Droit

Janvier 2023 – VMI Paris Descartes

Pratique

Si vous souhaitez me joindre :
a.pronier@evolve-avocats.com

Mettre : c.aldebert@evolve-avocats.com en copie

Partiel : le 15 décembre de 10h à 12h

Plan

I – LE RGPD

II – PROPRIETE INTELLECTUELLE, VIE PRIVEE ET DROIT A L'IMAGE

III – INTELLLIGENCE ARTIFICIELLE & CAS PRATIQUES

IV – APERCU DES CONTRATS INFORMATIQUES

Le RGPD (Règlement Général sur la Protection des Données)

Janvier 2023 – VMI Paris Descartes

En bref

De quoi s'agit-il ?

Le RGPD est la base de l'ensemble des législations des pays européens sur le traitement des données

Règlement européen adopté en avril 2016, est **applicable depuis le 25 mai 2018**

La loi Informatique et libertés en France existante depuis 1978 a été modifiée en 2018 pour s'adapter

Application de cette règlementation par les autorités nationales de protection des données : la CNIL en France

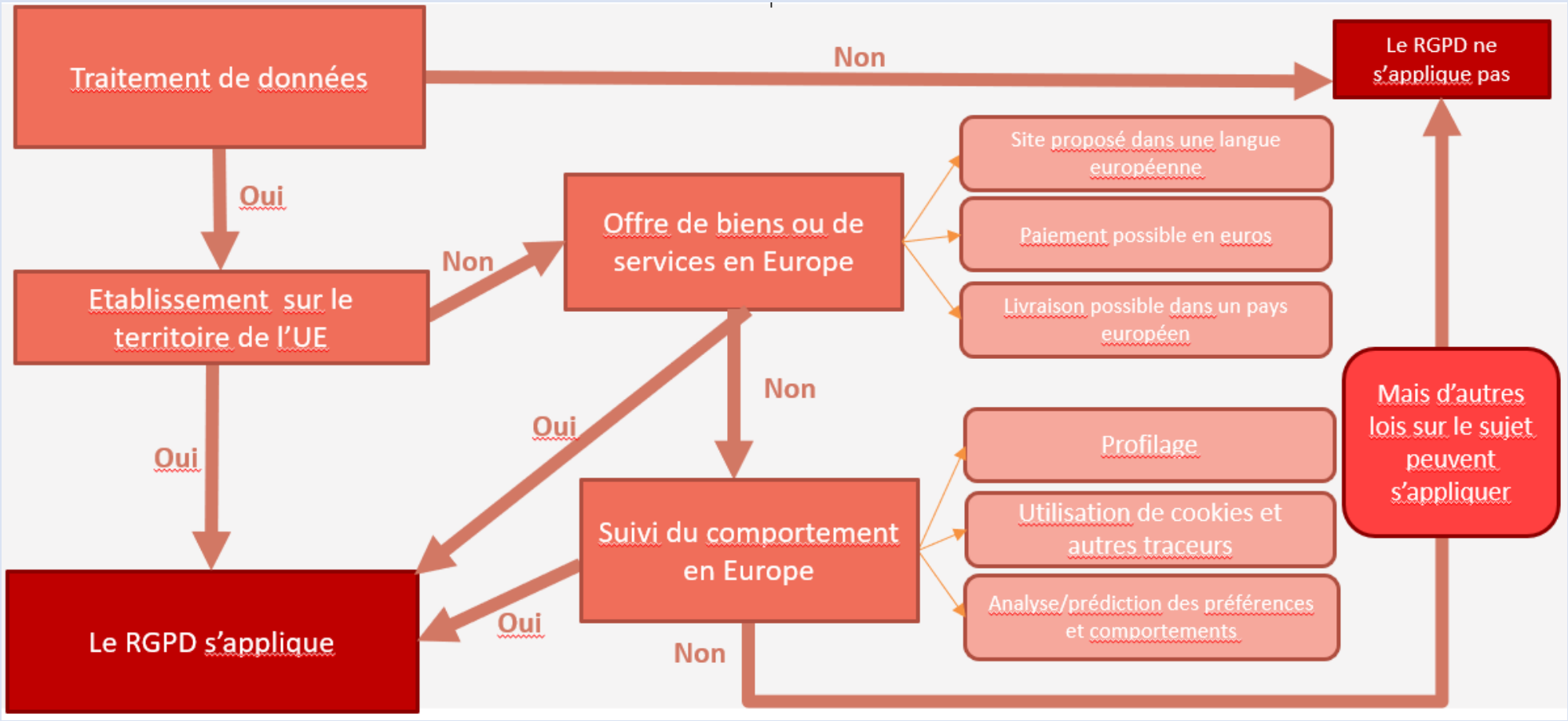
Objectifs

- Harmoniser les législations européennes
- Viser les entreprises notamment US qui utilisent les données des Européens mais estimaient que la loi européenne ne leur était pas applicable jusqu'ici
- Donner plus de pouvoir aux citoyens sur leurs données

