Atelier « RGPD, les points essentiels »

Garance Mathias et Charlène Gabillat
Mathias Avocats

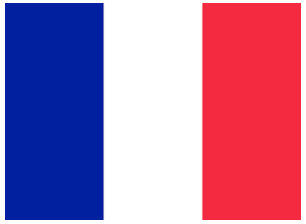
3 juillet 2019

Introduction

Quel est le nouveau cadre juridique général applicable à la protection des données en France ?

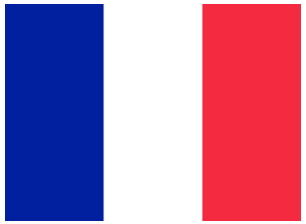
Règlement général sur la protection des données (RGPD) 2016/679 du 27 avril 2016

→ Applicable depuis le 25 mai 2018 dans tous les Etats membres de l'Union européenne



Loi n°78-17 du 6 janvier 1978 relative à la l'informatique, aux fichiers et aux libertés

→ Applicable depuis 1978, modifiée pour la dernière fois en 2018



Décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

→ Applicable depuis le 1er juin 2019

Les définitions clés

Qu'est-ce qu'une donnée à caractère personnel ?

« *Toute information se rapportant à une* ***personne physique identifiée ou identifiable****, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » (RGPD, article 4, 1)).

Que retenir ?

- ✓ La notion de « donnée à caractère personnel » est large.
- ✓ Une personne peut être directement identifiée par exemple par son nom et son prénom.
- ✓ Une personne peut être identifiable par exemple au moyen d'un identifiant, d'un numéro, de ses habitudes de vie, de ses préférences ou encore de caractéristiques qui lui sont propres (numéro de matricule, adresse électronique, numéro de sécurité sociale, numéro de téléphone, voix, image, pratiques culturelles, activités sportives/loisirs, etc.).

Qu’est-ce qu’un traitement de données à caractère personnel ?

« ***Toute opération ou tout 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* » (RGPD, article 4, 2)).

Que retenir ?

- ✓ La notion de traitement est large.
- ✓ Un traitement de données à caractère personnel n’est pas nécessairement automatisé : les fichiers au format papier sont également concernés.
- ✓ Un fichier ne contenant que des coordonnées relatives à des personnes morales de droit privé ou de droit public (dénomination sociale, adresse du siège social, numéro de téléphone du standard, adresse électronique générique de contact de type « entité@email.fr ») ne constitue pas un traitement de données à caractère personnel.

Les principaux acteurs de la protection des données

Qu’est-ce qu’un responsable du traitement ?

« *La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres,* ***détermine les finalités et les moyens du traitement*** » (RGPD, Article 4, 7)).

Que retenir ?

- ✓ Le responsable du traitement des données détermine les finalités (**objectifs du traitement**) et les moyens du traitement des données à caractère personnel.
  - ✓ **Finalité(s)** : objectif(s) poursuivi(s) par l’utilisation des données à caractère personnel.
  - ✓ **Moyens** : moyens techniques et organisationnels du traitement des données (Exemples : matériels informatiques, logiciels, typologie des données à collecter, définition de la durée de conservation, autorisation d’accès aux données, modalités de collecte des données (formulaires, etc.), choix d’une solution proposée par un éditeur, etc.).

Qu’est-ce qu’un responsable conjoint du traitement ?

« *1. Lorsque* ***deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement****, ils sont les responsables conjoints du traitement.* [Ils] *définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du* [RGPD]*, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14,* ***par voie d'accord entre eux****, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.* » (RGPD, article 26, 1.).

Que retenir ?

- ✓ La notion de responsabilité conjointe de traitement existait antérieurement à l’entrée en application du RGPD. Toutefois, elle n’avait pas été transposée en droit français.

  ➔ **Notion nouvelle en droit français**

- ✓ Un accord doit être conclu entre les responsables conjoints.

Qu’est-ce qu’un sous-traitant ?

« *La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel* ***pour le compte*** *du responsable du traitement* » (Article 4, 8° du RGPD).

Que retenir ?

- ✓ Le sous-traitant traite les données à caractère personnel uniquement pour le compte du responsable du traitement.
- ✓ Le RGPD impose directement des obligations au sous-traitant (désignation d’un DPO dans certains cas, obligation d’assurer la sécurité et la confidentialité des données, tenue de registres).
- ✓ Les obligations du sous-traitant et le traitement qui lui est confié doivent être définis dans le contrat qui le lie au responsable du traitement.
- ✓ Exemples de sous-traitants : prestataire assurant la maintenance du site internet, hébergeur, etc.

Références principales sur les notions de responsable du traitement et de sous-traitant

- ✓ **Groupe de travail « Article 29 » sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant » adopté le 16 février 2010** :

  - ✓ Le responsable du traitement définit la finalité et les moyens essentiels du traitement (données à traiter, durées de conservation, destinataires des données, etc.).
  - ✓ Le sous-traitant peut participer au choix des moyens techniques et organisationnels (matériel informatique ou logiciel utilisé).

- ✓ **Commission nationale de l'informatique et des libertés, Délibération de la formation restreinte n° SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire** :

  - ✓ La rédaction de plusieurs documents clés (dont des directives relatives à la gestion des données personnelles collectées), la réalisation de la formation ou encore la signature des contrats avec plusieurs sociétés tierces fournissant des outils essentiels au fonctionnement du traitement sont autant d'éléments qui témoignent de la qualité de responsable du traitement.
  - ✓ *La gestion des conséquences de la violation de données n'est pas une simple question technique ou d'organisation qui peut entièrement relever de la marge de manœuvre dont dispose un sous-traitant. Au contraire, la gestion d'une violation de données est une question attachée à un élément essentiel d'un moyen de traitement, dont le responsable de traitement ne peut être dessaisi.*
  - ✓ Même en présence d'un contrat de sous-traitance de traitement, la formation restreinte de la Commission nationale de l'informatique et des libertés a retenu que les sociétés de transport étaient responsables conjoints de traitement.

Références principales sur les notions de responsables conjoints

- ✓ **Groupe de travail « Article 29 » sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant » adopté le 16 février 2010**.

