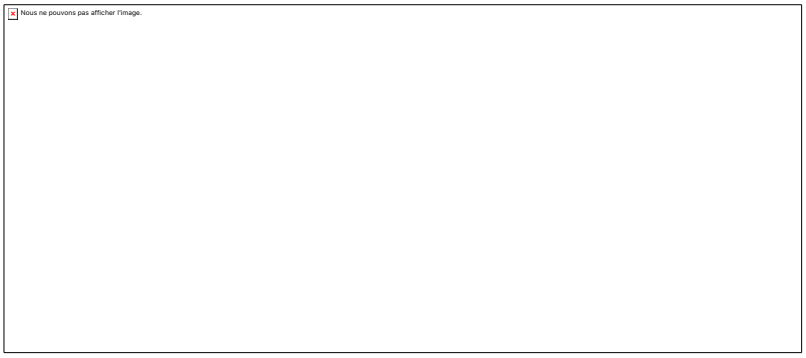


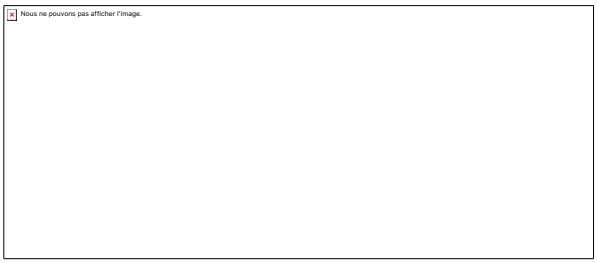
1. Le droit à l'information

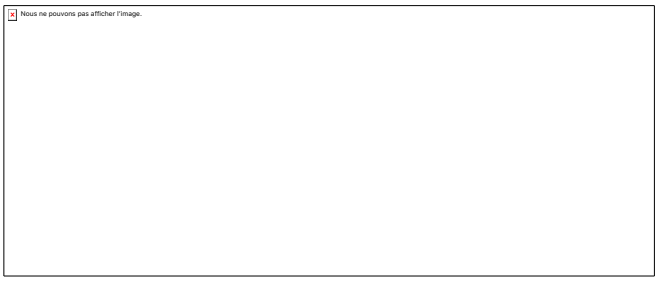


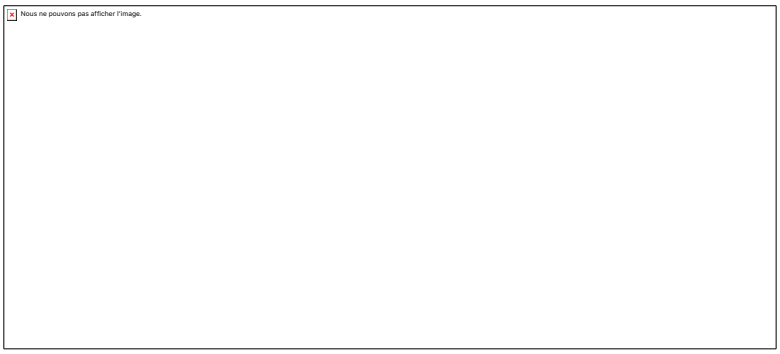




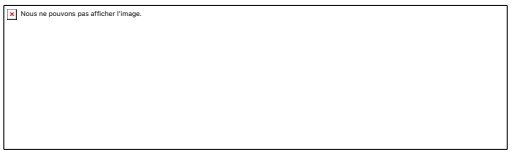


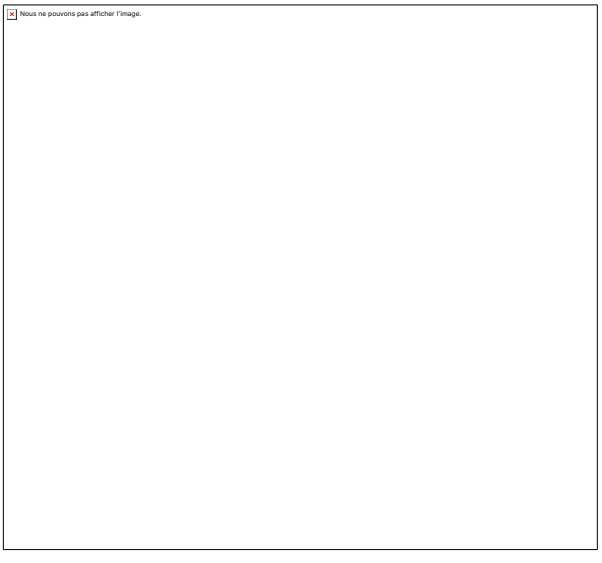


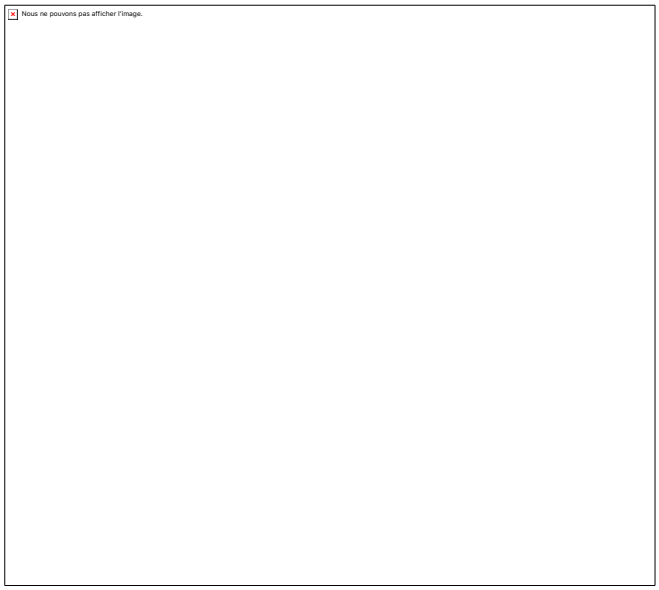




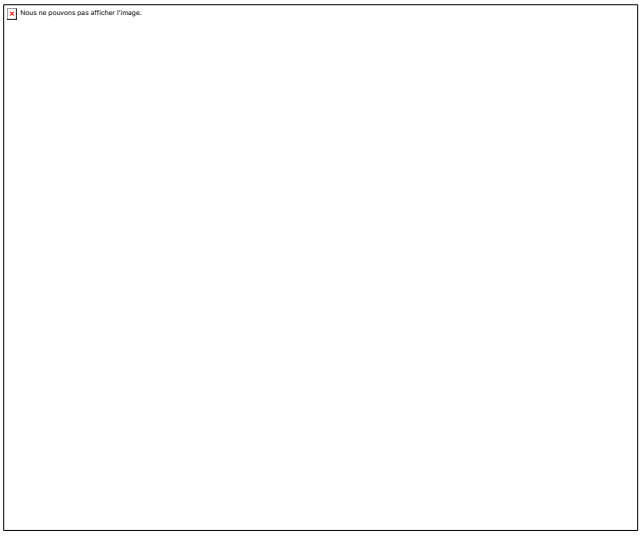
2. Informations à communiquer en cas de collecte directe des données



