La protection des données à caractère personnel

Le 12 juin 2019, Saint-Nazaire

Carole Couson-Warlop, Avocat

ARTLEX
CABINET D'AVOCATS

La protection des données à caractère personnel

1. **CONTEXTE**
2. **Champ d'application du RGPD**
3. **Principes directeurs**
4. **Obligations des responsables de traitements**
5. **Droit des personnes concernées**
6. **Transfert des données hors UE**
7. **Délégué à la protection des données**
8. **Recours de la personne concernée**
9. **Pouvoirs de la CNIL et sanctions**
10. **Bilan de la CNIL**
11. **Recommandations pour la mise en conformité**

1. CONTEXTE

➢ Etat du droit :

- ✓ **Loi n°78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés
- ✓ **Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- ✓ **Loi n°2004-801 du 6 août 2004** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- ✓ **Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016** relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46 « Règlement Général sur la protection des données », ci-après « RGPD »
- ✓ **Loi n°2016-1321 du 7 octobre 2016** pour une République numérique

- **Loi n° 2018-493 du 20 juin 2018** relative à la protection des données personnelles
- **Décret n° 2018-687 du 1er août 2018** pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- **Ordonnance n° 2018-1125 du 12 décembre 2018** prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel (qui entrera en vigueur au plus tard au 1er juin 2019)
- **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

1. CONTEXTE

- **Objectifs du RGPD**
  - ✓ Harmoniser les réglementations au sein de l'UE
  - ✓ S'adapter aux évolutions technologiques
  - ✓ Augmenter le niveau de protection
  - ✓ Protéger les droits et libertés des personnes physiques : **(Considérant 1 et 2)**
    - **Droit fondamental… mais non absolu (Considérant 4)**
  - ✓ Responsabiliser les acteurs :
    - changement de paradigme : abandon de l'approche formaliste et de l'obligation générale de notification

1. CONTEXTE

Mise en application du RGPD

- Application directe sans transposition
- Mise en application le **25 mai 2018**
- A partir de mai 2018 : nouvelles sanctions : jusqu'à **20.000.000 d'euros** ou, dans le cas d'une entreprise, jusqu'à **4 % du chiffre d'affaires annuel mondial total de l'exercice précédent**, le montant le plus élevé étant retenu
  - 99 articles et 173 considérants interprétatifs : de nouveaux droits pour les personnes concernées, de nouvelles obligations pour les responsables et les sous-traitants et surtout une nouvelle organisation pour la gestion des traitements à prévoir et à mettre en place
- Le règlement n'est pas rétroactif….mais les traitements déjà en cours d'application devront être mis en conformité **(Considérant 171)**
- Mise en conformité coûteuse et malaisée :
  - Marge d'appréciation importante laissée aux Etats membres
  - Des notions floues à préciser

1. Contexte
2. **CHAMP D'APPLICATION DU RGPD**
3. Principes directeurs
4. Obligations des responsables de traitements
5. Droit des personnes concernées
6. Transfert des données hors UE
7. Délégué à la protection des données
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

2. CHAMP D'APPLICATION DU RGPD

➢ Champ d'application matériel & notions clés

✓ Traitement de données personnelles : (Article 4 alinéa 2)

«*Toute opération ou tout ensemble d'opérations effectuées* ***<u>ou non à l'aide de procédés automatisés</u>*** *et appliquées à des données ou des ensembles de données,* ***<u>telles que</u>*** *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, diffusion ou toute autre forme de mise a disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* »

Collecte	Enregistrement	Organisation	Structuration	Conservation
Adaptation	Modification	Extraction	Consultation	Utilisation
Communication	Diffusion	Mise à disposition	Rapprochement	Interconnexion
Limitation	Effacement	Destruction		

2. CHAMP D'APPLICATION DU RGPD

- **Données à caractère personnel (Article 4 alinéa 1)**

« Toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologiques, génétique, psychique, économique, culturelle ou sociale »

- Toute information permettant d'identifier **directement ou indirectement** une **personne physique** :
  - Directement : nom, prénom, photographie, etc.
  - Indirectement : numéro de téléphone, numéro de carte bancaire, adresse IP, cookies, données de géolocalisation, habitudes de consommation, opinion, état de santé, etc.
- Une donnée pseudonymisée est une donnée personnelles ≠ Une donnée anonymisée n'est pas une donnée personnelle

2. CHAMP D'APPLICATION DU RGPD

- **Données sensibles** : données faisant apparaître directement ou indirectement : **(Article 9)**
  - Les origines raciales ou ethniques
  - Les opinions politiques, philosophies ou religieuses
  - L'appartenance syndicale des personnes
  - Les données génétiques et biométriques
  - Les données de santé
  - Les données relatives à la vie sexuelle et à l'orientation sexuelle

- Traitement de ces données sensibles est en principe **interdit** – mais exceptions prévues **(Article 9)**
- **Nouvelles exceptions** ajoutées en droit français **(Article 44 de la LIL réécrite par l'ordonnance)**
- Particularités en droit français relatives aux données comportant **le NIR (Article 30 de la LIL réécrite par l'ordonnance)**

2. CHAMP D'APPLICATION DU RGPD

- **Responsable :** La personne physique ou morale, l'autorité publique, le service ou l'organisme qui détermine **les finalités et les moyens du traitement**
  - Nouveauté : possibilité de responsables conjoints du traitement : « co-responsable » **(Article 26)**

- **Sous-traitant :** La personne physique ou morale, l'autorité publique, le service ou l'organisme qui traite des données à caractère personnel **pour le compte** du responsable du traitement, **sous son autorité et sur ses instructions**.

- **Destinataires** : toute personne qui reçoit communication des données qu'il s'agisse ou non d'un tiers

- **Fichier** : Tout ensemble structuré de données accessibles selon des critères déterminées, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique

- **Personnes concernées** : Personne à laquelle se rapportent les données qui font l'objet du traitement

- Nouvelles définitions: consentement, pseudonymisation, violation de données, profilage, établissement principal, règles d'entreprises contraignantes, etc.)

2. CHAMP D'APPLICATION DU RGPD

- ✓ **Exclusions : (Article 2)**
  - Les traitements des données des **personnes morales**
  - Les traitements des données effectuées dans le cadre d'une activité qui ne relève **pas du champ d'application du droit de l'Union**
  - Les traitements de données effectués par les Etats membres dans le cadre d'activités qui relèvent de la **politique étrangère et de sécurité commune**
  - Les traitements effectués par une personne physique dans le cadre d'une **activité strictement personnelle ou domestique**
  - Les traitements de données effectués par les autorités compétentes à des fins de **prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales**, y compris la protection contre des menaces pour la sécurité juridique et la prévention de telles menaces

2. CHAMP D'APPLICATION DU RGPD

➢ Champ d'application territorial (Article 3)

- ✓ **Responsable (ou sous-traitant) du traitement est établi en UE :** « *traitement des données effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union,* ***que le traitement ait lieu ou non dans l'UE*** »

- ✓ **Traitement de données relatives à des personnes qui se trouvent sur le territoire de l'UE, par un responsable ou un sous-traitant du traitement non établi dans l'UE,** lorsque les activités de traitement sont liées:
  - **À l'offre de biens ou de services** à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ;
  - **Au suivi du comportement de ces personnes**, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union

- ✓ Traitement des données effectué par un responsable du traitement qui n'est pas établi dans l'UE mais dans un lieu où **la législation nationale d'un Etat membre s'applique en vertu du droit international public**