Importance du RGPD

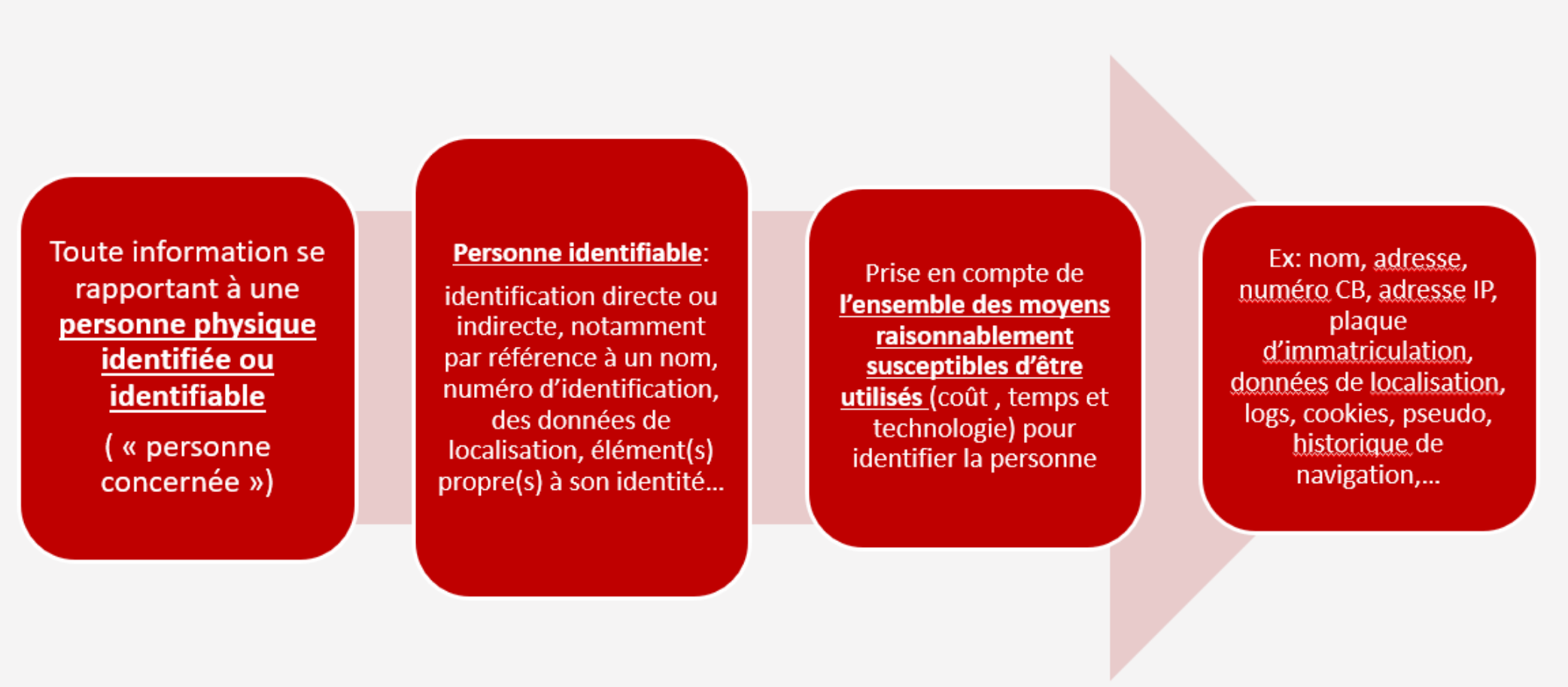
- Amendes jusqu'à **4% du chiffre d'affaires annuel du groupe** ou 20 millions d'euros (le montant le plus élevé des deux)
- L'une des amendes la plus importante infligée par la CNIL : Meta en 2023 = 1,2 milliards d'euros
- Amende d'Amazon prononcée par la CNIL luxembourgeoise : 746 millions d'euros (traitement de données pour des analyses comportementales et ciblages publicitaires sans consentement préalable des personnes concernées : identité, adresse IP, données de connexion, etc.)
- Préjudice important en termes d'image
- Associations peuvent agir pour représenter les victimes
- Charge de la preuve repose sur le responsable de traitement

Modalités d'application du RGPD

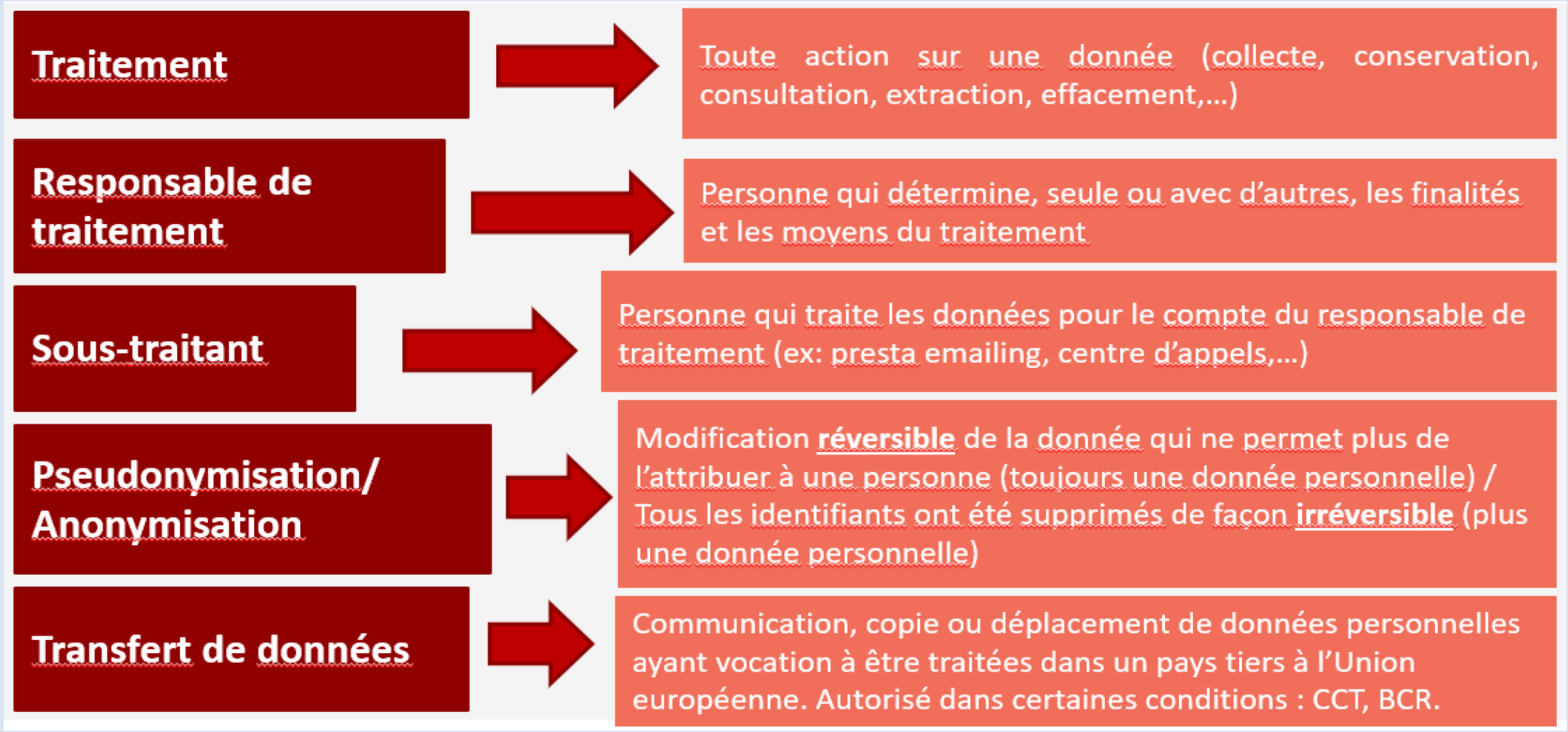


Définitions

Donnée à caractère personnel



Principales notions du RGPD



Principes généraux

Privacy dès la conception et par défaut

Protection dès la conception

- Prise en compte des principes de la protection des données dès la conception du produit/service + tout au long de sa durée de vie
- Bonnes pratiques: **minimisation des données & pseudonymisation**

Protection par défaut

- S'assurer que seules les données nécessaires sont traitées, par les personnes appropriées.
- Bonnes pratiques: **minimisation des données, limitation de la durée de conservation & gestion des accès**