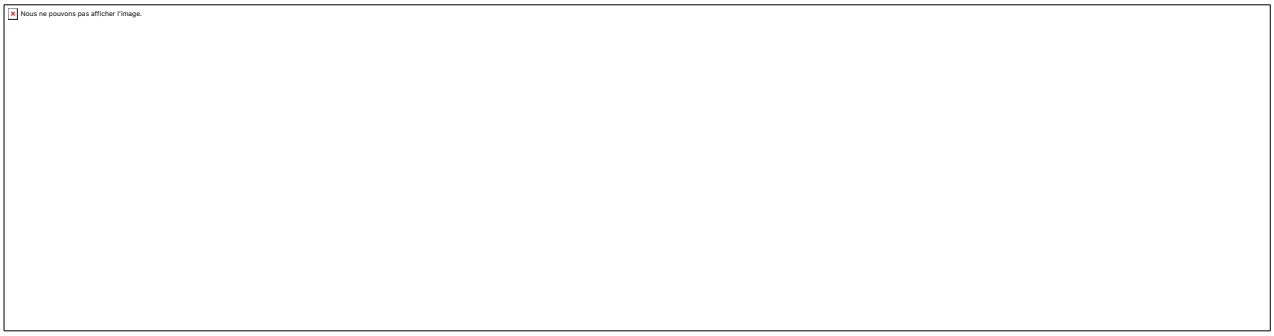




3. Informations à communiquer en cas de collecte indirecte des données



4. Les dérogations à l'obligation d'information



Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

5. La forme de l’information

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

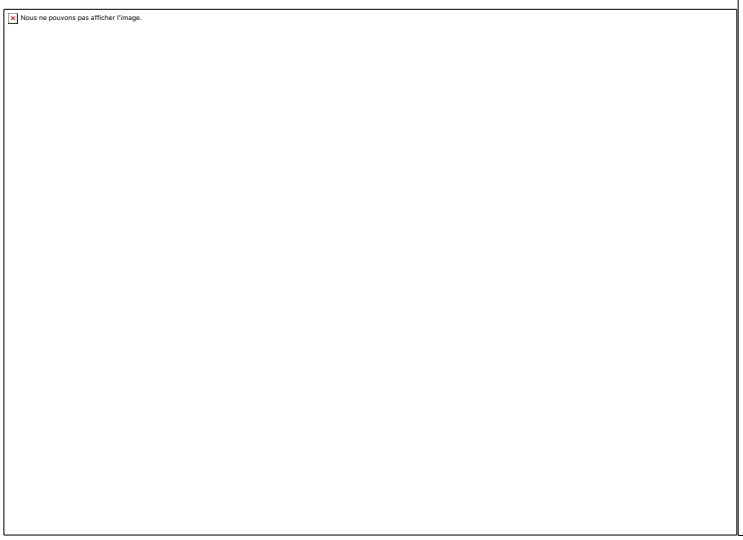
Nous ne pouvons pas afficher l'image.

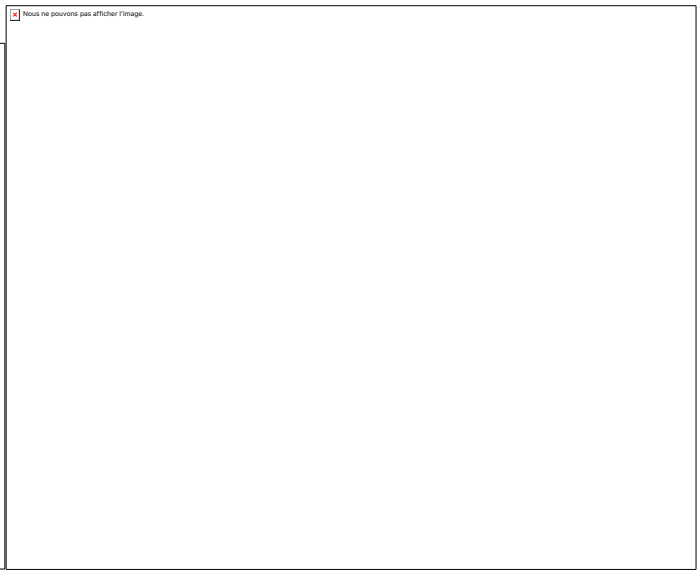
Nous ne pouvons pas afficher l'image.