1. Contexte
2. Champ d'application du RGPD
3. **PRINCIPES DIRECTEURS**
4. Obligations des responsables de traitements
5. Droit des personnes concernées
6. Transfert des données hors UE
7. Délégué à la protection des données
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

3. PRINCIPES DIRECTEURS

Principe de licéité
Principe de loyauté et de transparence
Principe de finalité
Principe de proportionnalité
Principe d'exactitude
Principe de sécurité

3. PRINCIPES DIRECTEURS

Principe de licéité

Le traitement n'est licite que dans l'un des cas suivants :

- **Consentement donné** : Nouvelle définition **(Article 4 et Considérant 42)**
  - Consentement **exprès et explicite**
  - Consentement **éclairé** après avoir obtenu toutes les informations nécessaires listées (voir droit à l'information de la personne concernée)
  - Consentement par un **acte positif clair** (case à cocher, signature, etc.)
  - Le responsable doit pouvoir prouver qu'il a obtenu le consentement
  - Consentements spécifiques nécessaires dans certains cas
  - Consentement du mineur libre et éclairé fixé à **15 ans** **(Article 45 de la LIL réécrite par l'ordonnance)**
  - Principe du **double consentement** pour l'enfant mineur **(Article 45 la LIL réécrite par l'ordonnance)**
- **Mesures contractuelles**
- **Obligation légale**
- **Sauvegarde des intérêts vitaux**
- **Mission d'intérêt public**
- **Intérêt légitime du responsable du traitement**

3. PRINCIPES DIRECTEURS

- **Principe de loyauté et de transparence**
  - ✓ Les données doivent être collectées de manière loyale et en toute transparence

  → Information renforcée des personnes concernées

- **Principe de finalité**
  - ✓ Les données doivent être collectées pour des finalités **déterminées, explicites et légitimes** et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités

- **Principe de proportionnalité**
  - ✓ Minimisation des données : Les données collectées doivent être **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées
  - ✓ Limitation de la durée de conservation des données

- **Principe d'exactitude**
  - ✓ Les données collectées doivent être **exactes et tenues à jour**, si nécessaire

- **Principe de sécurité**
  - ✓ Toutes les mesures doivent être prises pour assurer la sécurité des traitements

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS
5. Droit des personnes concernées
6. Transfert des données hors UE
7. Délégué à la protection des données
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

Protection dès la conception « Privacy by design »	**Protection par défaut** « Privacy by default »	**Accountability**	**Analyse d'impact**	**Tenue d'un registre des traitements**
Sécurité	**Notification**	**Communication**	**DPO**	

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Protection dès la conception** « Privacy by design » **(Article 25-1)**

  - La protection des données dès la conception implique :
    - Prise en compte des aspects de protection des données **dès la conception** des produits ou services
    - Mise en conformité **tout au long du cycle de vie** des produits et services

  - La protection des données dès la conception suppose :
    - L'élaboration de **méthodologies, de procédures** permettant de l'intégrer concrètement dans les projets et de s'assurer de la conformité des produits ou services dès création et tout au long de son cycle de vie
    - Implémentation de **mesures techniques et organisationnelles** permettant de s'assurer de la conformité au RGPD

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Protection par défaut** **(Article 25-1)** « Privacy by default »

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **« Accountability » (Article 24)**

Définition : Processus permanent et dynamique de mise en conformité d'une entreprise au RGPD

Implique pour le responsable du traitement et le sous-traitant de :	Prendre des **mesures appropriées** pour se conformer au RGPD	Pouvoir **apporter la preuve** que les mesures appropriées ont été prises pour se conformer au RGPD
Induit une double responsabilité pour le responsable du traitement :	**Être en conformité avec le RGPD**	**Être en mesure de démontrer cette conformité**

L'écrit est essentiel → Documenter les traitements

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

Exemples de **mesures techniques et organisationnelles** permettant de s'assurer de la conformité au RGPD

Sensibilisation	Organisation	Procédure
Formation du personnel	Analyse d'impact	Système de gestion des plaintes des personnes concernées
Guide d'utilisation – charte de bonnes pratiques	Documentation : Rapport annuel d'incidents	Procédure d'audits des traitements
DPO	Registre des traitements	Système de gestion des failles de sécurité
Certification / Label CNIL	Sécurisation (locaux, serveur, site web, matériel informatique, habilitation)	Procédure de gestion des droits des personnes
Alerte, rappel, mémo	Gestion de la sous-traitance	Procédure de destruction et d'archivages des données

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

➢ Analyse d'impact (Article 35)

✓ Traitements concernés par l'analyse d'impact

- Traitement présentant **un risque élevé pour les droits et libertés des personnes physiques,** en particulier par le recours à de nouvelles technologies et compte tenu de sa nature, de sa portée, du contexte et de ses finalités
- 3 catégories de traitements visés spécifiquement :
  - **Surveillance systématique à grande échelle d'une zone accessible au public**
  - **Traitement à grande échelle d'informations sensibles (données sensibles et/ou données personnelles relatives à des condamnations pénales et à des infractions)**
  - **Evaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire**
- Liste publique établie par la CNIL

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- ✓ **Modalités de l'analyse d'impact**
  - Analyse de l'impact du traitement envisagé sur la protection des données à caractère personnel : Evaluation des risques
  - **Préalablement** à la mise en œuvre du traitement (protection dès la conception et par défaut »), mais **obligation de mettre à jour** l'analyse d'impact au fur et à mesure des modifications apportées au traitement
  - **Assistance du sous-traitant** sur demande du responsable du traitement
  - **Conseil du DPO**
- ✓ **Contenu de l'analyse d'impact**
  - Description générale des traitements envisagés et des finalités
  - Evaluation de la nécessité et de la proportionnalité des opérations de traitements
  - Evaluation des risques pour les droits et libertés des personnes concernées
  - Mesures envisagées pour faire face aux risques
- ✓ **Conséquences**
  - Mesures adéquates pour protéger les droits et libertés des personnes concernées
  - Si cette analyse révèle des risques élevés qui ne peuvent être atténués par les mesures envisagées, le responsable de traitement aura alors **l'obligation de consulter préalablement l'autorité de contrôle (Article 36)**

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Tenue d'un registre des traitements (Article 30)**

  - **Suppression du système de formalités préalables auprès de la CNIL, sauf cas spécifiques (Articles 36 et 46)**
    - **Maintien de formalités préalables simplifiées** (traitements portant sur des données génétiques ou biométriques mis en œuvre pour le compte de l'Etat et nécessaires à l'authentification ou le contrôle de l'identité des personnes, traitements effectués dans le domaine de la santé) **(Articles 31 et 32 de la LIL réécrite par l'ordonnance)**
  - **Principe : tenue d'un registre écrit des activités de traitement qui doit faire apparaître:**
    - Identité et coordonnées du responsable du traitement (+ responsable conjoint, représentant du responsable et DPO)
    - Finalités du traitement
    - Description des catégories de personnes concernées
    - Description des catégories de données
    - Destinataires des données
    - Transfert vers un pays tiers ou une organisation internationale
    - Délai prévu pour l'effacement des données
    - Description générales des mesures de sécurité techniques et organisationnelles

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Dérogation à l'obligation de tenue d'un registre pour les entreprises comptant moins de 250 employés, sauf dans les cas suivants :**
  - Si le traitement qu'elles effectuent est susceptible de comporter un **risque pour les droits et libertés des personnes concernées**
  - Si le traitement n'est **pas occasionnel**
  - Si le traitement porte notamment sur des **données sensibles** (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, biométriques, données concernant la santé, la vie sexuelle ou l'orientation sexuelle)
  - Si le traitement porte sur des **données relatives à des condamnations pénales et des infractions**

Fiche de registre ref-000

Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images…		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale,		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		

RESPONSABLE DE TRAITEMENT

Titre : **Gestion du Recrutement**

N°/ Réf.