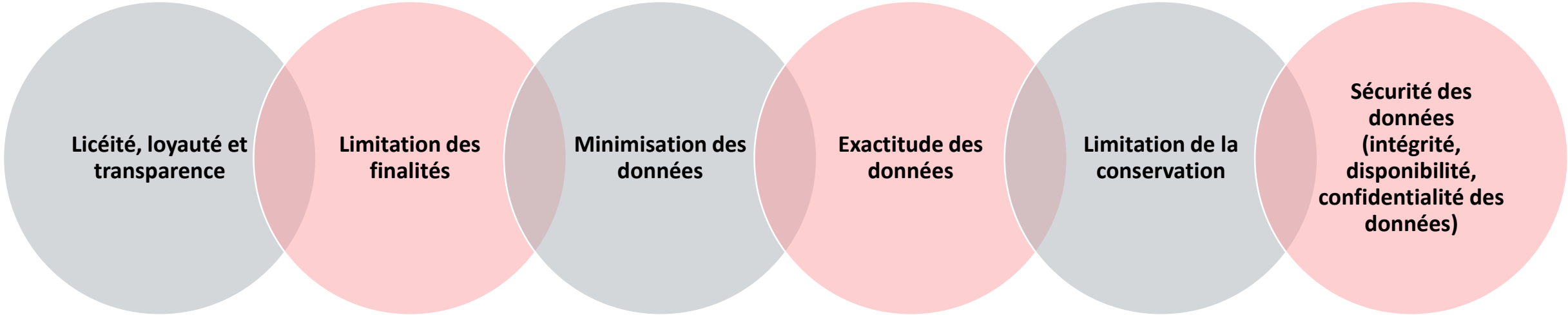
- ✓ **CJUE, Aff. C-210/16 (Wirtschaftsakademie), 5 juin 2018**

  - ✓ L'administrateur d'une page fan hébergée sur Facebook, par la création d'une telle page, offre à Facebook la possibilité de placer des cookies sur l'ordinateur ou sur tout autre appareil de la personne ayant visité sa page fan.
  - ✓ L'administrateur d'une page fan hébergée sur Facebook réalise une action de paramétrage en fonction de certains critères (audience cible, objectifs de gestion ou de promotion de ses activités), définit les critères à partir desquels les statistiques doivent être établies, la nature des données traitées (données démographiques, données relative au style de vie, centres d'intérêt, données relatives aux achats/comportement d'achat…) et les catégories de personnes concernées.

- ✓ **CJUE, Aff. C-25/17, 10 juillet 2018**

  - ✓ La notion de responsable du traitement peut concerner plusieurs acteurs participant au traitement, chacun d'entre eux devant alors être soumis aux dispositions applicables en matière de protection des données.
  - ✓ L'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente, pour un même traitement de données à caractère personnel, des différents acteurs.
  - ✓ La responsabilité conjointe de plusieurs acteurs pour un même traitement, en vertu de cette disposition, ne présuppose pas que chacun d'eux ait accès aux données à caractère personnel concernées.

Les principes clés de la protection des données


Licéité, loyauté et transparence
Limitation des finalités
Minimisation des données
Exactitude des données
Limitation de la conservation
Sécurité des données (intégrité, disponibilité, confidentialité des données)

Licéité du traitement

- ✓ Tout traitement **doit** avoir une base juridique. Ce n'est pas une nouveauté. Il est donc nécessaire de définir, pour chaque projet informatique impliquant des données à caractère personnel, la ou les bases.

- ✓ Les bases juridiques sont **énumérées par le RGPD**.

« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

*a) la **personne concernée a consenti** au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;*
*b) le traitement est **nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles** prises à la demande de celle-ci ;*
*c) le **traitement est nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis ;*
*d) le **traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique** ;*
*e) le **traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi** le responsable du traitement ;*
*f) le **traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers**, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ».*

Loyauté et la transparence du traitement

Le responsable du traitement doit traiter les données de manière loyale et transparente

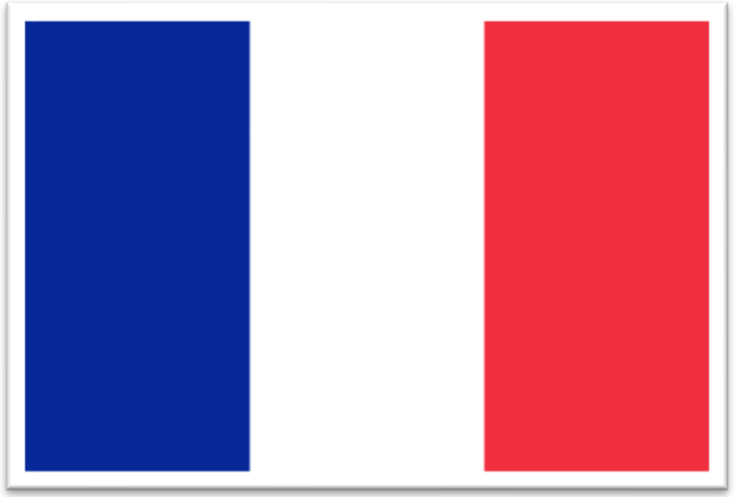
Ex. : Il ne peut y avoir de collecte de données à l'insu des personnes.

Le respect de ce principe implique qu'un traitement de données ne puisse être effectué qu'après une **information complète sur le traitement**, accessible et formulée en des termes clairs et simples.

Ex: mentions sur les formulaires, clause dans les documents contractuels, politique de protection des données en ligne…

Il convient de déterminer avec les équipes opérationnelles comment l'information pourra être délivrée dans le cadre de tout projet.

Licéité, loyauté et transparence du traitement : illustrations pratiques



Sanction prononcée par la Commission nationale de l'informatique et des libertés le 21 janvier 2019 (Délibération n°SAN-2019-001 du 21 janvier 2019) :

- **Violation du principe de transparence et manquement à l'obligation d'information** : insuffisance de l'information délivrée par la société, qui renvoyait à une politique de confidentialité complexe portant sur un grand nombre de traitements sans permettre à l'utilisateur d'identifier facilement les informations pertinentes.
- **Manquement à l'obligation de disposer d'une base légale pour le traitement** : le consentement des utilisateurs aux traitements de ciblage publicitaire n'était pas valablement recueilli (cases pré-cochées, parcours utilisateur trop complexe).
- Nature de la sanction : sanction pécuniaire de **50 millions d'euros rendue publique pendant 2 ans**.
- La société a annoncé interjeter appel de la décision.

Licéité, loyauté et transparence du traitement : illustrations pratiques

Sanction prononcée par l'autorité polonaise de protection des données en mars 2019 à l'encontre d'une société :

La société sanctionnée traitait des données issues de l'équivalent polonais du RCS (le CEiDG). Toutefois, elle n'informait du traitement que les personnes concernées pour lesquelles elle disposait d'une adresse de courrier électronique. Elle justifiait cette absence d'information par un coût important généré par le fait d'informer les autres personnes concernées.