Nous ne pouvons pas afficher l'image.

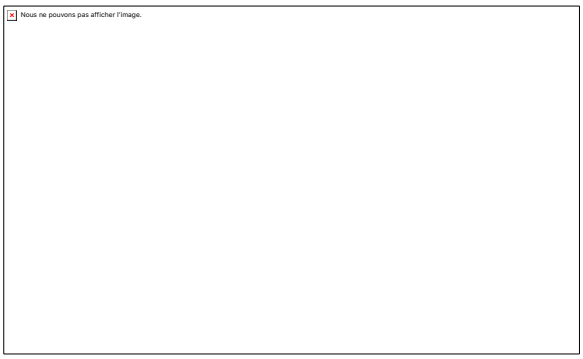
Nous ne pouvons pas afficher l'image.

6. Droit et forme de l’information



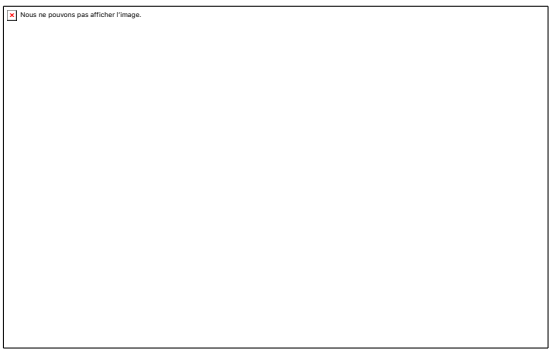


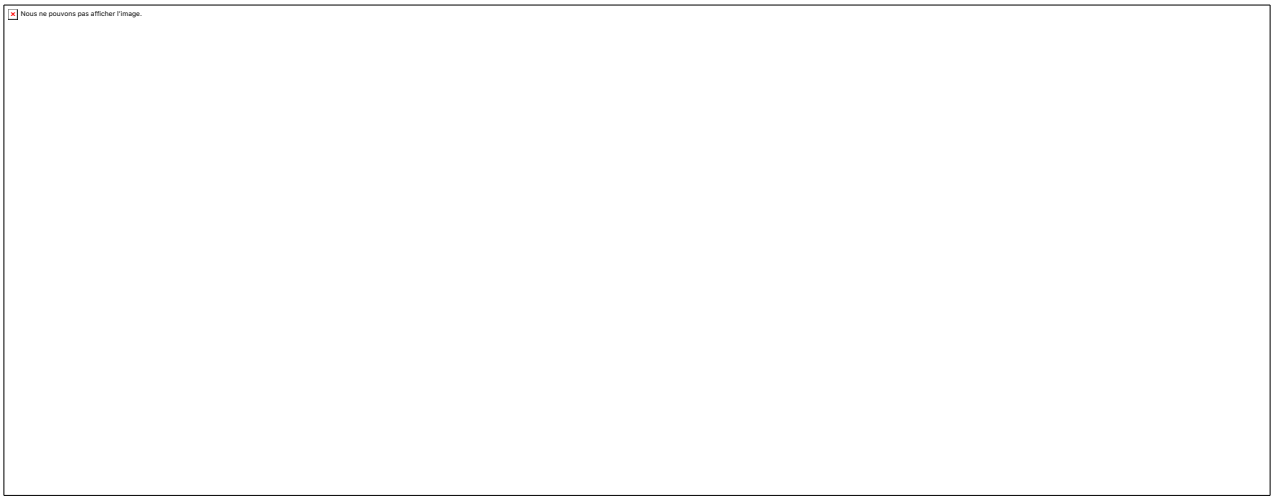
Synthèse



Unité 9 : droit des personnes sur leurs données

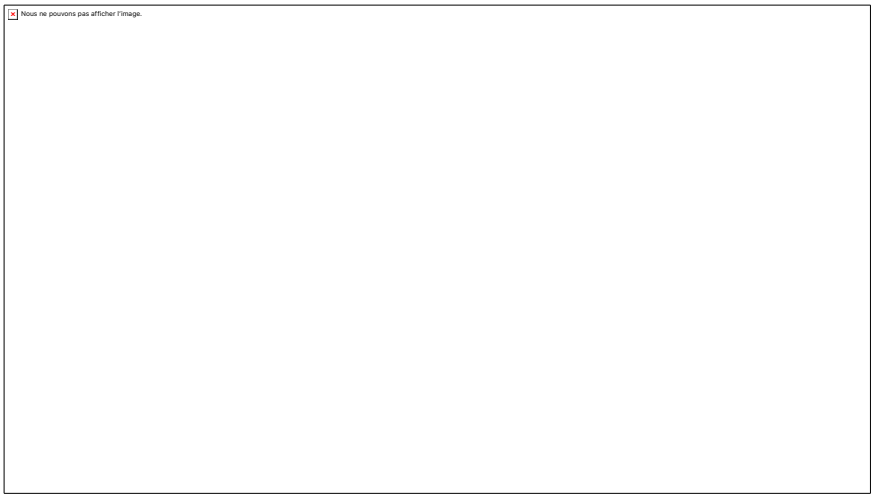
Introduction

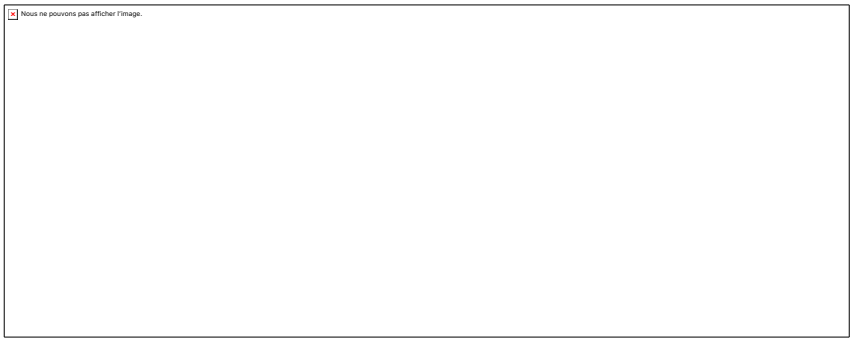


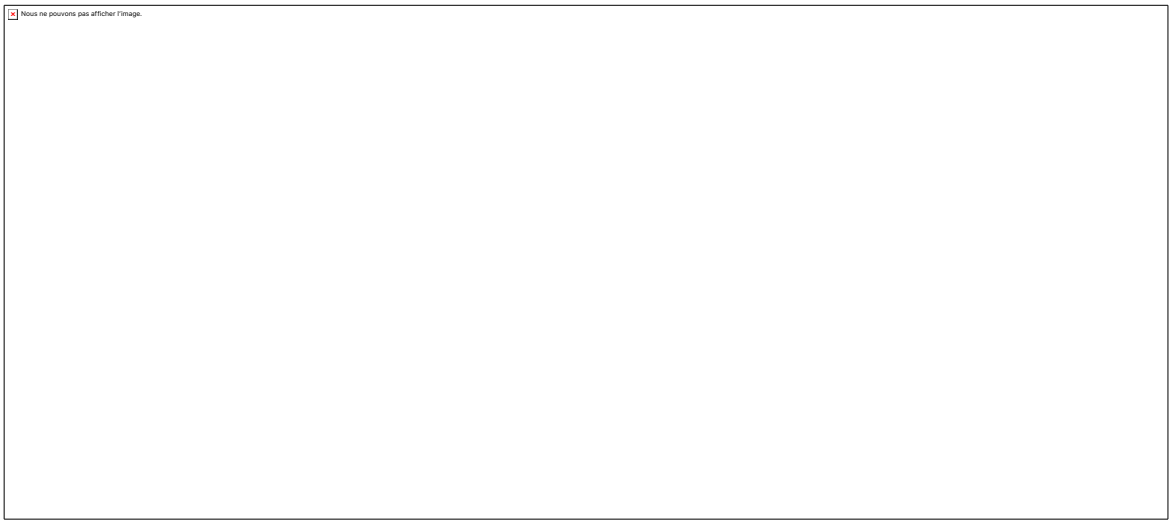


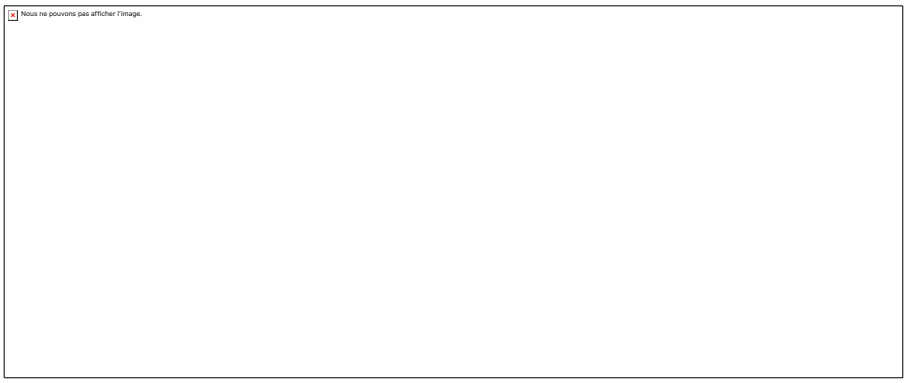
1. Droits renforcés par le RGPD

Il y a : le droit d’accès, le droit de rectification, le droit d’opposition et enfin le droit à l’effacement.









Exemple :
Antoine a commis une erreur lorsqu'il a rempli le formulaire de création de son dossier. Les calculs effectués sur cette base d'informations ont estimé un remboursement inférieur à ce qu'il aurait été en droit d'avoir.

Antoine peut faire valoir son droit de rectification pour que l'erreur soit corrigée et que le montant du remboursement soit actualisé.

DROIT D'OPPOSITION

RGPD - ARTICLE 21

Les personnes peuvent **s'opposer au traitement de leurs données**. Ce droit d'opposition peut être exercé à tout moment pour des raisons tenant à la situation particulière de la personne. Dans le cas de la prospection, la personne n'a pas besoin de fournir de motif pour exercer son droit d'opposition.

Le droit d'opposition **n'est pas un droit à la suppression simple et définitive** de toutes les données ou du compte qui est rattaché à une personne.

Par exemple, seule une rupture de contrat permet la suppression d'un compte chez un opérateur mobile ou un site de e-commerce.