I. INFORMATIONS GENERALES	
1. Date de mise en œuvre du Traitement	
2. Mise à jour (date et objet)	
II. IDENTIFICATION DES PARTIES PRENANTES	
3. Entité concernée	 Coordonnées :
4. Direction/ département concerné(e)	 Coordonnées :
5. Personne responsable	 Coordonnées :
III. FINALITES DU TRAITEMENT	
6. Description de la/des finalité(s) du traitement	
7. Nom de l'/des outil(s) ou de l'/des application(s) utilisé(s)	

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Obligation de sécurité (Articles 25-2 et 32)**

  - ✓ **Niveau de protection allégé dans le RGPD**

  - ✓ **Obligation de garantir un niveau de sécurité adapté** :
    - Pseudonymisation et chiffrement des données
    - Mise en place de moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et services de traitement
    - Mise en place de moyen permettant de rétablir la disponibilité des données et leur accès dans des délais appropriés
    - Mise en place d'une procédure visant à tester, analyser, et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles des mesures techniques de sécurité
  - ✓ **Moyens permettant de démontrer le respect de cette obligation:**
    - Application de code de conduite ou mécanisme de certification

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

➢ Obligation de sécurité (Articles 25-2 et 32)

Critères d'appréciation des mesures

- Etat des connaissances et **coûts de mise en œuvre**
- **Nature, portée, contexte, finalité** du traitement
- **Risques présentés par le traitement** (degré de probabilité et de gravité) résultant de la destruction, perte, altération, divulgation, accès non autorisé aux données

Catégories de mesures

- **Pseudonymisation / chiffrement** des données
- **Moyens permettant de garantir la confidentialité** des systèmes de traitement…
- **Moyens permettant de rétablir la disponibilité / accès** aux données en cas d'incident physique ou technique
- Procédure **d'évaluation régulière des mesures de sécurité**

Pseudonymisation

- Les données ne peuvent plus être attribuées à un individu sans avoir recours à des informations supplémentaires conservées de manière séparée afin de garantir qu'il ne soit plus identifié ou identifiable
- **RÉVERSIBLE**

Anonymisation

- Technique consistant à supprimer tout caractère identifiant à un ensemble de données
- **IRRÉVERSIBLE**

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Obligation de notification (Article 33)**
  - Le **responsable** doit notifier à la **CNIL les violations de données susceptibles d'engendrer un risque pour les droits et libertés des personnes physiques** dans les meilleurs délais et, si possible **72h au plus tard** après en avoir pris connaissance
    - Le **sous-traitant** doit notifier **au responsable toute violation de données dans les meilleurs délais** après en avoir pris connaissance
  - Contenu de la notification :
    - Description de la violation de données
    - Coordonnées du DPO
    - Description des conséquence probables de la violation de données
    - Description des mesures prises ou proposées pour remédier à la violation de données et le cas échéant, les mesures pour atténuer les conséquences négatives de la violation
  - Le responsable de traitement doit tenir **un registre des failles de sécurité** contenant :
    - Les faits de violation
    - Ses effets
    - Les mesures prises pour y remédier

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Obligation de communication (Article 34)**

  - **Principe** : Obligation pour le responsable de traitement d'informer directement la personne concernée **dans les meilleurs délais** des violations de données susceptibles d'engendrer un **risque élevé** pour leurs droits et libertés.

  - **Contenu** de la communication *a minima* :
    - Description claire et simple de la nature de la violation de données
    - Nom et coordonnées du DPO
    - Conséquences probables de la violation de données
    - Description des mesures prises ou proposées pour remédier à la violation de données et, le cas échéant, les mesures pour en atténuer les conséquences négatives

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Exceptions :**
  - Le responsable a mis en œuvre les **mesures de protection techniques et organisationnelles appropriées** et les a appliquées aux données affectées par la violation
  - Le responsable a pris des **mesures ultérieures** qui garantissent que le risque n'est plus susceptible de se matérialiser
  - La communication exigerait des **efforts disproportionnés** : RGPD recommande dans ce cas une communication publique
  - **Dérogations spécifiques** introduites en droit français, qui peuvent être apportées par décret en Conseil d'Etat lorsque cette notification est susceptible de représenter un risque pour **la sécurité nationale, la défense nationale ou la sécurité publique (Article 58 de la LIL réécrite par l'ordonnance)**

- La CNIL, informée de la violation, peut exiger du responsable qu'il procède à cette communication

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- **Focus sur le sous-traitant : de nouvelles règles et un nouveau rôle**
  - Le sous-traitant doit présenter **les garanties appropriées** au respect du RGPD **(Art. 28)**
  - Le sous-traitant ne pourra pas recruter de sous-traitant sans **autorisation préalable écrite** du responsable de traitement **(Art. 28)**
  - Le sous-traitant a des obligations directes à respecter, notamment :
    - Obligation de **traiter sur instruction** du responsable de traitement **(Art. 29)**
    - Obligation de tenir **un registre du traitement (Art. 30)**
    - Obligation de **coopérer avec l'autorité de contrôle (Art. 31)**
    - Obligation **d'assurer la sécurité des données (Art. 32)**
    - Obligation de **notifier la violation des données** au responsable du traitement **(Art. 33)**
    - Obligation de nommer un **délégué à la protection des données (Art. 37)**
    - Le sous-traitant sera **tenu de réparer le dommage** qu'il causé du fait du non respect de ses obligations prévues au RGPD **(Art. 82)**
    - Obligation générale **d'aider le responsable** dans l'accomplissement de ses obligations, dans sa démarche permanente de mise en conformité **(Art. 28)**

4. OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- Le contrat de sous-traitance devra contenir des **stipulations impératives** comprenant :
  - objet et durée du traitement
  - nature et finalités du traitement
  - type de données à caractère personnel concernées
  - catégories de personnes concernées
  - obligations et droits du responsable de traitement
  - obligations du sous-traitant de ne traiter que sur instruction, de veiller à la sécurité des données, ainsi qu'à leur confidentialité, et d'aider le responsable dans l'accomplissement de ses obligations **(Article 28)**

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. Obligations des responsables de traitements
5. **DROIT DES PERSONNES CONCERNEES**
6. Transfert des données hors UE
7. Délégué à la protection des données
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

5. DROITS DES PERSONNES CONCERNEES

Avant le RGPD	Depuis le RGPD
	Droit à la compréhension
Droit à l'information	Droit à l'information
Droit d'accès	Droit d'accès
Droit de rectification	Droit de rectification
Droit d'effacement	Droit d'effacement
Droit d'opposition	Droit d'opposition
	Droit à la limitation
	Droit à la portabilité
	Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé
	Droit de réclamation et de recours et droit réparation

5. DROITS DES PERSONNES CONCERNEES

- Identité et coordonnées du RT
- Coordonnées du DPO
- Finalité(s) du traitement
- Base juridique du traitement
- Intérêt légitime poursuivi par le RT
- Destinataires et catégories de destinataires des données
- Durée de conservation des données
- Transfert en dehors de l'UE
- Droits des personnes
- Droit de retirer son consentement à tout moment
- Droit de réclamation auprès de la CNIL
- Obligation réglementaire ou contractuelle à la fourniture des données
- Existence, mesures et effets d'une prise de décision automatisée, dont le profilage
- Caractère facultatif ou obligatoire des réponses et conséquences d'un défaut de réponse