- **Manquement à l'obligation d'information** : l'autorité polonaise estime que **les coûts n'étaient pas suffisamment élevés pour justifier de ne pas informer les personnes pour lesquelles la société disposait d'une adresse postale et/ou du numéro de téléphone**.
- Pour fixer le montant de l'amende, l'autorité souligne que **la société avait conscience de ses obligations et que son manquement était intentionnel**. De plus, elle n'a pris aucune mesure pour mettre fin à la violation avant la sanction et n'a pas indiqué vouloir le faire.
- Nature de la sanction : sanction pécuniaire d'**environ 220 000 euros.**

Limitation des finalités

- ✓ Un traitement de données doit avoir **un objectif ou plusieurs objectifs (finalité(s))**.
- ✓ **Ces finalités doivent être définies** clairement et portées à la connaissance des personnes concernées.
- ✓ Il n'est pas possible de collecter des données à caractère personnel au cas où elles seraient utiles un jour.

Limitation des finalités : illustration pratique

Sanction prononcée le 28 mai 2019 par l'Autorité de Protection des Données (APD) à l'encontre d'un bourgmestre (détenteur du pouvoir exécutif au niveau communal) :

- Les adresses email des personnes concernées avaient été obtenues lors d'un échange par voie électronique avec l'architecte de la commune au sujet d'une modification de lotissement. La veille des élections communales, le bourgmestre a utilisé les adresses email de ces personnes afin de leur envoyer un « message électoral ».
- L'APD a jugé que la réutilisation de données obtenues dans le cadre d'un projet urbanistique à des fins de campagne électorale constituait un **manquement au principe de limitation des finalités du traitement**.
- Pour fixer le montant de l'amende, l'APD a pris en compte le nombre limité des personnes touchées ainsi que la nature, la gravité et la durée de l'infraction
- Nature de la sanction : sanction pécuniaire de **2 000 euros.**

Principe de minimisation des données

✓ Les informations traitées doivent être **strictement nécessaires au regard de la finalité du traitement**.

Principe d'exactitude des données

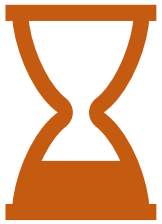
✓ Seules les **données adéquates, pertinentes et non excessives** pour la réalisation de la finalité sont collectées.

Minimisation des données : illustration pratique

Sanction prononcée par la Commission nationale de l'informatique et des libertés à l'encontre d'une société de traduction le 13 juin 2019 (Délibération n°SAN-2019-006) :

- **Manquement au principe de minimisation des données** : l'une des caméras filmait en continu les postes de travail de 6 salariés.
- **Manquement au principe de limitation de la durée de conservation** : les images étaient conservées pour une durée excessive (régularisé suite à une mise en demeure le 26 juillet 2018).
- **Manquement à l'obligation d'informer les personnes concernées** : les salariés n'étaient pas informés de l'existence du dispositif.
- **Manquement à l'obligation d'assurer la sécurité et la confidentialité des données** : absence de mot de passe sur les postes de travail, boite de messagerie électronique commune aux collaborateur sans mesure de traçabilité.
- Nature de la sanction :
  - sanction pécuniaire de **20 000 euros**,
  - **injonction** d'assurer la traçabilité des accès à la messagerie professionnelle partagée dans un délai de 2 mois, **assortie d'une astreinte de 200 euros par jour de retard** passé ce délai,
  - Publicité de la sanction pendant un an.

Conservation limitée des données



CE QUE DIT LE RGPD

➔Les données à caractère personnel **doivent être conservées** sous une forme permettant l'identification des personnes concernées **pendant une durée n'excédant pas celle nécessaire au regard des finalités** pour lesquelles elles sont traitées.

➔**Conservation limitée** des données à caractère personnel.

➔**Définition** des durées de conservation **selon les finalités poursuivies.**

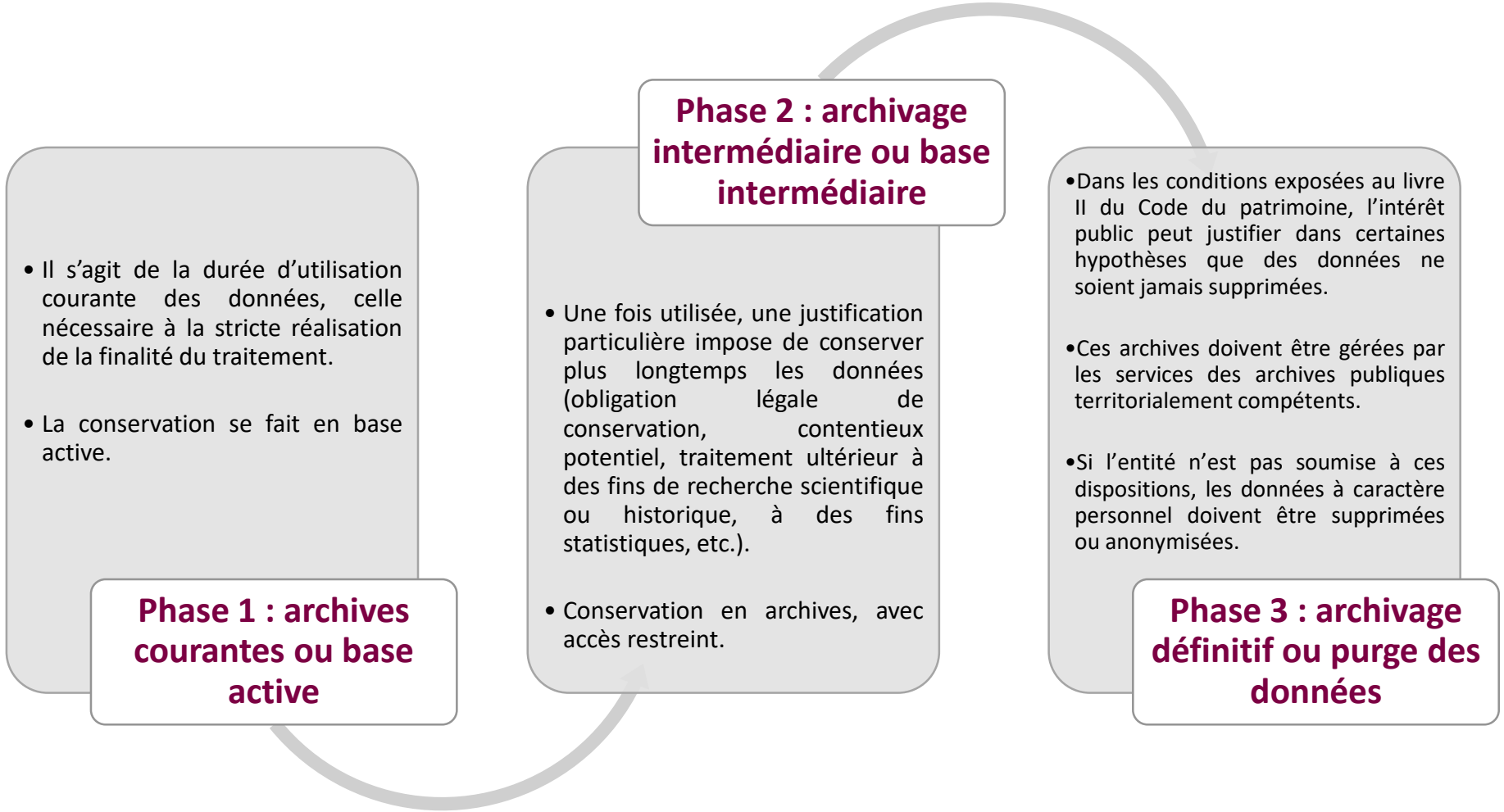
CE QUE NE DIT PAS LE RGPD

➔Le RGPD **ne définit pas les durées de conservation** des données à caractère personnel à appliquer.