Si une demande d'opposition ne **concerne pas la prospection**, l'organisme pourra justifier son refus au motif que :

- il existe des motifs légitimes et impérieux à traiter les données ou que celles-ci sont nécessaires à la constatation, l'exercice ou la défense de droits en justice
- la personne a consenti (elle doit alors retirer son consentement)
- un contrat lie la personne avec l'organisme (la personne peut mettre fin au contrat)
- une obligation légale impose à l'organisme de traiter les données
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Exemple :
Une personne reçoit des emails publicitaires sur sa boite e-mail personnelle et ne souhaite plus figurer dans la base de prospection ou une personne refuse de figurer dans l'annuaire universel des abonnés au téléphone

DROIT À L'EFFACEMENT (« DROIT À L'OUBLI »)

RGPD - ARTICLE 17

Les personnes peuvent demander à un organisme l'effacement des données personnelles les concernant. Ce droit s'applique seulement dans l'une de ces **six situations** :

- les données ne sont plus nécessaires au regard des finalités pour lesquelles elles sont collectées ou traitées
- la personne retire son consentement au traitement de ses données
- la personne s'oppose au traitement et il n'existe pas de motif légitime impérieux
- le traitement est illicite (ex : le traitement s'effectue en violation d'une disposition du code de la santé publique)
- les données doivent être effacées pour respecter une obligation légale
- les données ont été collectées auprès de mineurs dans le cadre de l'offre de services de la société de l'information.

En revanche, **le droit à l'effacement ne peut pas s'appliquer s'il va à l'encontre** :

- de la liberté d'expression et d'information
- du respect d'une obligation légale
- d'un motif d'intérêt public dans le domaine de la santé publique
- des fins archivistiques dans l'intérêt public, des fins statistiques, de recherche scientifique ou historique
- de la constatation, de l'exercice ou de la défense de droits en justice.

2. Nouveaux droits

L'objectif du droit à la portabilité est de permettre aux personnes de **gérer leurs données** en les réutilisant par exemple pour un usage personnel. Il s'agit également de **faciliter la libre circulation des données d'un prestataire à un autre** afin de stimuler la concurrence entre responsables de traitement.

Ce droit permet à toute personne de **récupérer les données personnelles qu'elle a fournies à un responsable de traitement**. Ces données doivent être transmises à la personne qui les demande dans un format structuré, couramment utilisé et lisible par une machine.

Ce droit inclut aussi la possibilité de **transmettre ces données à un nouveau responsable de traitement**, en demandant au responsable initial de procéder au transfert, si cela est techniquement possible.

L'existence de ce nouveau droit implique que les responsables de traitement travaillent ensemble à l'élaboration de formats **interopérables** pour permettre l'exercice effectif de ce droit.

Ce droit est applicable seulement si les deux conditions cumulatives suivantes sont réunies :

- **le traitement est fondé sur le consentement de la personne ou sur un contrat**.
Sont donc exclus les traitements fondés sur l'intérêt public, l'intérêt légitime du responsable de traitement ou une obligation légale. Le droit à la portabilité ne peut donc pas s'appliquer à la vidéosurveillance, à la lutte contre la fraude ou au contrôle d'accès à des locaux

- **le traitement est effectué à l'aide de procédés automatisés.**

Exemple :
Martin souhaite changer de fournisseur de messagerie électronique.
En faisant valoir son droit à la portabilité, il peut demander que toutes ses données d'agenda et de contacts ainsi que ses messages soient transmis au nouveau fournisseur.

Les données concernées par ce droit à la portabilité sont :

- **les données fournies** par la personne.
Ce sont les données déclarées comme son nom, son âge, son adresse.

- **les données générées** par son activité.
Ce sont des données observées comme par exemple les données de localisation, de rythme cardiaque, de trafic, d'historique d'achats.

En revanche, ce droit ne porte pas sur :

- **les données anonymes**

- **les données déduites ou dérivées.**
Ce sont des données créées par l'organisme comme par exemple le résultat d'analyse de risque de crédit ou d'une appréciation relative à la santé d'un utilisateur, etc.

Exemple :
À son domicile, Brigitte dispose d'un compteur intelligent.
Son fournisseur d'énergie possède trois catégories d'informations la concernant :
- les données qu'elle a fournies : son nom, prénom, adresse, etc.
- les données générées par le compteur, à savoir les relevés de consommation.
- les données déduites par le fournisseur pour établir un profil à partir des relevés de consommation.

Si Brigitte souhaite exercer son droit à la portabilité vers un fournisseur d'énergie concurrent, seules les données qu'elle a fournies et les relevés de compteur pourront être transférés.

Les données issues des analyses menées par le fournisseur ne sont pas concernées.

Enfin, l'exercice du droit à la portabilité **ne doit pas porter atteinte aux droits et libertés des tiers** dont les données se trouveraient dans les données transmises suite à une demande de portabilité.
Cela signifie que le nouveau responsable de traitement ne doit pas traiter les données qu'il reçoit d'une manière qui porterait atteinte aux droits et libertés des autres personnes concernées.

Exemple :
Martin a demandé la portabilité de sa messagerie électronique.
Le nouveau fournisseur de messagerie ne pourra pas utiliser les adresses de ses contacts à des fins de prospection commerciale.

Découvrons maintenant le droit à la **limitation du traitement**.

Le droit à la limitation vient compléter les cinq autres droits que nous venons de voir.

Lorsqu'une personne souhaite rectifier des informations ou s'opposer à ce qu'elles soient traitées, **l'organisme dispose d'un délai d'un mois pour traiter la demande**.
Pendant ce délai, cette personne peut faire valoir son droit à la limitation pour **geler l'utilisation de ces données**.
Concrètement, **l'organisme ne devra plus utiliser les données mais devra les conserver**.

Exemple :
Sophie découvre qu'une photo gênante d'elle a été publiée sur un réseau social. Elle décide de contacter le réseau social pour s'opposer à la publication de cette photo. Dans l'attente de savoir s'il existe un motif légitime à la conserver, Sophie fait valoir son droit à la limitation pour que la photo soit retirée du réseau pendant ce délai.