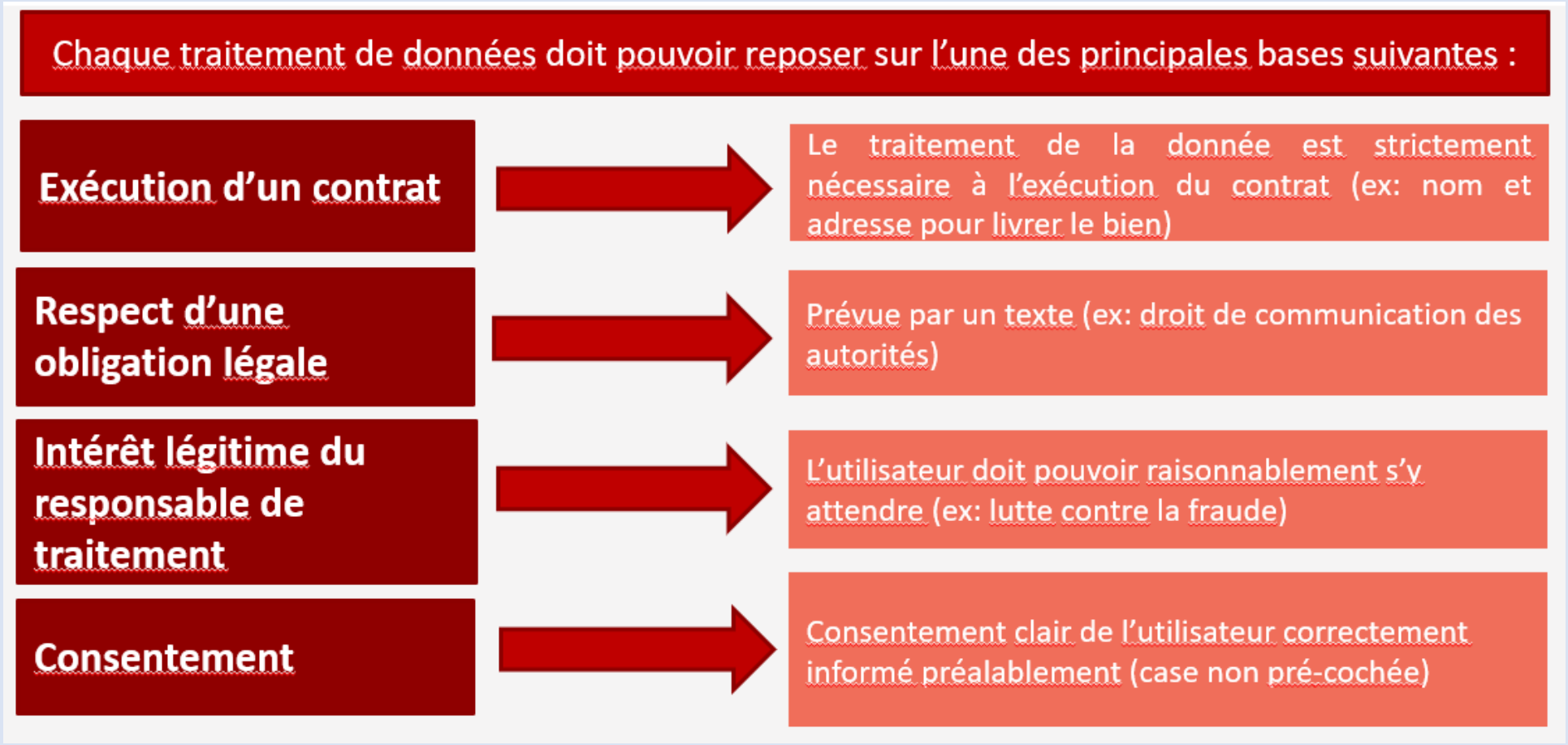
Objectif du traitement

- Un traitement de données doit avoir un objectif, une **finalité** → pas de collecte ou traitement de données « au cas où ».

- A chaque traitement de données **doit être assigné un but**, qui doit bien évidemment être **légal** et **légitime** au regard de votre activité professionnelle.

- **Exemple** : vous collectez sur vos clients de nombreuses informations, lorsque vous effectuez une livraison, éditez une facture ou, proposez une carte de fidélité. Toutes ces opérations sur ces données constituent votre traitement de données personnelles ayant pour objectif la gestion de votre clientèle.

Bases juridiques



Bases juridiques

2 bases juridiques sont moins courantes :

- **le traitement est nécessaire à la sauvegarde des intérêts vitaux** de la personne concernée;

- **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;

Principes de traitement

Chaque traitement de données doit respecter les principes suivants :

Licéité, loyauté & transparence	La personne concernée doit savoir pourquoi et comment ses données sont utilisées (via la politique de confidentialité).
Limitation des finalités	Les données sont uniquement collectées pour des **finalités déterminées**, légitimes et portées à la connaissance de la personne concernée. Les données ne peuvent être utilisées que pour les finalités pour lesquelles elles ont été collectées.
Minimisation des données	Seules les données adéquates et pertinentes doivent être collectées. Ne pas collecter plus de données que celles strictement nécessaires à la réalisation des finalités.

Principes de traitement

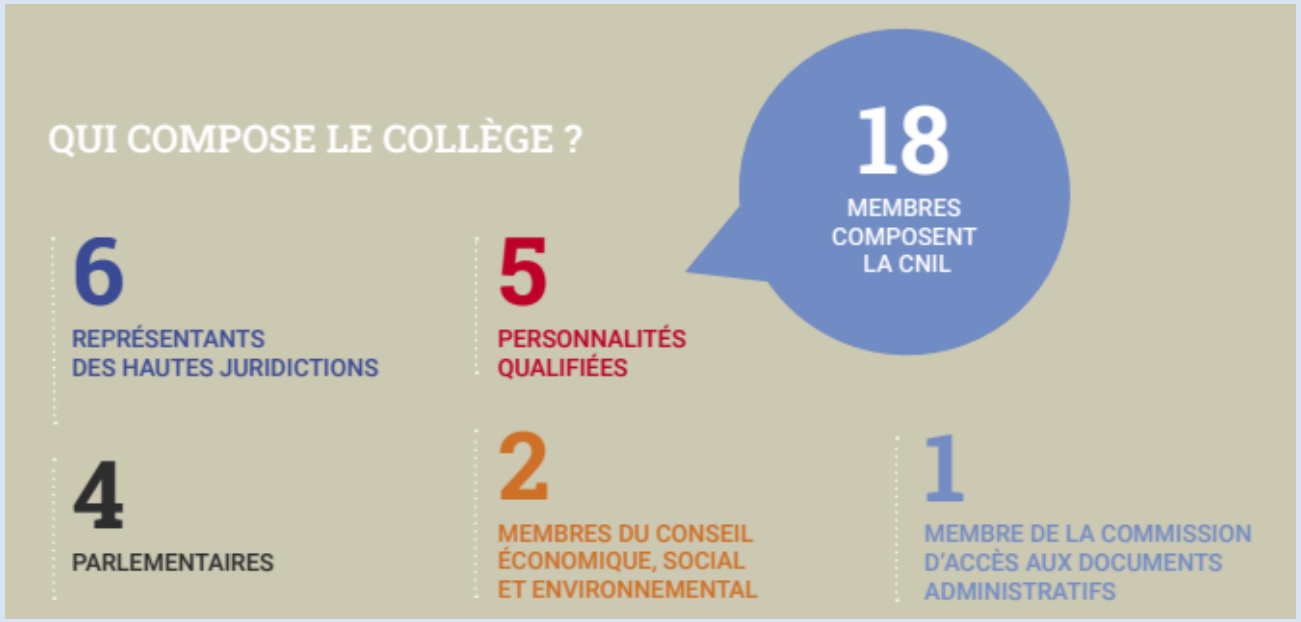
Chaque traitement de données doit respecter les principes suivants :