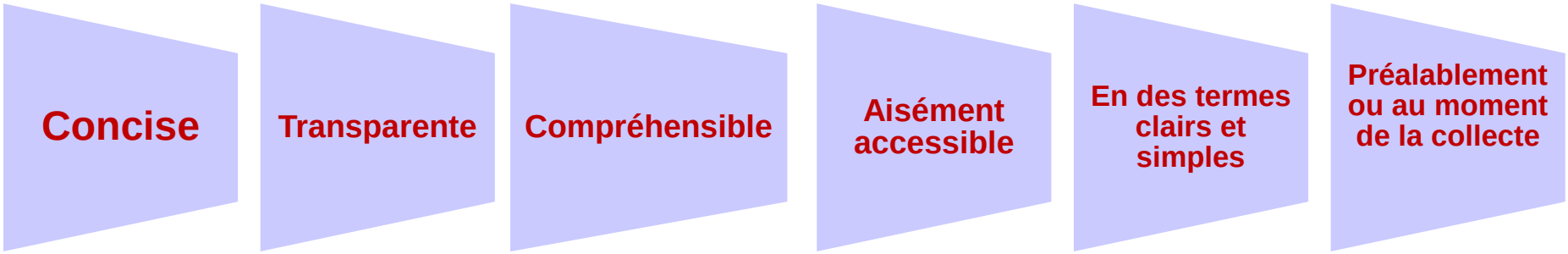
En cas de collecte indirecte :

- Source des données
- Catégories des données concernées par le traitement

5. DROITS DES PERSONNES CONCERNEES

➢ Droit à la compréhension (Article 12)

- Toutes les informations fournies à la personne concernée doivent l'être de manière :



L' écrit pas exigé mais recommandé :

- Contrat / avenant
- Affichage
- Politique de confidentialité
- Email pour régulariser

5. DROITS DES PERSONNES CONCERNEES

- **Droit d'accès (Article 15 du RGPD)**
  - Accès permanent à la finalité du traitement et à ses droits
  - Spécificité introduite en droit français pour les **données de santé** : communication des données concernées par une demande d'exercice d'un droit d'accès à un médecin désigné par la personne qui en fait la demande **(Article 49 de la LIL réécrite par l'ordonnance)**

- **Droit de rectification (Article 16)**
  - Mise à jour et correction des données inexactes

- **Droit d'opposition (Article 21)**
  - Toute personne a le droit de s'opposer, **pour des motifs légitimes**, à ce que des données personnelles la concernant fassent l'objet d'un traitement

  - Spécificités introduites en droit français : **dérogations prévues aux droits d'accès, de rectification et d'effacement (Article 52 de la LIL réécrite par l'ordonnance)**

5. DROITS DES PERSONNES CONCERNEES

- **Droit à l'effacement « droit à l'oubli » (Article 17)**

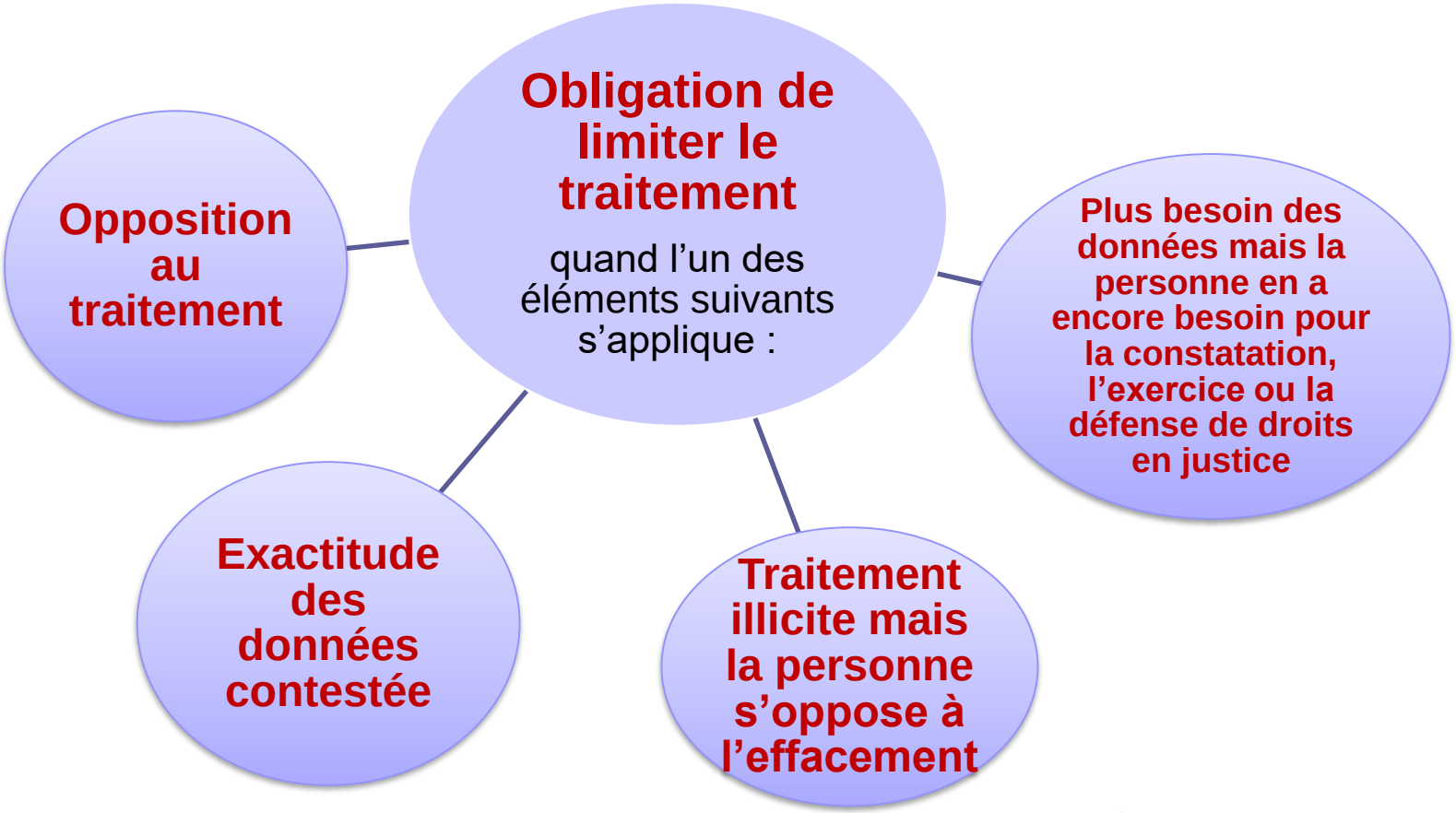
  - **Principe** : Obligations d'effacer dans les meilleurs délais les données d'une personne concernée dans les 6 cas suivants :
    - Les données ne sont **plus nécessaires** au regard des finalités pour lesquelles elles ont été collectées ou traitées
    - La personne concernée **retire le consentement** sur lequel est fondé le traitement et aucun fondement légal n'existe
    - La personne concernée **s'oppose au traitement** et aucun motif légitime impérieux pour le traitement
    - Les données ont fait l'objet d'un **traitement illicite**
    - Existence d'une **obligation légale** d'effacer les données à laquelle serait soumise le responsable de traitement
    - Les données ont été collectées dans le cadre de l'offre de services de la société de l'information pour des **enfants âgés de moins de 16 ans**