Inversement, il est possible de **demander la limitation du traitement** de certaines données lorsque l'organisme souhaite lui-même les effacer.

Exemple :
Sébastien intente une action en justice qui se fonde notamment sur des extraits de vidéosurveillance.

Les images de vidéosurveillance doivent en principe être supprimées au bout d'un mois.

Sébastien peut faire valoir son droit à la limitation du traitement pour empêcher leur suppression jusqu'à l'issue de la procédure judiciaire.

La limitation du traitement peut être demandée uniquement dans l'**une des 4 situations suivantes** :

- lorsque la personne a fait valoir son **droit de rectification**.
Le droit à la limitation s'applique le temps que le responsable de traitement vérifie l'exactitude des données personnelles concernées

- Lorsque la personne a fait valoir son **droit d'opposition**.
Le droit à la limitation s'applique le temps de déterminer si les intérêts légitimes du responsable de traitement prévalent sur ceux de la personne concernée

- lorsque des données sont sur le point d'être effacées alors qu'elles sont encore nécessaires à la personne concernée pour **la constatation, l'exercice ou la défense de droits en justice**

- lorsque le **traitement est illicite** mais que la personne concernée préfère la limitation plutôt que l'effacement des données.

Le responsable de traitement doit informer la personne concernée qui a obtenu la limitation du traitement avant la levée d'une telle limitation.

La limitation entraîne le **gel temporaire** du traitement des données, sauf si :

- la personne donne son consentement à une autre forme de traitement

- le traitement de ces données est nécessaire à la constatation, l'exercice ou la défense de droits en justice, à la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

Découvrons maintenant la décision individuelle automatisée.

DROIT DE NE PAS FAIRE L'OBJET D'UNE DÉCISION EXCLUSIVEMENT FONDÉE SUR UN TRAITEMENT AUTOMATISÉ

RGPD - ARTICLE 22

Le **profilage** consiste à utiliser les données personnelles d'un individu en vue d'**analyser** et de **prédire son comportement**, comme par exemple déterminer ses performances au travail, sa situation financière, sa santé, ses préférences, ses habitudes de vie, etc.

Toute personne a le droit de ne pas faire l'objet d'une décision entièrement automatisée - souvent basée sur un profilage - qui a un effet juridique ou qui l'affecte sensiblement.

Un organisme peut néanmoins automatiser ce type de décision si l'une de ces conditions est remplie :

- la personne concernée a donné son consentement explicite
- la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et l'organisme
- la décision automatisée est autorisée par des dispositions légales spécifiques.

Exemples :
Les décisions produites de **manière automatique** peuvent avoir des **effets significatifs sur les individus** notamment si cette décision :

- entrave l'accès à un service (ex. rejet automatique d'un crédit)
- désavantage financièrement la personne (ex. absence de prime, hausse du coût d'un service)
- ferme l'accès à un emploi (ex. refus automatique d'une candidature à un emploi déposée en ligne)
- produit un effet juridique concernant la personne (ex. exclusion du bénéfice d'un contrat ou d'une prestation sociale).

Dans tous les cas, la personne doit pouvoir :

- **être informée** qu'une décision entièrement automatisée a été prise à son encontre
- **demander à connaître** la logique et les critères employés pour prendre la décision
- **contester** la décision et **exprimer** son point de vue
- **demander l'intervention** d'un être humain qui puisse réexaminer la décision.

3. La possibilité de ne pas donner suite à la demande de la personne concernée

Le responsable de traitement est tenu de **faciliter l'exercice des droits** et ne peut en aucun cas refuser de donner suite à une demande sans le justifier auprès de la personne concernée.

Le RGPD autorise ainsi les responsables de traitement à ne pas donner suite à une demande dans les cas suivants :

S'agissant du droit d'opposition, lorsqu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou pour la constatation, l'exercice ou la défense des droits en justice.

S'ils peuvent démontrer qu'ils ne sont pas en mesure d'identifier la personne concernée.

S'agissant du droit à l'effacement, lorsque leur mise en œuvre porte atteinte à l'exercice d'un droit individuel (liberté d'expression et d'information, exercice des droits en justice) ou s'oppose à un motif d'intérêt public (obligation légale, mission d'intérêt général, archive).

S'agissant des droits d'accès et à la portabilité, lorsque sa mise en œuvre porte atteinte aux droits ou libertés d'autrui (notamment secret des affaires, propriété intellectuelle, droit d'auteur protégeant un logiciel).

S'ils peuvent démontrer que les demandes d'une personne sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif (dans ce cas le responsable pourra choisir de répondre en exigeant le paiement de frais raisonnables).

Dans chaque cas,
le responsable de traitement doit informer la personne concernée de cette décision sans tarder.

Il dispose d'un mois à compter de la réception de la demande pour lui indiquer les motifs de son inaction, ainsi que de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel.

4. Notification de l'exercice des droits

Lorsqu'une personne exerce son droit de rectification, d'effacement ou de limitation, **le responsable de traitement doit en informer tous les organismes à qui il a transmis les données personnelles en question**.

Cette communication doit impérativement être effectuée à moins qu'elle ne se révèle impossible ou n'exige des efforts disproportionnés.

Synthèse

Les personnes concernées sont placées au cœur de la règlementation en matière de protection des données.

Les droits renforcés ou nouveaux dont elles bénéficient leur permettent de garder la main sur leurs données et de pouvoir réagir en cas d'atteinte à leurs droits, voire en cas de préjudice.