Exactitude des données	Les données collectées doivent être exactes et maintenues à jour. Les données non exactes doivent être rectifiées ou effacées.
Limitation de la conservation	Pas de conservation des données pendant plus de temps que ce qui est strictement nécessaire. Nécessité de prendre en compte tous les autres impératifs de conservation pour établir une politique de durée de conservation (archivage).
Intégrité & confidentialité	Nécessité de garantir la sécurité des données.
Responsabilité (“accountability”)	Etre en mesure de démontrer le respect de tous ces principes (via des procédures internes).

Application pratique du RGPD

LA CNIL (Commission nationale de l'informatique et des libertés)

Autorité administrative indépendante, la CNIL est composée d'un Collège pluridisciplinaire de **18 membres** élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent, par le Premier ministre et les présidents du Sénat et de l'Assemblée nationale.



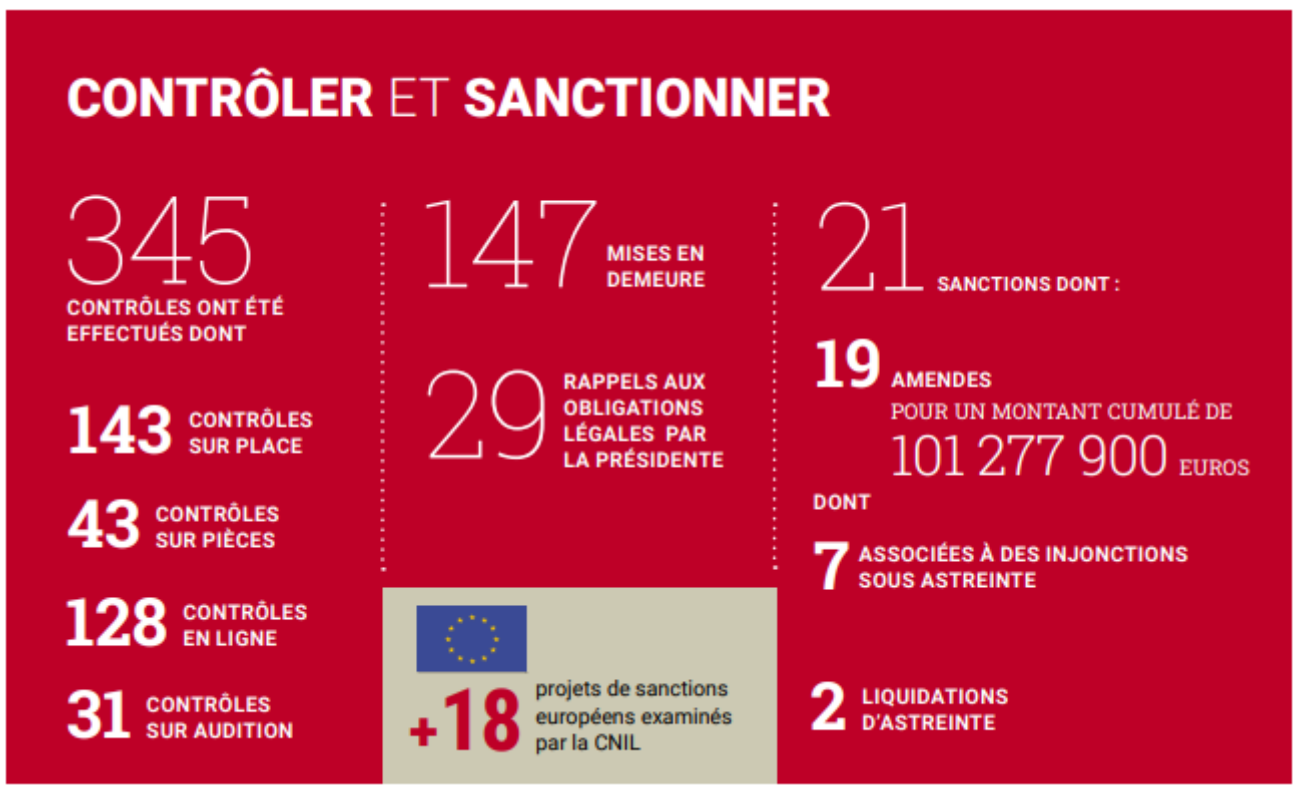
Missions :

- Informer et protéger les droits des personnes.
- Accompagner la conformité des organismes publics et privés, conseiller les pouvoirs publics.
- Anticiper les nouveaux usages et contribuer à l'innovation.
- Contrôler et sanctionner les organismes non conformes au RGPD et à la loi Informatique et Libertés.