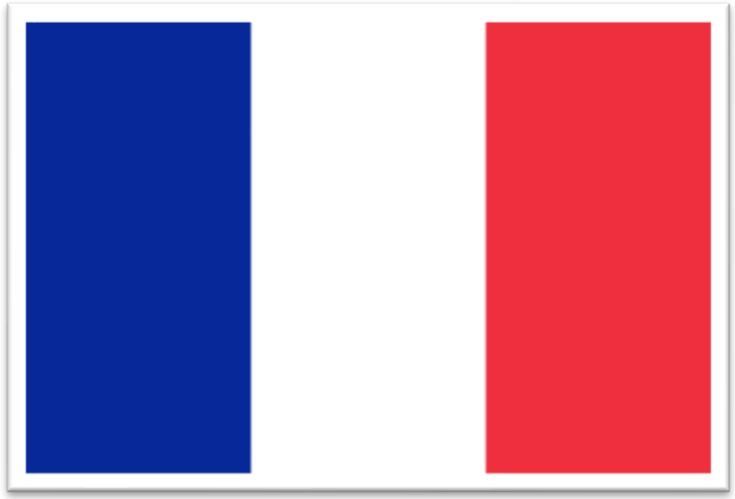
➔**Les durées de conservation sont définies par le responsable du traitement** (sauf durées résultant de textes législatifs imposant une durée de conservation).

Conservation limitée des données

Cycle de vie des données identifié par la Commission nationale de l'informatique et des libertés



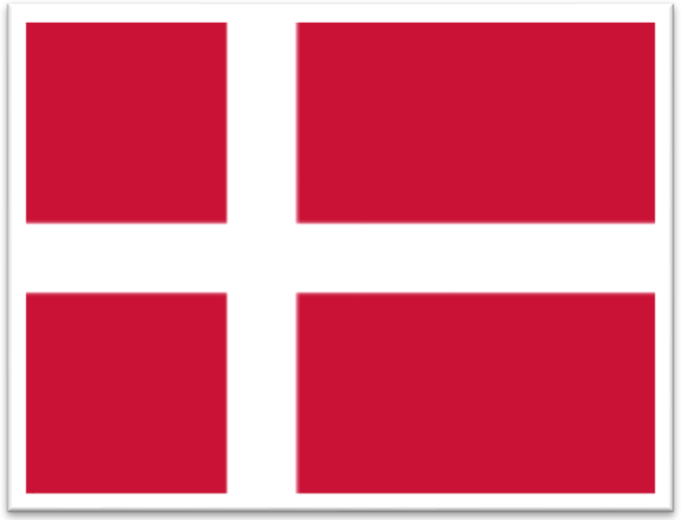
Conservation limitée des données : illustration pratique



Sanction prononcée par la Commission nationale de l'informatique et des libertés à l'encontre d'une société du secteur de l'immobilier le 28 mai 2019 (Délibération n°SAN-2019-005 du 28 mai 2019) :

- **Manquement au principe de limitation de la durée de conservation** :
  - Conservation en base active des documents relatifs aux candidats n'ayant pas accédé à la location pour une durée excédant celle nécessaire au regard de la finalité principale de la collecte (attribution d'un logement).
  - Absence d'archivage intermédiaire ou de séparation logique dans la base active des données nécessaires à la gestion des demandes du Défenseur des droits ou à la défense de ses intérêts dans le cadre d'un précontentieux ou contentieux.
- **Manquement à l'obligation d'assurer la sécurité et la confidentialité des données** : absence de mise en place d'une procédure d'authentification des utilisateurs accédant aux documents.
- Pour calculer le montant, la Cnil déclare avoir pris en compte : la gravité du manquement, le manque de diligence de la société dans la correction de la vulnérabilité, le fait que certaines des données avaient un « caractère intime », ainsi que la situation financière de la société.
- Nature de la sanction : sanction pécuniaire de **400 000 euros rendue publique pendant 2 ans**.

Conservation limitée des données : illustration pratique



Sanction recommandée par l'autorité danoise en mars 2019 à l'encontre d'une société de taxis :

- L'autorité danoise ne peut pas directement prononcer d'amende administrative. Le prononcé revient aux tribunaux.

- **Manquement au principe de minimisation des données et à la conservation limitée des données** :
  - La société déclarait « anonymiser » les données qu'elle collectait sur ses clients au bout de deux ans. En réalité, elle se contentait de supprimer les noms et prénoms des clients. En revanche, elle conservait de nombreuses données telles que leurs données de géolocalisation ou leur numéro de téléphone. Ces données étaient conservées pendant trois ans à compter de « l'anonymisation ».
  - **La société n'a pas été en mesure de démonter qu'elle supprimait les données selon les durées indiquées car elle n'avait mis en place ni mesure de traçabilité, ni mécanismes de purge automatique**.
- Nature de la sanction recommandée : sanction pécuniaire d'**environ 161.000 euros**.

Sécurité des données

Le responsable du traitement **et** le sous-traitant doivent assurer la sécurité des données à caractère personnel.

Les mesures de sécurité informatiques et physiques doivent être adaptées aux risques (nature des données, volume de données traitées, nature des personnes concernées, etc.).

Le RGPD ne définit pas les mesures de sécurité à mettre en œuvre.

Les mesures de sécurité doivent être documentées et matérialisées dans le système d'information.

Sécurité des données : illustrations pratiques

Sanction prononcée le 11 octobre 2018 par la CNPD à l'encontre d'un hôpital :

- **Manquement à l'obligation d'assurer la sécurité des données** :
  - des personnels non autorisés ont pu accéder à des données relatives aux patients.
  - le personnel disposant d'un accès à la base de données de l'hôpital avait accès aux données de tous les patients (absence de niveaux d'habilitations distincts) et pouvait accéder aux données de patients d'autres hôpitaux, sans justification.
  - Absence de surveillance continue du système d'information pour veiller à l'intégrité et de la confidentialité des données.
- Nature de la sanction : sanction pécuniaire de **400.000 euros**.