5. DROITS DES PERSONNES CONCERNEES

- **Exception** quant le traitement des données est nécessaire **:**
  - À l'exercice du droit à la **liberté d'expression** et d'information
  - Pour le respect d'une **obligation légale** auquel le responsable est soumis
  - Pour des **motifs d'intérêt public** dans le domaine de la **santé publique**
  - À des **fins d'archivage** dans l'intérêt public ou à des fins de **recherche scientifique ou historique ou à des fins statistiques**
  - À la constatation, l'exercice ou la défense **de droits en justice**

5. DROITS DES PERSONNES CONCERNEES

- **Droit à la limitation du traitement (Article 18)**

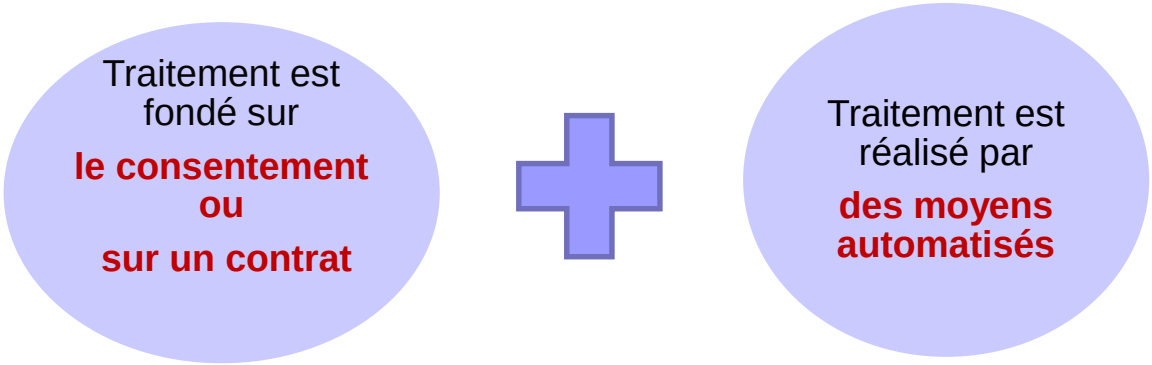


5. DROITS DES PERSONNES CONCERNEES

➢ Droit à la portabilité des données (Article 20)

✓ Principe :

- La personne concernée a le droit de **recevoir** les données la concernant **qu'elle a fourni** à un responsable de traitement dans un **format structuré couramment utilisé et lisible par machine**
- La personne a le droit de les **transmettre** à un autre responsable de traitement sans que le 1er responsable de traitement s'y oppose. Les données à caractère personnel peuvent aussi être **transmises directement** d'un responsable du traitement à un autre, lorsque cela est techniquement possible
- **2 conditions cumulatives** pour bénéficier de ce droit



✓ Exclusion :

- Les traitements nécessaires à l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont sont investis les responsables du traitement

5. DROITS DES PERSONNES CONCERNEES

- **Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (Article 20)** y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire **(Article 22)**

- Spécificité introduite en droit français : faculté pour l'Administration de prendre des décisions individuelles automatisées sous certaines conditions **(Article 47 de la LIL réécrite par l'ordonnance)**

- **Droit de réclamation et de recours et droit de réparation**
  - Toute personne a le droit d'introduire une réclamation auprès d'une autorité de contrôle, de former un recours contre une autorité de contrôle, contre un responsable de traitement et un sous-traitant seul ou dans le cadre d'une action de groupe **(Articles 77, 78 et 79)**
  - Toute personne a le droit d'obtenir la réparation intégrale du **dommage matériel ou moral** causé du fait d'une violation du règlement auprès du **responsable de traitement ou du sous-traitant (Article 82)**
  - Précision du régime de l'action de groupe **(Articles 37, 38, 39 de la LIL réécrite par l'ordonnance)**

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. Obligations des responsables de traitements
5. Droit des personnes concernées
6. **TRANSFERT DES DONNEES HORS UE**
7. Délégué à la protection des données
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

6. TRANSFERT DES DONNEES HORS UE

- ✓ **Articles 44 à 48**

- ✓ **En principe**, le transfert des données personnelles hors de l'U.E. est **interdit**

- ✓ **Par dérogation,** il est autorisé lorsque le transfert est réalisé dans un cadre défini :
  - **Décision d'adéquation** rendue par la Commission de l'Union Européenne constatant que le pays tiers destinataire des données dispose d'un niveau de protection suffisant **(Article 45)**
  - **Garanties appropriées données par le responsable du traitement (Article 46)**
    - Clauses contractuelles (subordonnées à l'autorisation préalable de la CNIL)
    - Binding corporate rules « BCR » Règles d'entreprises contraignantes
    - Certifications ou codes de conduite
  - **Décision d'une juridiction ou d'une autorité administrative d'un pays tiers fondée sur un accord international**, tel qu'un traité d'entraide judiciaire en vigueur entre le pays tiers demandeur et l'Union ou un Etat membre **(Article 48)**

6. TRANSFERT DES DONNEES HORS UE

- ✓ **Par exception**, le RGPD prévoit la possibilité de transfert hors de l'UE dans l'un des cas suivants : **(Article 49)**
  - En cas de consentement exprès de la personne concernée
  - Transfert nécessaire à l'exécution d'un contrat entre la personne concernée et les responsables du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée
  - Transfert nécessaire à la conclusion ou l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable de traitement et une autre personne physique ou morale
  - Transfert nécessaire pour des motifs importants d'intérêt public
  - Transfert nécessaire à la constatation, l'exercice ou la défense de droits en justice
  - Transfert nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes quand la personne concernée est dans l'incapacité de donner son consentement
  - Transfert a lieu au départ d'un registre destiné à fournir des informations au public et est ouvert à la consultation au public

6. TRANSFERT DES DONNEES HORS UE

✓ Traitement transfrontalier

- **Principe : Système du Guichet unique (Article 56)**

  En cas de traitement transfrontalier effectué par un responsable de traitement ou sous-traitant (notamment lorsque celui-ci a des filiales dans plusieurs Etats membres), ce dernier ne traitera qu'avec **l'autorité de contrôle de l'Etat membre dans lequel il a son établissement principal ou de son établissement unique**, qui est appelé « autorité chef de file » ou « Guichet unique »

- **Dérogation :**

  Chaque autorité de contrôle est compétente pour traiter une réclamation introduite auprès d'elle ou une éventuelle violation du RGPD, si son objet concerne uniquement un établissement dans l'Etat membre dont elle relève ou affecte sensiblement des personnes concernées dans cet Etat membre uniquement

- **Procédure :**

  L'autorité de contrôle chef de file devra coopérer avec les autres autorités de contrôle concernées s'efforçant de parvenir à un consensus **(Article 60)**

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. Obligations des responsables de traitement
5. Droit des personnes concernées
6. Transfert des données hors UE
7. **DELEGUE A LA PROTECTION DES DONNEES**
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

7. DELEGUE A LA PROTECTION DES DONNEES

- Les Responsables et le sous-traitant doivent désigner **un DPO** dans les cas suivants **(Article 37)** :
  - Traitement effectué par une autorité publique ou un organisme public
  - Leurs activités de base consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées
  - Leur activité de base consistent en un traitement à grande échelle des données particulières visées à l'article 9 (Données sensibles), et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10

- Il est désigné pour ses **qualités professionnelles** et en particulier, ses connaissances spécialisées du droit et ses pratiques en matière de protection des données, et sa capacité à accomplir ses missions

- Il peut être un **membre du personnel**, ou exercer ses missions en vertu d'un **contrat de prestation de service**

- Ses coordonnées sont publiées et communiquées à l'autorité de contrôle

7. DELEGUE A LA PROTECTION DES DONNEES

- Il doit être **associé à toutes les questions relatives à la protection des données personnelles (Article 38)**

- Un groupe d'entreprise peut désigner **un seul DPO** à condition qu'il soit facilement joignable à partir de chaque lieu d'établissement.