Impact de l'application du RGPD vu par la CNIL

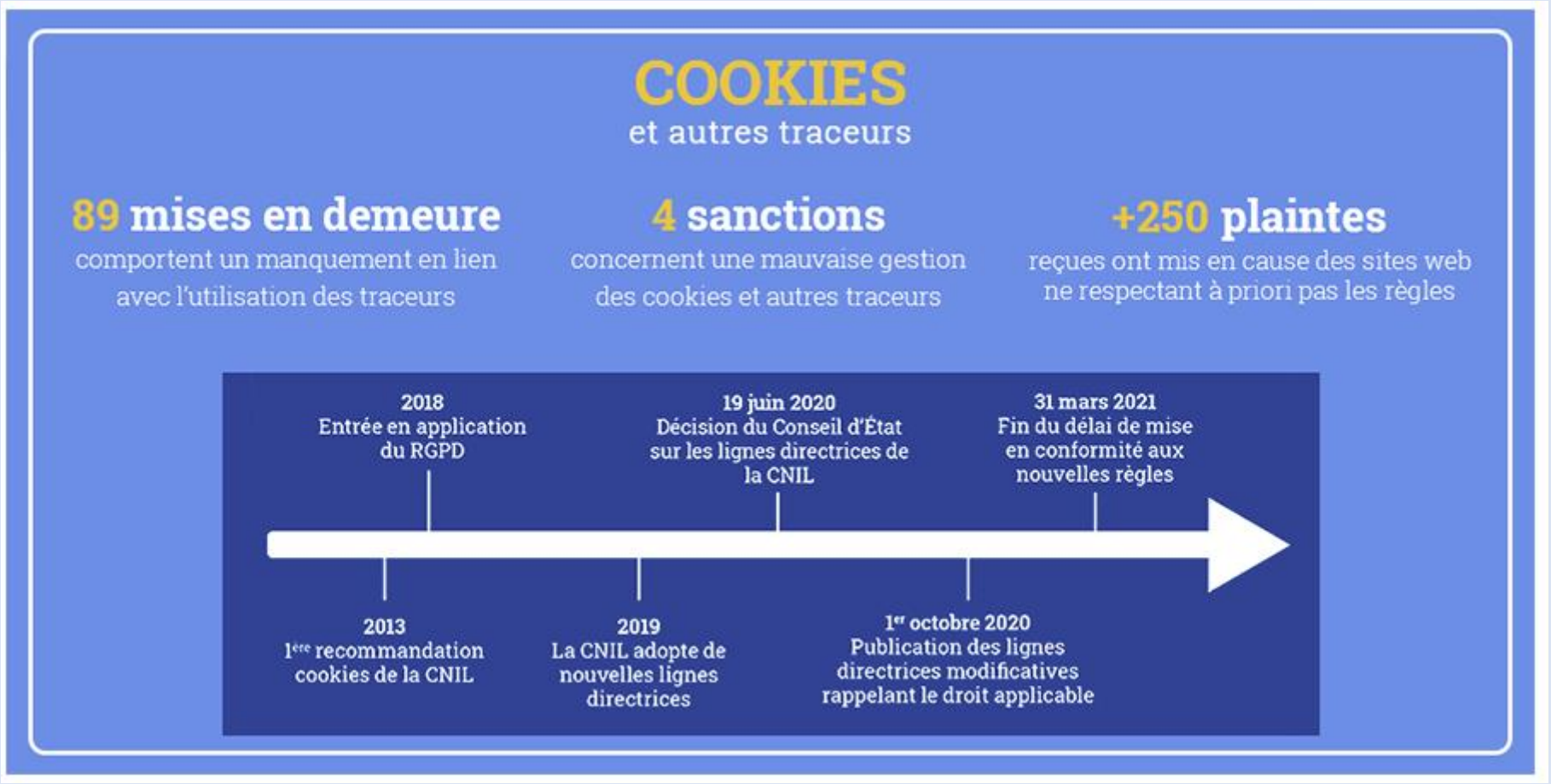
Les sanctions de la CNIL en 2022

En 2022, la CNIL a effectué **345 contrôles** ayant entrainé **147 mises en demeure**, **29 rappels aux obligations** et **21 sanctions**.



Impact de l'application du RGPD vu par la CNIL

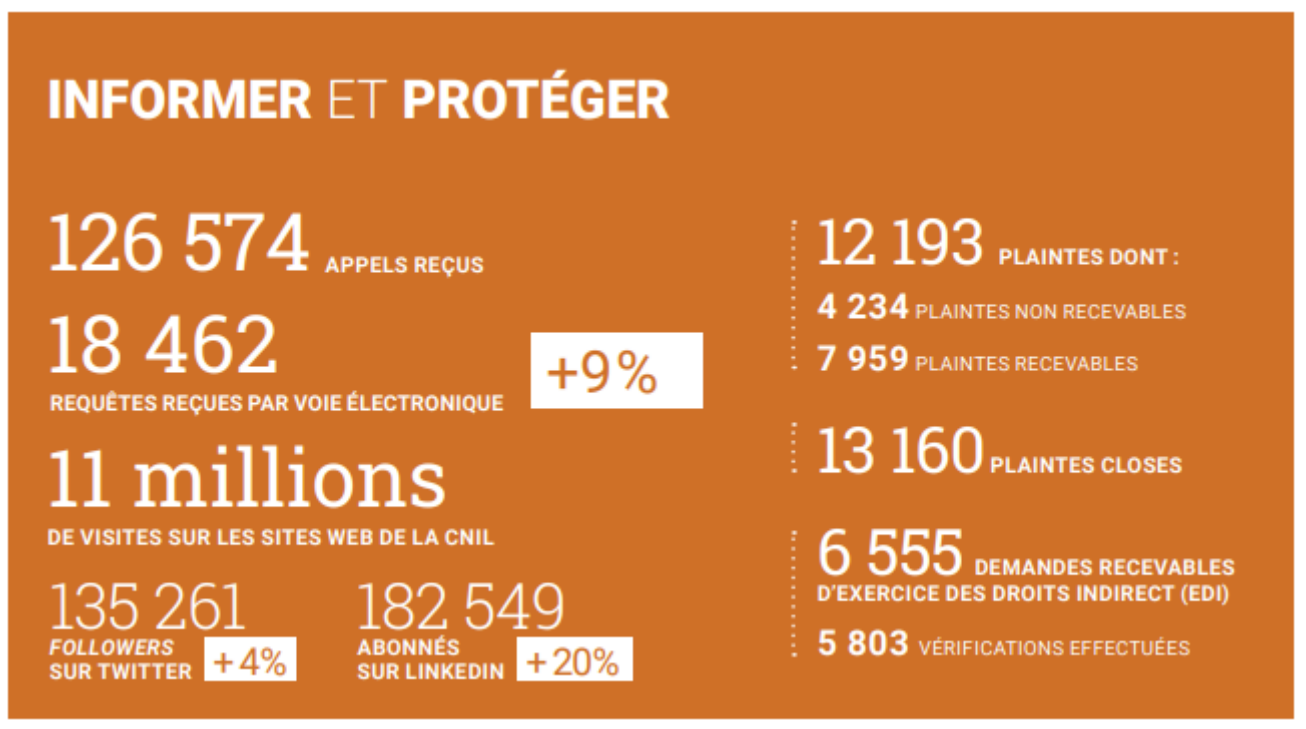
Focus sur les cookies : principal sujet des mises en demeure prononcées



Source : cnil.fr

Impact de l'application du RGPD vu par la CNIL

Les chiffres de la CNIL en 2022



Quelques chiffres en 2023

- **1,2 milliards d'euros** : amende à Meta le 22 mai 2023 pour ne pas avoir respecté le RGPD s'agissant du transfert de données vers les USA

- **345 millions d'euros** : amende à TikTok le 15 septembre 2023 pour avoir rendu publics les nouveaux profils d'adolescents de 13 à 17 ans par défaut.