Sécurité des données : illustrations pratiques

Sanction prononcée le 21 novembre 2018 par la LfDI à l'encontre d'un réseau social :

- Manquement à l'obligation d'assurer la sécurité des données : Le site avait subi une cyberattaque en septembre 2018. Les mots de passe des utilisateurs étaient conservés en clair dans la base de données copiée par les attaquants.
- La LfDI a toutefois déclaré avoir pris en compte la « *coopération exemplaire* » dont a fait preuve la société lors de la procédure. Celle-ci a notifié sans délai l'autorité et les personnes concernées et a rapidement mis en œuvre d'importants moyens pour se mettre en conformité.
- Nature de la sanction : sanction pécuniaire de **20.000 euros**.

Sécurité des données : illustrations pratiques

Sanction prononcée le 4 avril 2019 par l'autorité de contrôle italienne à l'encontre d'une association (mouvement politique) :

- Les sites de l'association avaient fait l'objet d'un premier contrôle à l'été 2017. De nombreux défauts de sécurité avaient été révélés.

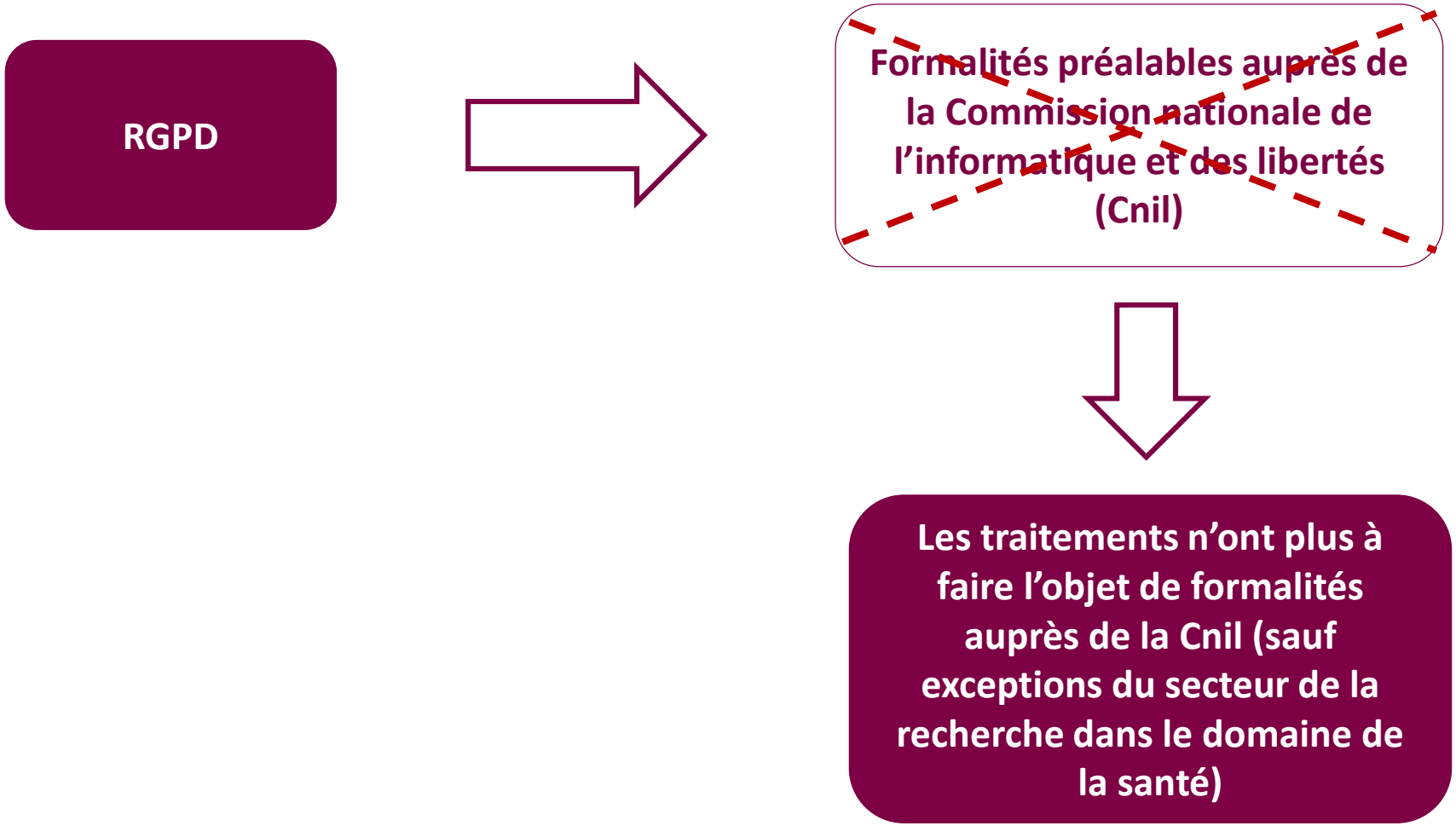
- **Manquement à l'obligation d'assurer la sécurité des données** :

  - absence de traçabilité des accès à la base de données,
  - partage d'identifiants entre plusieurs personnes en charge de l'une des plateformes qui avaient été contrôlées,
  - absence de définition de profils d'habilitation pour restreindre l'accès aux données.

- Nature de la sanction : sanction pécuniaire de **50 000 euros**.

Les principaux changements liés à l'application du RGPD

La suppression des formalités préalables



La démonstration de la conformité

En contrepartie de la disparition de l'accomplissement de démarches administratives auprès de la Cnil, chaque entité doit être en mesure de démontrer à tout moment le respect des règles relatives à la protection des données.

=

***ACCOUNTABILITY* OU PRINCIPE DE RESPONSABILITÉ**

L’élaboration d’un registre des traitements

- ✓ **La tenue du registre des activités de traitement constitue** :
  - ✓ **Une obligation tant pour le responsable de traitement, que pour le sous-traitant.**
  - ✓ Un **document susceptible d’être demandé par la Cnil en cas de contrôle**. Le registre est également un outil interne permettant d’avoir une vision des traitements mis en œuvre dans le cadre d’une démarche de responsabilisation (« *accountability* »).

L’élaboration d’un registre des traitements

- ✓ Le registre des activités de traitement doit recenser **l’ensemble des traitements de données à caractère personnel mis en œuvre par votre entité.**

- ✓ Pour chaque traitement, **le registre devra contenir des informations suivantes** :

✓ **Qui ?** Identification du responsable du traitement, Coordonnées du DPO, les catégories de personnes concernées

✓ **Pourquoi ?** Les finalités du traitement

✓ **Quoi ?** Les catégories de données à caractère personnel

✓ **Communication des données à qui ?** Les catégories de destinataires (destinataires internes, destinataires externes à l’entité (sous-traitants, partenaires))

✓ **Jusqu’à quand ?** Les durées de conservation des données (base active, base intermédiaire, purge/anonymisation)

✓ **Quelle protection ?** La description générale des mesures de sécurité

✓ **Où ?** Les transferts de données de données hors UE (le cas échéant)

- ✓ L’objectif est de **disposer d’une vue d’ensemble des traitements** mis en œuvre par votre entité.