- **Ses missions (Article 39)** :
  - Informer et conseiller le responsable de traitement ou le sous-traitant, et le personnel chargé du traitement, de leurs obligations.
  - Faire directement rapport au niveau le plus élevé de la direction
  - Contrôler le respect du RGPD, ainsi que des autres dispositions de l'UE dont l'objet est de protéger les données à caractère personnel.
  - Conseiller, sur demande, lorsqu'une analyse d'impact est effectuée et vérifier son exécution
  - Coopérer avec l'autorité de contrôle
  - Faire office de point contact pour l'autorité de contrôle

Le DPO peut exécuter d'autres missions si cela n'entraine pas de conflit d'intérêts

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. Obligations des responsables de traitements
5. Droit des personnes concernées
6. Transfert des données hors UE
7. Délégué à la protection des données
8. **RECOURS DE LA PERSONNE CONCERNEE**
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

8. RECOURS DE LA PERSONNE CONCERNEE

Réclamation auprès d'une autorité contrôle (Article 77)

- Toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle (sans préjudice de tout autre recours administratif ou juridictionnel)
- Si elle considère que le traitement de données la concernant constitue une **violation du RGPD**
- Auprès de l'autorité de contrôle de l'Etat membre dans lequel se trouve **sa résidence habituelle, son lieu de travail ou le lieu où la violation a été commise**

Recours juridictionnel contre une autorité de contrôle (Article 79)

- Toute personne concernée a droit à un **recours juridictionnel effectif**
  - Contre une **décision juridiquement contraignante** d'une autorité de contrôle qui la concerne
  - Lorsque l'autorité de contrôle **ne traite pas une réclamation** ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de sa réclamation introduite sur le fondement de l'article 77 du RGPD

8. RECOURS DE LA PERSONNE CONCERNEE

- **Recours juridictionnel contre un responsable ou un sous-traitant (Article 79)**
  - Toute personne concernée a droit à un **recours juridictionnel effectif** contre un responsable de traitement ou un sous-traitant (sans préjudice de tout autre recours administratif ou extrajudiciaire dont celui prévu à l'article 77 RGPD)
  - Si elle considère que les **droits que lui confère le RGPD ont été violés** du fait d'un traitement de ses données effectuées en violation du RGPD
  - Auprès des juridictions de l'Etat membre dans lequel :
    - le responsable de traitement ou le sous-traitant dispose **d'un établissement**.
    - La personne concernée **a sa résidence personnelle** (sauf si le responsable est une autorité publique d'un Etat membre agissant dans l'exercice de ses prérogatives de puissance publique)

- **Action de groupe (Article 80)**
  - Une personne pourra **mandater un organisme, une organisation ou une association à but non lucratif**, constituée conformément au droit d'un Etat membre, dont les objectifs sont d'intérêts publics, et dont l'objet est de protéger les droits et libertés des personnes concernées, pour qu'il introduise une réclamation **en son nom et exerce en son nom** les droits visés aux articles 77, 78 et 79 et exerce en son nom le droit d'obtenir réparation du préjudice subi en raison de la violation du RGPD

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. Obligations des responsables de traitement
5. Droit des personnes concernées
6. Transfert des données hors UE
7. Délégué à la protection des données
8. Recours de la personne concernée
9. **POUVOIRS DE LA CNIL ET SANCTIONS**
10. Bilan de la CNIL
11. Recommandations pour la mise en conformité

9. POUVOIRS DE LA CNIL ET SANCTIONS

- **Missions principales (Article 57)**

Contrôler | Sensibiliser | Traiter les réclamations | Enquêter | Informer | Participer à l'élaboration de clauses types

- **Principaux pouvoirs (Article 58)**

Demander tout type d'informations ou de documents à la personne contrôlée | Contrôler: sur place, sur pièces, sur convocation, en ligne | Réaliser des audits | Prévenir, rappeler à l'ordre, ordonner et sanctionner

- **Sanctions (Considérant 148)**

Injonction sous astreinte | Mise en demeure | Rappel à l'ordre | Amende administrative

9. POUVOIRS DE LA CNIL ET SANCTIONS

- **Amendes administratives (Article 83)**

10.000.000 euros d'amende ou 2% du chiffre d'affaires annuel mondial	Absence de protection des données dès la conception
	Absence de tenue de registre des activités de traitement
	Absence de protection des données par défaut
	Absence d'analyse d'impact
	Absence de notification à la CNIL d'une violation de données
20.000.000 euros d'amende ou 4% du chiffre d'affaires annuel mondial	Non respect des principes fondamentaux (transparence, proportionnalité, légitimité, consentement, et.)
	Non respect de l'un des droits des personnes
	Non respect des dispositions relatives aux transferts de données

9. POUVOIRS DE LA CNIL ET SANCTIONS

- **Eléments pris en compte** pour décider s'il y a lieu d'imposer une amende et pour décider du montant de l'amende

Nature gravite et durée de la violation	Portée, finalité du traitement et catégories de données concernées	Nombre de personnes concernées et niveau de dommage subi
Violation délibérée ou commise par négligence	Mesures prises pour atténuer le dommage subi	Degré de responsabilité du responsable ou du sous-traitant compte tenu des mesures techniques et organisationnelles mises en œuvre
Violations précédemment commises	Degré de coopération avec l'autorité de contrôle pour remédier à la violation et atténuer les dommages	Application de code de conduites ou de mécanismes de certification
Manière dont l'autorité de contrôle a eu connaissance de la violation	Respect des mesures précédemment ordonnées à l'encontre du responsable ou sous-traitant	Toute autre circonstance aggravante ou atténuante (avantages financiers obtenus ou pertes évitées par la violation)

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. Obligations des responsables de traitement
5. Droit des personnes concernées
6. Transfert des données hors UE
7. Délégué à la protection des données
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. BILAN DE LA CNIL
11. Recommandations pour la mise en conformité

10. BILAN DE LA CNIL

INFORMER

18.9877 appels reçus

+ 22 %

283.742 consultations Questions / Réponses

+59%

8 millions de visites sur *cnil.fr*

+ 80 %

16.877 requête sur la plateforme « Besoin d'aide »