Quelques chiffres en 2022

- **60 millions d'euros** : amende à Microsoft Ireland le 19/12/2022 en raison de l'inexistence d'un mécanisme permettant à l'internaute de refuser les cookies aussi facilement que de les accepter.

- **20 millions d'euros** : amende à Clearview AI t injonction de cesser de collecter et d'utiliser sans base légale les données des personnes se trouvant en France et de supprimer celles déjà collectées. Cette société aspire des photos de sites web, y compris les réseaux sociaux, puis commercialise l'accès à sa base de données d'images sous forme de moteur de recherche (but : identifier les auteurs ou victimes d'infractions entre autres). Des particuliers se sont plaints au sujet du logiciel utilisé. Une mise en demeure a été envoyée à Clearview, elle est restée sans réponse –> la CNIL a prononcé la sanction la plus importante possible, soit 20 millions d'euros.

- **1 million d'euros** : amende à TotalEnergies, pour manquement aux obligations en matière de prospection commerciale et de droits des personnes. Des personnes se sont plaintes de leurs difficultés à accéder à leurs données et d'opposition à recevoir des appels de prospection commerciale. Les utilisateurs autorisaient l'utilisation de leurs données personnelles pour de la prospection commerciale, sans avoir la possibilité de s'y opposer.

- **800 000 euros** : amende à DISCORD INC. pour manquement aux durées de conservation (2 474 000 comptes non utilisés depuis plus de 3 ans et 58 000 comptes non utilisés depuis plus de 5 ans, avant mise en conformité) et sécurité des données personnelles. DISCORD est un service de voix sur IP et de messagerie instantanée, pour créer des serveurs, salons textuels, vocaux ou audio, sachant que son business model n'est pas fondé sur l'exploitation des données personnelles.

- **600 000 euros** : amende à EDF le 24/11/2022, pour ne pas avoir respecté ses obligations en matière de prospection commerciale et de droits des personnes (consentement préalable pas recueilli).

- **300 0000 euros** : amende à Free le 30/11/2022, pour ne pas avoir respecté les droits des personnes (droit d'accès et droit d'effacement) et la sécurité de leurs données (faible robustesse des mots de passe; stockage et transmission en clair des mots de passe, etc.), à la suite de plaintes de plusieurs personnes qui avaient des difficultés à faire respecter leurs droits.

Quelques cas concrets : objets connectés (source CNIL)

Qu'est-ce qu'un robot de cuisine connecté ?

Un robot de cuisine, ou robot multifonction, est un appareil qui permet d'automatiser certaines tâches culinaires. Il s'adresse à un public de plus en plus large avec une vaste palette de modèles.

Certains modèles sont équipés de fonctionnalités telles qu'une connexion Wi-Fi, qui permet d'accéder à des services en ligne (recettes, mode d'emploi, etc.) ou encore d'un microphone. L'utilisateur est également incité à se créer un compte sur le site web du fabriquant pour bénéficier de services supplémentaires (recettes, conseils, etc.).

Quelles sont les données collectées ?

Comme pour tous les objets connectés, les données qui peuvent être récoltées par un robot de cuisine dépendent des fonctionnalités de celui-ci. Pour les robots, il peut donc s'agir, entre autres, de :

- vos habitudes d'utilisation (cuisine pour famille nombreuse, pour un couple...) ;
- vos habitudes alimentaires (via les recettes choisies) ;
- l'enregistrement de votre voix ou des conversations environnantes ; etc.

Ces données pourraient servir au constructeur ou à ses partenaires commerciaux pour analyser vos habitudes pour vous proposer, notamment, des publicités ciblées selon vos centres d'intérêts. Dans ce cas, **vous devez être informé de l'objectif** de cette réutilisation, de la transmission des données à des partenaires, de la nature, voire l'identité de ces partenaires, etc. Vous devez aussi être mis en mesure **d'accepter ou de refuser** ces opérations.

Quelques cas concrets : objets connectés (source CNIL)

Quelle sécurité pour vos données ?

Un robot disposant du Wi-Fi se connectera à votre réseau informatique domestique, et aura donc accès à l'ensemble des ressources accessibles sur votre réseau (partages de fichier, imprimantes...).

Dans le cas de la présence d'un microphone, même si celui-ci n'est pas actif au moment de l'achat, il peut être activé par la suite par le fabriquant au moyen d'une simple mise à jour, sans que vous en soyez nécessairement informés. Le microphone peut alors enregistrer et transmettre à des tiers des extraits sonores contenant quelques mots voire des phrases entières.

Quels sont les conseils de la CNIL ?

- Renseignez-vous sur les fonctionnalités de l'appareil préalablement à l'achat, que ce soit sur les sites de vente ou sur les forums de discussion.
- Adaptez votre achat à vos besoins réels (les fonctions liées à la connectivité de l'appareil valent-elles le surcoût et le risque pour mes données ?).
- Vérifiez que vous pouvez désactiver de façon physique (par exemple via un bouton sur l'appareil) ou logicielle (par exemple via les réglages de l'appareil) le Wi-Fi, le microphone ou tout autre fonctionnalité que vous n'utilisez pas et qui peut être potentiellement intrusive.

Quelques cas concrets : objets connectés (source CNIL)

Téléviseurs connectés : 67% des téléviseurs vendus en 2018. Proportion grandissante au fur et à mesure des années

Qu'est-ce qu'un téléviseur connecté ?

Un téléviseur connecté, parfois nommé « intelligent » (ou *smart TV*), peut être raccordé à votre réseau informatique domestique pour accéder à des services supplémentaires via Internet (tels que des services de streaming ou des réseaux sociaux).

Quelles données sont collectées ?

Ces téléviseurs intelligents peuvent récolter plusieurs types de données, notamment :

- les programmes que vous regardez, qu'il s'agisse de chaînes classiques ou de services de vidéo à la demande ;
- les autres objets connectés au réseau domestique (enceintes, ordinateurs, consoles de jeux, etc.) ;
- les personnes qui utilisent la télévision (notamment si la télévision ou le service que vous utilisez propose un système de profils).

Certaines données personnelles peuvent également être collectées :

- vos identifiants, courriels, mots de passe, noms, prénoms, dates de naissances que vous saisissez lors de l'inscription en ligne à des services ;
- votre historique de navigation ;
- etc.

Ces données pourraient servir au constructeur ou à ses partenaires commerciaux pour analyser votre consommation de contenu pour vous proposer, notamment, des publicités ciblées selon vos centres d'intérêts. Dans ce cas, **vous devez être informé de l'objectif** de cette réutilisation, de la transmission des données à des partenaires ainsi que de la nature, voire l'identité de ces partenaires, etc. Vous devez aussi être mis en mesure **d'accepter ou de refuser** ces opérations.