Unité 10 : encadrement des transferts de données hors de l'Union Européenne

Introduction

L'application des huit règles d'or assure une protection maximale des données personnelles.

Cette protection doit être assurée à tout moment, et ce même si les données sortent de l'Union européenne.

1. Bulle de protection

Le RGPD vise à créer une bulle de protection autour des données personnelles.

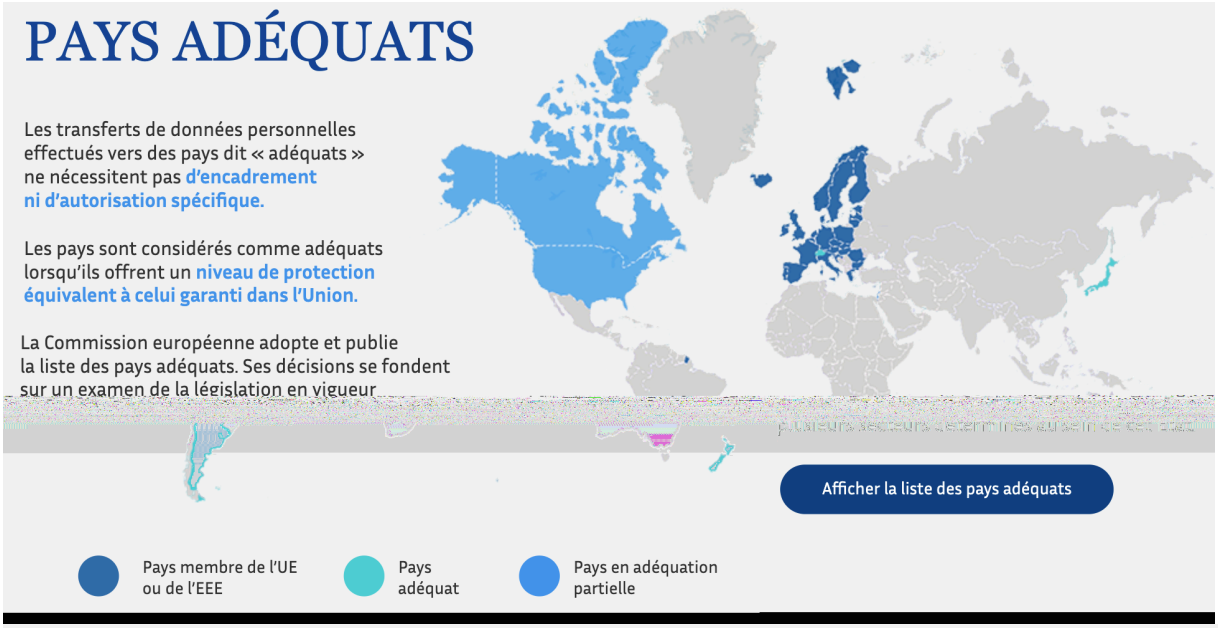
Il autorise les responsables de traitement et les sous-traitants à transférer les données personnelles hors de l'Union européenne ou de l'Espace économique européen, à condition d'assurer aux données un niveau de protection équivalent.

Cette protection s'applique aux données personnelles, y compris celles qui sont codées et chiffrées.
Seules les données anonymisées ne sont pas concernées.

La bulle de protection doit suivre les données, peu importe où elles sont transmises.

Les principes du RGPD doivent donc être respectés par tous les destinataires successifs.