+ 15%

10. BILAN DE LA CNIL

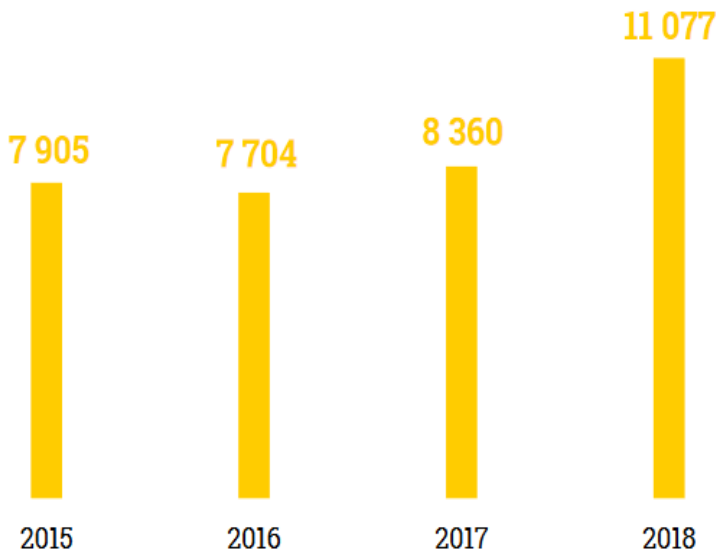
Protéger

1.170 notifications de violations de données

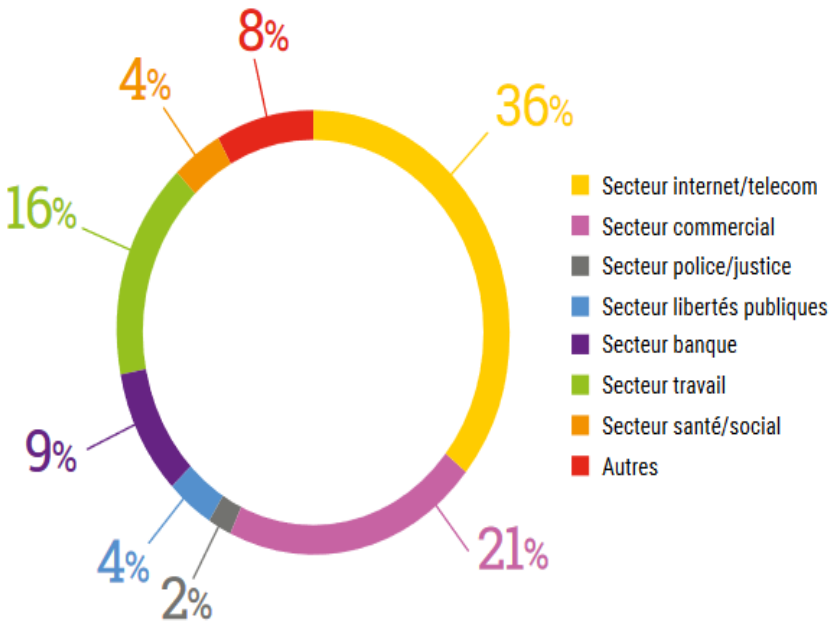
11.077 de plaintes déposées **+ 32,5 %**

10. BILAN DE LA CNIL

Évolution du nombre de plaintes depuis 2015

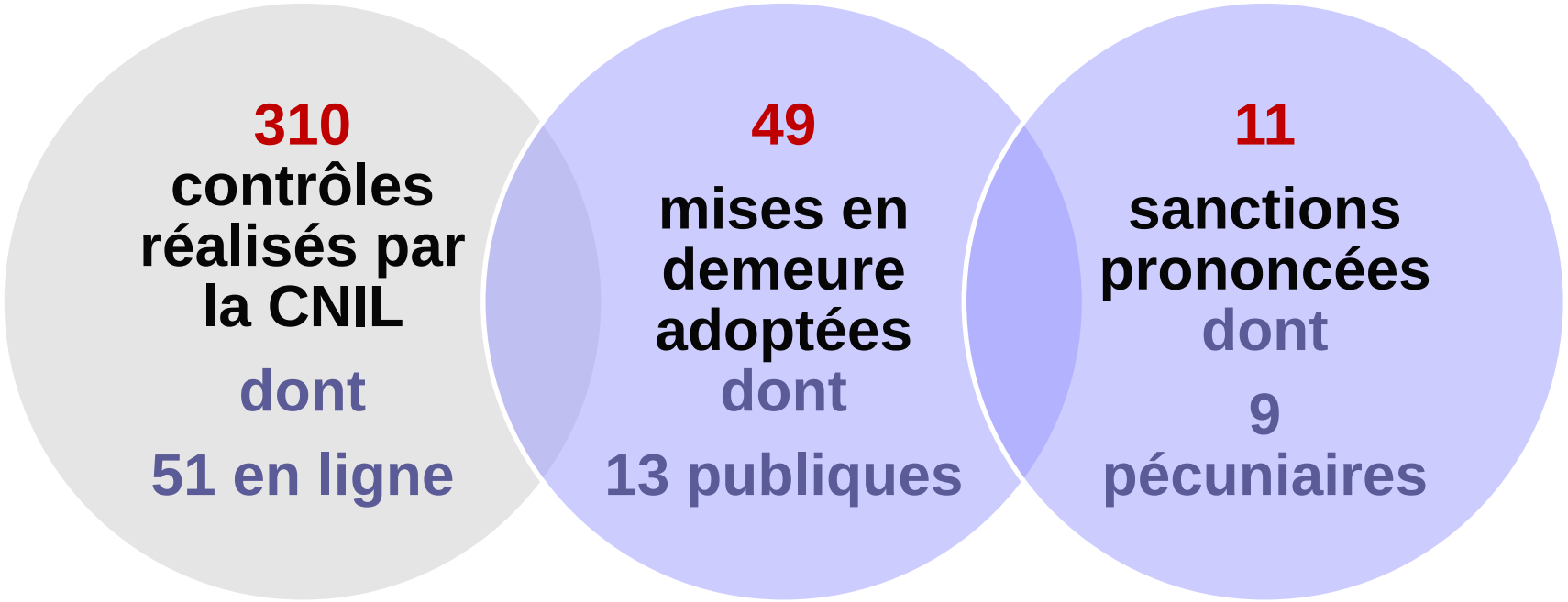


Répartition des plaintes par secteur d'activité (2018)