La notification et la communication des violations de données

« *Violation de la sécurité entraînant, de manière accidentelle ou illicite, la* ***destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel*** *transmises, conservées ou traitées d'une autre manière, ou* ***l'accès non autorisé à de telles données****.* » (Article 4, 12) RGPD).

En bref

- ✓ Tout incident de sécurité,
- ✓ d'origine malveillante ou non,
- ✓ se produisant de manière intentionnelle ou non,
- ✓ ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données à caractère personnel.

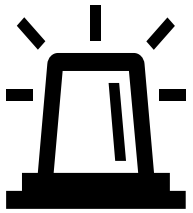
=

VIOLATION DE DONNEES

La notification et la communication des violations de données

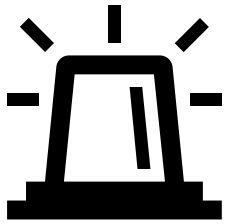
Catégories de violation de données

La notification et la communication des violations de données



QUE FAIRE SUITE A UNE VIOLATION DE DONNEES ?

- ✓ Documenter la violation
- ✓ **Notifier la violation qui génère un risque à la Commission nationale de l'informatique et des libertés 72 heures** au plus tard après en avoir pris connaissance



La notification et la communication des violations de données

En cas de risque élevé pour les personnes concernées

Information des personnes concernées dans les meilleurs délais sauf si :

- ✓ Les données à caractère personnel impliquées dans la violation de données étaient protégées de telle sorte qu'elles sont incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès

  Ex.: chiffrement des données et non compromission de la clé

- ✓ Le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes n'est plus susceptible de se matérialiser

  Ex.: mots de passe d'employés ayant accès à une base de données sensibles ont été subtilisés, mais n'ont pas été utilisés et ont été réinitialisés.

- ✓ La communication de la violation aux personnes concernées exigerait des efforts disproportionnés

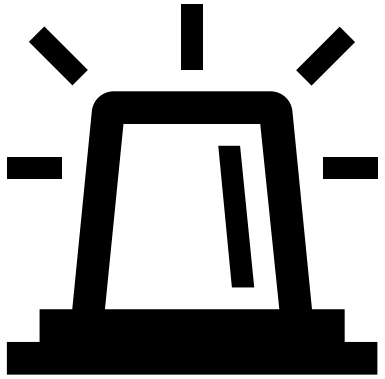
  Ex.: Le responsable du traitement ne dispose d'aucun élément permettant de contacter les personnes concernées. **Toutefois**, une communication publique, ou une mesure similaire permettant aux personnes concernées d'être informées de manière aussi efficace, doit être réalisée.

La notification et la communication des violations de données

➔ Dans le cadre de la contractualisation avec les prestataires, négociez des délais de transmission des informations utiles.

➔ En cas de violation de données, ne pas hésiter à solliciter toutes informations utiles du prestataire. Il doit collaborer.

➔ Identifier les éventuels manquements contractuels.



La notification et la communication des violations de données : illustrations pratiques

Avertissement prononcé le 9 novembre 2018 par l'autorité hellénique à l'encontre d'un établissement bancaire :

- L'établissement bancaire a communiqué par erreur des données à caractère personnel de certains de ses clients à d'autres.
- Toutefois, il a notifié cette violation à l'autorité de contrôle et aux personnes cinq jours après en avoir eu connaissance.
- Le délai étant de 72h maximum, l'autorité de contrôle a prononcé un avertissement à l'encontre du responsable du traitement.

La notification et la communication des violations de données : illustrations pratiques

Sanction prononcée le 16 mai 2019 à l'encontre d'un prestataire de paiement électronique :

- Les données à caractère personnel relatives aux clients d'un prestataire de paiement électronique ont été rendues publiques sur un site internet pendant au moins deux jours, en juillet 2018.
- L'autorité de contrôle a constaté l'absence de mesures de sécurité adéquates et un manquement au principe de minimisation des données.
- La **société n'a notifié le manquement ni à l'autorité de contrôle, ni aux personnes concernées**.
- Nature de la sanction : sanction pécuniaire d'un montant de **61 500 euros**.

Le renforcement des droits des personnes concernées

Focus sur la vérification de l'identité du demandeur : impacts majeurs du RGPD sur le décret d'application de la loi française

- ✓ La réglementation française est plus précise que le RGPD sur les modalités de contrôle de l'identité de la personne concernée. Le décret d'application n°2019-536 du 29 mai 2019 précise que (article 77) :
  - ✓ Lorsque la personne concernée forme une demande, y compris par voie électronique, « *elle justifie de son identité* ***par tout moyen*** ».
  - ✓ « *Lorsque le responsable du traitement ou le sous-traitant a des* ***doutes raisonnables*** *quant à l'identité de cette personne, il* ***peut demander des informations supplémentaires*** *apparaissant nécessaires, y compris,* ***lorsque la situation l'exige****, la photocopie d'un titre d'identité portant la signature du titulaire* ».

➔ La fourniture d'une copie de pièce d'identité n'est pas obligatoire et sa demande par le responsable du traitement ne doit pas être systématique.

Le renforcement des droits des personnes concernées

	Définition	Conséquences
Droit à l'information (Articles 12 à 14 du RGPD)	Toute personne concernée dont les données à caractère personnel ont vocation à faire l'objet d'un traitement doit être **informée de l'identité du responsable du traitement, des caractéristiques di traitement (finalités, destinataires, durées de conservation, base légale, etc.) ainsi que de ses droits et des modalités d'exercice de ces derniers.**	Veiller à ce que l'information des personnes soit réalisée pour tout traitement mis en œuvre (mentions d'information , charte ou politique de protection des données, panneaux, affiches, clause contractuelle, etc.).
Droit d'accès (Article 15 du RGPD)	Toute personne concernée doit pouvoir obtenir la **confirmation que des données la concernant font l'objet d'un traitement** et, si tel est le cas, en **obtenir une copie**. Elle a également droit **d'obtenir communication des caractéristiques des traitements** dont ses données font l'objet.	Être en mesure **d'identifier les caractéristiques des traitements** dont les données du demandeur font l'objet (outil utile : registre des activités de traitement). Être en mesure de **fournir une copie des données** au demandeur.

Le renforcement des droits des personnes concernées : illustration pratique

Avertissement prononcé à l'encontre d'une société d'assurance par l'autorité tchèque de protection des données :

- **Non-respect du droit d'accès** : un client a souhaité exercer son droit d'accès par courrier électronique. La société a refusé sa demande au motif que ce moyen de communication ne permettait pas de s'assurer de l'identité du client. Elle lui a demandé de fournir une pièce d'identité comportant sa signature certifiée avant de traiter sa demande.
- L'autorité a jugé que l'exercice du droit d'accès par la personne concernée a été soumis à une **condition injustifiée**.
- L'autorité n'a pas prononcé de sanction pécuniaire au motif que la société a immédiatement remédié à son manquement en faisant droit à la demande de la personne concernée.