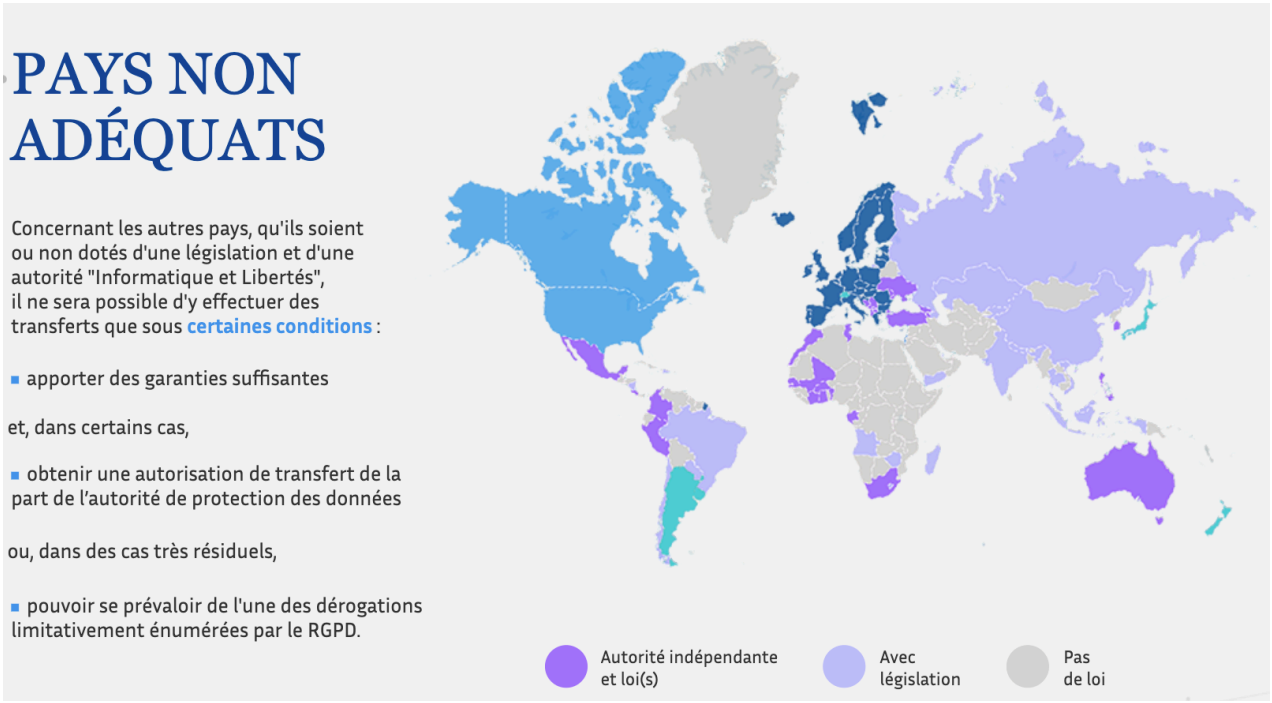
2. Pays adéquats



Pays adéquats (au 01/03/2019) :
Andorre, Argentine, Suisse, Îles Féroé, Guernesey, Israël, Île de Man, Jersey, Nouvelle Zélande, Uruguay, Japon

Adéquation partielle (au 01/03/2019) :
Canada (adéquation limitée au secteur commercial)
Etats-Unis (adéquation limitée aux entreprises adhérentes au Privacy Shield)

3. Pays non adéquats



GARANTIES APPROPRIÉES

Le RGPD offre des outils juridiques aux responsables de traitement et aux sous-traitants **afin d'encadrer les transferts vers les pays non adéquats.**

Il s'agit :

- des **règles d'entreprise contraignantes** (BCR) approuvées par l'autorité de contrôle compétente. Cet outil concerne les multinationales implantées dans plusieurs pays européens, et effectuant de nombreux transferts de données depuis leurs entités ou entre celles-ci, vers des pays n'assurant pas un niveau de protection équivalent à celui de l'Union européenne

- des **certifications** approuvées par l'autorité de contrôle compétente

- des **codes de conduite** approuvés par l'autorité de contrôle compétente. Ces codes de bonnes pratiques élaborés par des représentants de communautés de professionnels déclinent pour un secteur d'activité les conditions de mise en application des règles de protection des données

- des **clauses contractuelles types** (CCT) adoptées par la Commission européenne ou les autorités de contrôle. Il s'agit de modèles de clauses à insérer dans les contrats, encadrant les transferts entre deux responsables de traitement et les transferts entre un responsable de traitement et un sous-traitant

- des **instruments juridiquement contraignants** entre autorités ou organismes publics. Par exemple, une convention internationale.

Lorsque les organismes s'appuient sur l'un de ces outils, ils peuvent procéder au transfert de données personnelles sans autorisation.

AUTORISATION DE TRANSFERT

En l'absence de ces garanties, les organismes doivent faire une **demande d'autorisation** auprès de l'autorité de contrôle compétente fondée sur :

- des **clauses contractuelles spécifiques** (ad hoc) entre l'organisme exportateur et l'importateur

ou

- des **dispositions intégrées à des arrangements administratifs** entre autorités ou organismes publics.

4. Dérogation à l'obligation d'encadrer le transfert

DÉROGATIONS À L'OBLIGATION D'ENCADRER LE TRANSFERT

Les organismes doivent s'efforcer de mettre en place des garanties appropriées et ne doivent recourir aux exceptions prévues par le Règlement qu'en l'absence de telles garanties.

L'article 49 du RGPD fait l'objet d'une interprétation stricte par les autorités de protection des données, **afin que l'exception ne devienne pas la règle.**

DÉFINITION

RGPD - Article 49-1

« **En l'absence de décision d'adéquation ou de garanties appropriées** y compris des règles d'entreprise contraignantes, un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes :

A la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle [...]

B le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée

C le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale »

D le transfert est nécessaire pour des motifs importants d'intérêt public

E le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice

F le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement

G le transfert a lieu au départ d'un registre qui [...] est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime[...].

L'article 49 prévoit une autre dérogation pour les transferts effectués vers des pays non adéquats et qui ne bénéficient ni de garanties appropriées, ni d'une des situations listées juste avant.

Cette dérogation est valable pour les transferts **nécessaires à des fins d'intérêts légitimes impérieux**, à condition :

- de respecter les intérêts et les droits des personnes concernées
- de ne toucher qu'un nombre limité de personnes
- de ne pas répéter ce transfert
- d'évaluer toutes les circonstances entourant ce transfert et d'appliquer des garanties appropriées.

Bien que cette dérogation évite à l'organisme de demander une autorisation, il doit tout de même informer l'autorité de contrôle avant d'effectuer le transfert.

5. Transfert des données non autorisées

Le RGPD protège les données des personnes se trouvant en Union européenne en indiquant qu'aucun jugement ou décision étrangère à l'Union européenne ne peut imposer à un responsable de traitement ou sous-traitant de transférer des données personnelles en dehors de l'Union, à moins qu'une convention internationale ne l'autorise.

6. Information des personnes et registres

Les transferts ainsi que leur encadrement (adéquation ou garanties appropriées) doivent figurer dans la **mention d'information** des personnes concernées et dans le **registre** du responsable de traitement ou du sous-traitant.

7. Sanctions

Le non-respect des dispositions sur les transferts de données personnelles en dehors de l'Union européenne est passible d'une amende de 20 000 000€ ou de 4% du chiffre d'affaires annuel mondial pour une entreprise.

Synthèse

Le RGPD met en place des mécanismes permettant de compenser l'insuffisance de protection des données de certains pays tiers. L'objectif est d'assurer que la « bulle de protection » suive la donnée à tout moment.

MODULE 3 : LES RESPONSABILITÉS DES ACTEURS