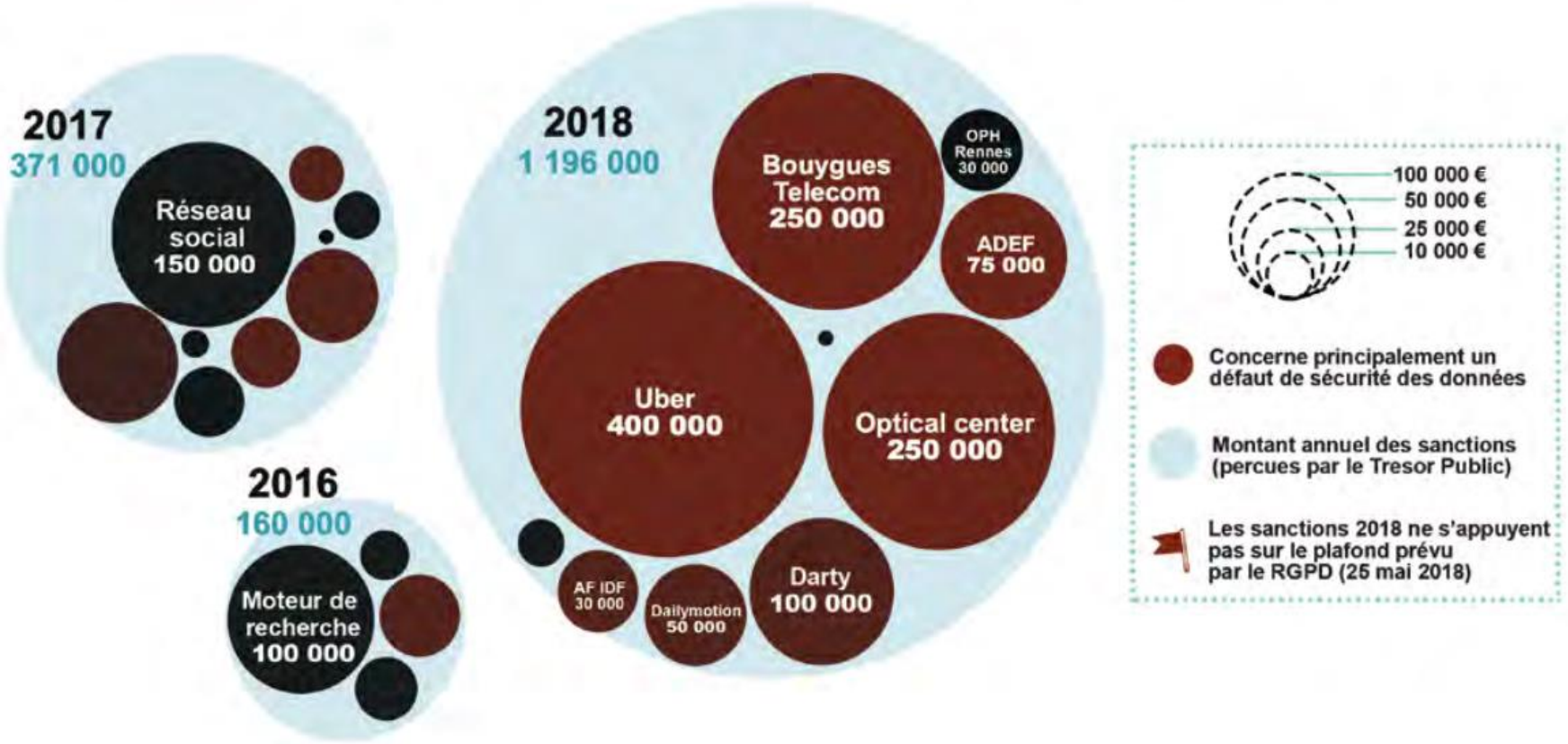


10. BILAN DE LA CNIL

CONTROLER ET SANCTIONNER



10. BILAN DE LA CNIL



10. BILAN DE LA CNIL

GRANDES TENDANCES

Prise de conscience des enjeux de la protection des données

Afflux de demandes d'informations de la part des professionnels

Augmentation du nombre de plaintes déposées

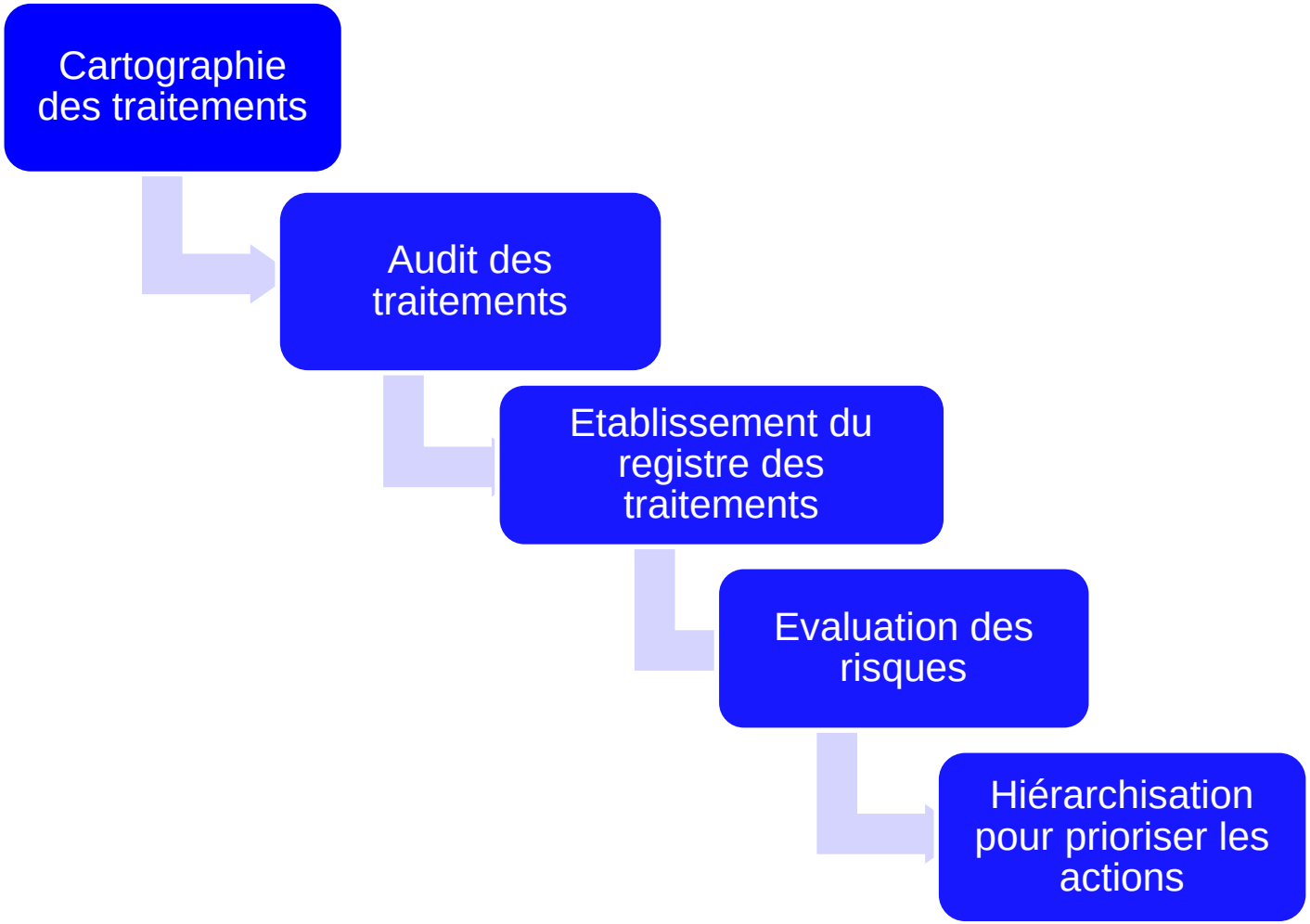
10. BILAN DE LA CNIL

ENJEUX

- Réussir la mise en œuvre du RGPD
- Approfondir sa capacité d'expertise sur les infrastructures et plateformes numériques, par l'exploration de l'impact des usages des innovations technologiques sur la vie privée et les libertés
- Rendre opérationnel ce nouveau cadre juridique par la pédagogie et la dissuasion
- Rendre pleinement effectif le RGPD par la multiplication des contrôles sur des domaines touchant une multiplicité d'acteurs, adopter pleinement le cadre correctif instauré par le RGPD
- Continuer à peser dans les discussions européennes et internationales

1. Contexte
2. Champ d'application du RGPD
3. Principes directeurs
4. Obligations des responsables de traitement
5. Droit des personnes concernées
6. Transfert des données hors UE
7. Délégué à la protection des données
8. Recours de la personne concernée
9. Pouvoirs de la CNIL et sanctions
10. Bilan de la CNIL
11. RECOMMANDATIONS POUR LA MISE EN CONFORMITE

11. RECOMMANDATIONS POUR LA MISE EN CONFORMITE



11. RECOMMANDATIONS POUR LA MISE EN CONFORMITE

- Mise en place des procédures, mesures techniques et organisationnelles
- Mise à jour des documents d'information
- Mise à jour des contrats avec les sous-traitants
- Sensibilisation des personnels
- Tests et audits

Merci de votre attention

* *

*

Carole Couson-Warlop

ARTLEX
CABINET D'AVOCATS