Le renforcement des droits des personnes concernées

	Définition	Conséquences pour l'organisme
Droit d'opposition (Article 21 du RGPD)	Toute personne concernée peut s'opposer, **pour des raisons tenant à sa situation particulière**, à un traitement de données la concernant dont la base légale est l'exercice d'une mission d'intérêt public (article 6 1. e)) ou l'intérêt légitime du responsable du traitement ou d'un tiers (article 6 1. f)). Spécificité en matière de prospection commerciale : droit d'opposition à tout moment, sans justification.	Opposition à la prospection commerciale : **lien de désabonnement** dans chaque envoi, fonctionnalité « Stop SMS », etc. Opposition hors prospection commerciale : le responsable du traitement peut ne pas faire droit à la demande dans certaines hypothèses, notamment : • **Motifs légitimes et impérieux** pour le traitement qui prévalent sur les intérêts, droits et libertés de la personne, • Traitement nécessaire à la **constatation, l'exercice ou la défense de droit en justice** ; • Le traitement **n'a pas pour fondement une mission d'intérêt public ou les fins d'intérêt légitime** (attention, si le fondement est le consentement la personne dispose du droit de retirer son consentement à tout moment) ; • Pour les traitements à des **fins de recherches scientifiques ou historiques ou à des fins statistiques** en application de l'article 89 du RGPD, si le traitement est nécessaire à l'exécution d'une mission d'intérêt public.
Droit de rectification (Article 16 du RGPD)	Toute personne concernée a le droit d'obtenir la **rectification des données la concernant qui sont inexactes**. Elle a également le droit d'obtenir que des **données incomplètes soit complétées**.	Si applicable, **notifier** à tout destinataire la rectification réalisée. **Répercuter** la modification dans toutes ses bases de données impactées.
Droit à la portabilité (Article 20 du RGPD)	Toute personne concernée doit pouvoir récupérer les données à caractère personnel qu'elle a fournies et qui résultent de l'utilisation des services mis à sa disposition par le responsable du traitement dans un format structuré, couramment utilisé et lisible par machine.	Identifier les données susceptibles de faire l'objet du droit à la portabilité. Identifier le format dans lequel les données sont restituées. Identifier les moyens techniques à mettre en œuvre.

Le renforcement des droits des personnes concernées

	Définition	Conséquences pour l'organisme
Droit à l'effacement (Article 17 du RGPD)	Toute personne concernée doit pouvoir obtenir l'effacement des données à caractère personnel la concernant si notamment : • Elle s'est opposée à la prospection commerciale et qu'il n'y a pas d'autres finalités pour lesquelles ses données sont traitées. • Elle a retiré son consentement au traitement de ses données et il n'y a pas d'autres bases légales au traitement. • Les données ont fait l'objet d'un traitement illicite.	L'entité **doit effacer** les données à caractère personnel du demandeur. L'entité pourrait **refuser de faire droit à la demande** notamment si : • Une obligation légale à laquelle l'organisme est soumis impose la conservation des données (ex.: conservation des pièces comptables telles les factures pendant 10 ans, règlementation relative aux essais cliniques). • Les données sont nécessaires à la défense de ses droits en justice. • Le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89 du RGPD, dans la mesure où le droit à l'effacement est susceptible de « *rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement* ».
Droit à la limitation du traitement (Article 18 du RGPD)	Toute personne concernée qui notamment conteste l'exactitude des données ou encore la licéité du traitement peut obtenir que le traitement se limite à la conservation desdites données le temps nécessaires à la réalisation de vérifications par le responsable du traitement.	Ne plus utiliser les données à caractère personnel à l'exception de leur conservation, sauf si la personne a donné son consentement à une autre finalité, ou pour la constatation, l'exercice ou la défense de droits en justice, pour la protection d'une autre personne physique ou morale, ou encore pour des motifs important d'intérêt public de l'Union ou d'un pays membre.

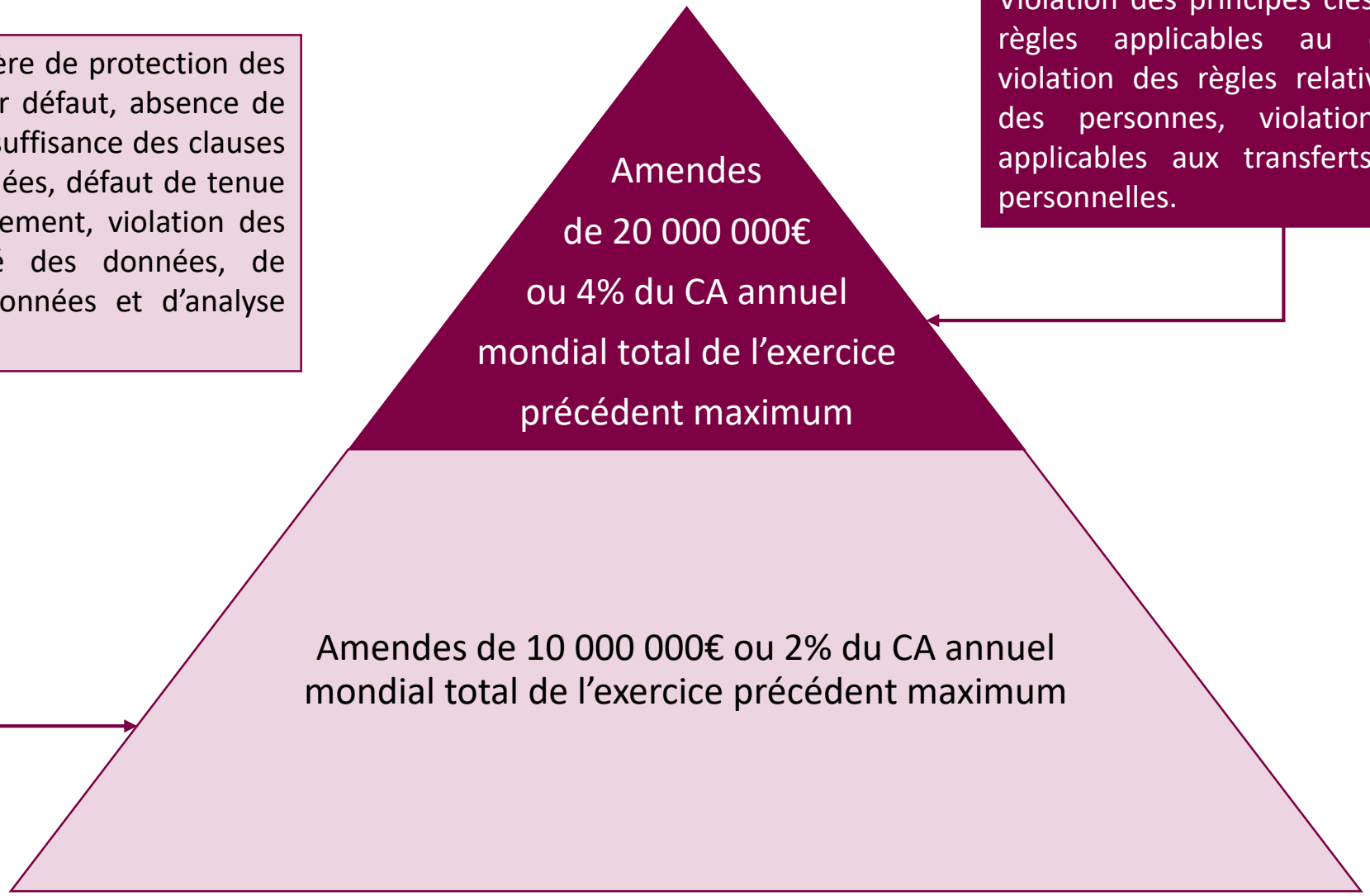
Le renforcement des droits des personnes concernées à l'échelle nationale