Quelques cas concrets : objets connectés (source CNIL)

Les conseils avant d'acheter une TV connectée

- Renseignez-vous sur toutes les fonctionnalités offertes par l'appareil, notamment sur les fiches produits (qui comprennent l'ensemble des fonctionnalités de la TV), ainsi que sur les forums de discussion (qui peuvent proposer des conseils d'achat ou des retours d'autres utilisateurs).
- Vérifiez notamment que le logiciel interne de la télévision est régulièrement mis à jour.
- Si ces téléviseurs sont dotés de microphone ou de caméra, vérifiez que vous pouvez à tout moment les désactiver lorsqu'ils ne vous sont pas utiles (par ex. occultation physique).
- Adaptez votre achat à vos besoins réels et aux objets que vous possédez déjà (tablette, ordinateur, téléphone, etc.).

Les conseils d'utilisation

- À la première configuration du téléviseur, indiquez seulement les informations qui vous semblent nécessaires.
- Si vous connectez ce téléviseur à un réseau Wi-Fi, assurez-vous que ce dernier est correctement sécurisé, notamment avec un mot de passe fort. Ne connectez jamais votre télévision à un réseau Wi-Fi public.
- Pour les télévisions disposant d'une caméra, pensez à la désactiver ou à l'occulter physiquement.
- Désactivez également votre microphone si vous ne l'utilisez pas.
- Vérifiez régulièrement les mises à jour système, des logiciels et du pare-feu de votre télévision.
- Désinstallez régulièrement les applications dont vous ne vous servez plus.
- Si la fonctionnalité est disponible, utilisez un mot de passe fort pour accéder à certaines applications, notamment celles avec lesquelles vous pouvez effectuer des paiements.
- N'enregistrez jamais vos informations bancaires dans les applications.
- Activez le filtrage parental pour protéger les plus jeunes.

Acteurs principaux dans le cadre du RGPD et répartition des rôles

Responsable de traitement et sous-traitant

Responsable de traitement	**Sous –traitant**
→**détermine** à la fois les finalités et les moyens du traitement	→**traite les données** pour le compte du responsable de traitement **sur instructions** documentées uniquement (i.e écrites)
→**donne des instructions** écrites au sous-traitant	→**ne décide pas du traitement**, ne définit ni les finalités ni les moyens

Critères de qualification

	Faisceau d'indices en faveur de la qualification de	
Critères de qualification	**Sous-traitant**	**Responsable de traitement**
Niveau des instructions préalable données par le RT	Instructions sur le niveau de sécurité, modalités de traitement détaillées, directives écrites données au cours de la prestation, présentation d'un niveau d'exigence	Le prestataire a une large autonomie dans la détermination des moyens du traitement ou agit uniquement sur instructions générales de la part de son client
Niveau de contrôle de l'exécution des prestations	Contrôle de la mise en œuvre du traitement en détail par le RT, qui réalise des audits réguliers, demande des comptes sur les opérations	Le RT ne surveille pas la réalisation de la prestation, pas de contrôle ou d'audits. Le prestataire pour utiliser les données pour ses propres besoins.
Transparence	Identité du prestataire non connue des personnes, le droit d'accès s'exerce auprès du RT	Identité du prestataire connue par les personnes, droit d'accès traitées géré par le prestataire.
Expertise	Prestataire utilise infrastructure technique définie ou mise à disposition par le RT	Prestataire est expert dans son domaine, impose la réalisation des opérations de traitement sur son propre système.

Répartition des rôles : exemples

- **Une entreprise qui propose des services de publicité ciblée**

→ Sous-traitant du client si elle traite les données de son client pour assurer la promotion de ses produits

→ Responsable de traitement si l'entreprise décide d'utiliser les données pour promouvoir d'autres produits

- **Mise en œuvre de systèmes intégrés et centralisés de paye au sein d'un groupe de sociétés**

→ La filiale peut être considérée comme responsable de traitement uniquement pour la gestion de la paye sur ses salariés et la société mère pour l'analyse et l'agrégation des données aux fins de détermination de politique de rémunération de groupe

- **Les organismes participant à la réalisation commune d'une enquête statistique**

→ Tous les organismes peuvent être qualifiés de responsable de traitement conjoints, soit pour l'ensemble de l'enquête, soit pour une partie (phase de collecte, phase d'analyse)

Répartition des rôles : exemples

Les autres questions à se poser :

- Pourquoi ce traitement a-t-il eu lieu ?
- Qui a entrepris le traitement?
- Qui dispose d'un pouvoir d'arbitrage sur le traitement ?
- Qui signe les études d'impact sur la vie privée?
- Qui détermine les droits d'accès des personnes concernées?
- Qui fixe la durée de conservation des données?
- Qui peut apporter des correctifs à ce traitement ?
- Qui a élaboré l'algorithme permettant le traitement des données ?

✓ **La qualification doit tenir compte de la complexité et diversité des situations**

✓ **Impossible de la calquer sur la qualité de l'intervenant (prestataire, partenaire, client)**

✓ **Être en mesure de justifier ce choix (parfois commun) auprès de la CNIL pour démontrer sa bonne foi**

✓ **Situation factuelle indépendante de la qualification des parties elles-mêmes**

Responsabilités du responsable de traitement et du sous-traitant

- **Les sous-traitants** se voient conférer des **obligations : endossent désormais une responsabilité propre.**

- **Principe :** Toute personne ayant subi un dommage, matériel ou moral, a le droit d'obtenir du responsable de traitement ou du sous-traitant réparation du préjudice subi.

- **Conditions :**
  - Le responsable de traitement est responsable lorsqu'il viole une obligation du règlement
  - Le sous-traitant est responsable lorsqu'il viole une obligation du règlement qui lui est propre ou lorsqu'il ne respecte pas des instructions du responsable de traitement.
  - Ils sont exonérés, s'ils prouvent que le dommage ne leur est nullement imputable.

- **Responsabilité solidaire :** Lorsqu'ils participent **à un même traitement,** le responsable de traitement et le sous-traitant sont tenus responsables pour **la totalité du dommage.**

→ Permet de garantir à la personne concernée une réparation effective.

- **Recours :** Chacun est en droit de réclamer auprès de l'autre la part de la réparation correspondant à sa part de responsabilité dans le dommage

Droits des personnes concernées

Détail des droits des personnes concernées

- **Droit à l'information** : informer clairement les utilisateurs du traitement et de ses modalités via la politique vie privée rédigée dans un langage clair
- **Droit d'opposition** : pour des motifs légitimes, sauf en cas d'obligation légale du responsable de traitement (ex : fichier des impôts)
- **Droits d'accès et de rectification** : accéder aux informations la concernant, connaître l'origine des informations, obtenir la copie de ces données, demander leur rectification, mise à jour, etc. Délai de réponse d'un mois du responsable de traitement à la suite de la demande
- **Droit à la portabilité** : transfert des données à une autre société
- **Droit d'effacement** de leurs données (dans certains cas)
- **Droit d'opposition** à la prospection/au profilage à des fins marketing
- **Droit à la limitation du traitement** : les personnes ont le droit de demander à ce que le traitement de leurs données soit bloqué pendant un certain temps, par exemple le temps d'examiner une contestation de sa part sur l'utilisation de ses données ou une demande d'exercice de droits.
- **Droit de donner des directives sur le sort de ses données à sa mort** : cas des réseaux sociaux notamment
- Droit d'introduire une **réclamation auprès de la CNIL**

Cas pratique : droit d'information

L'entreprise ABCD se dote d'un système non biométrique d'accès par badge afin de permettre le contrôle des personnes qui entrent dans ses locaux (salariés et visiteurs).