	Définition	Conséquences
Droit de définir des directives relatives au sort de ses données post-mortem (Article 85 de la loi n°78-17 modifiée)	Toute personne peut **définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès.** Ces directives sont générales ou particulières.	Ces directives définissent la manière dont la personne entend que soient exercés ses droits après son décès. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel. Pour les directives générales, il est prévu la création d'un registre unique amené à recueillir les références des directives générales et du tiers de confiance à qui elles sont confiées.

Le renforcement du pouvoir de sanction pécuniaire des autorités de contrôle

Violation des obligations en matière de protection des données dès la conception et par défaut, absence de contrat avec les sous-traitants, insuffisance des clauses relatives à la protection des données, défaut de tenue du registre des activités de traitement, violation des règles en matière de sécurité des données, de notification des violations de données et d'analyse d'impact.

Violation des principes clés, violation des règles applicables au consentement, violation des règles relatives aux droits des personnes, violation des règles applicables aux transferts de données personnelles.



Autres changements à ne pas oublier

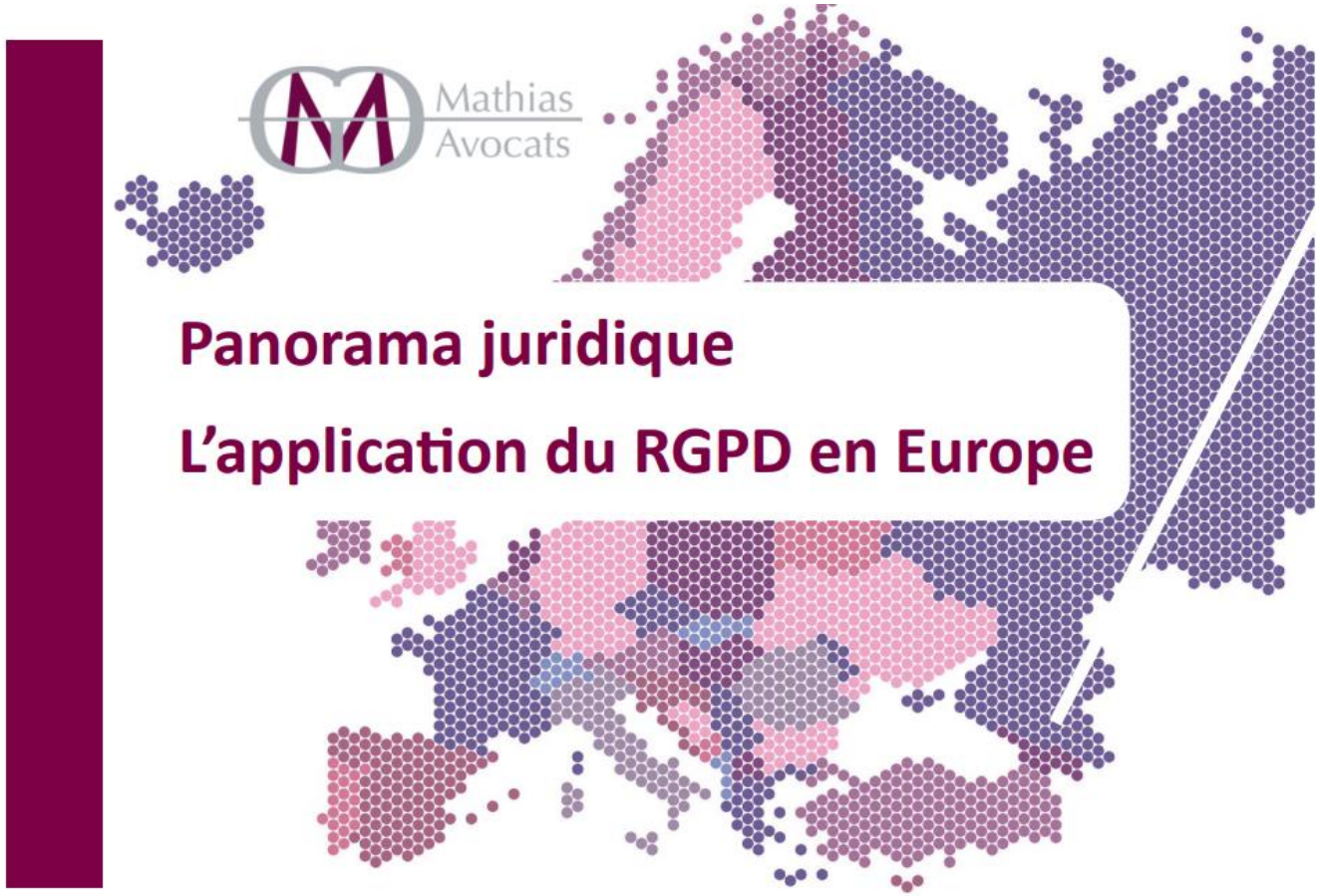
- ✓ La réalisation d’analyses d’impact sur la vie privée
- ✓ La désignation du délégué à la protection des données

Merci de votre participation

Mathias Avocats

19 rue Vernier – 75017 Paris
Tél.: 01 43 80 02 01
contact@avocats-mathias.com
www.avocats-mathias.com

Pour aller plus loin



Mathias Avocats vient de publier un panorama de décisions et sanctions prises en application du RGPD par différentes autorités de contrôle européennes.

https://www.avocats-mathias.com/telechargement-livres-blancs