Question : comment les personnes sont-elles informées du traitement et de ses modalités ?

Cas pratique : droit d'information

La société ABCD peut informer les visiteurs en utilisant deux niveaux d'information :

- **Pour le niveau 1,** il est diffusé sur un panneau d'information affiché à proximité du dispositif de contrôle d'accès aux locaux de la société ABCD
- **Pour le niveau 2**, une notice d'information plus complète relative à la gestion des données personnelles et aux droits des personnes doit être mise à la disposition des visiteurs lors de la délivrance de leur badge.

Si la société ABCD adresse des consignes d'accès aux visiteurs avant leur venue, cette notice peut également être envoyée en amont, par courriel, à cette occasion.

Cas pratique : droit d'information

- **Autre option** : la société ABCD peut informer ses salariés sur un support unique.

- Par exemple :

  - ✓ par un courriel à l'attention de l'ensemble du personnel ;
  - ✓ sur une notice, fournie systématiquement à l'embauche du salarié lors de la signature de son contrat de travail.

- Cette information devrait également figurer de manière permanente sur son intranet / règlement intérieur à la rubrique « Politique de protection des données » - Onglet « Accès par badge », pour permettre aux salariés d'exercer leurs droits. A défaut d'un intranet ou de l'existence d'un règlement intérieur, cette information doit pouvoir être fournie, à tout moment, sur demande des salariés adressée à dpo@abcd.fr (ou à securite@abcd.fr en l'absence d'un DPO)

Données sensibles

- Données sensibles : catégorie particulière de données personnelles.

- Informations relatives à la prétendue **origine raciale ou ethnique**, les **opinions politiques**, les **convictions religieuses ou philosophiques** ou l'**appartenance syndicale**, ainsi que le traitement des **données génétiques**, des **données biométriques** aux fins d'identifier une personne physique de manière unique, des données concernant la **santé** ou des données concernant **la vie sexuelle ou l'orientation sexuelle** d'une personne physique.

- Interdiction de principe de traiter ces données.

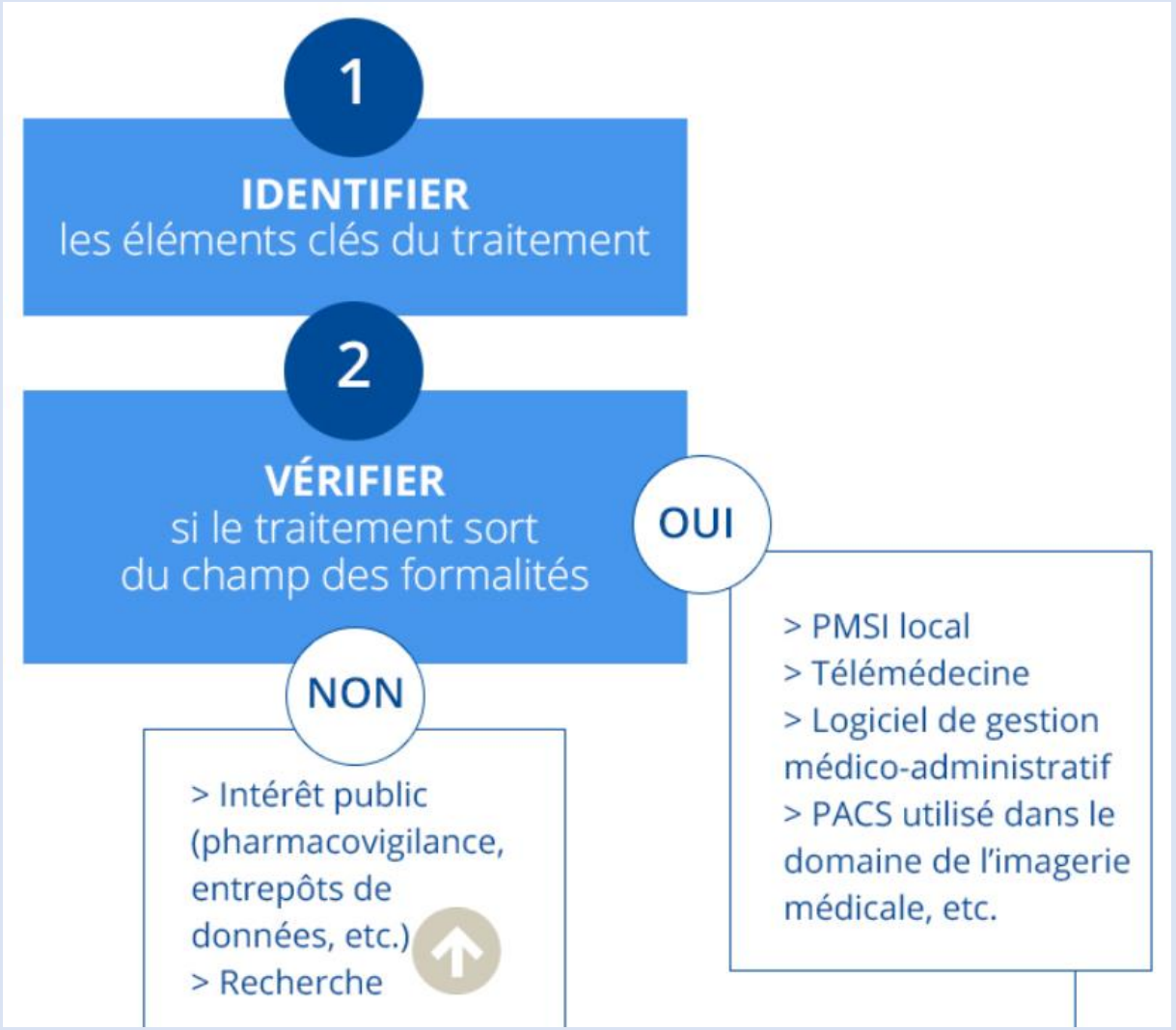
- Exceptions :
  - consentement exprès de la personne ;
  - informations rendues publiques par la personne concernée ;
  - données nécessaires à la sauvegarde de la vie humaine ;
  - utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
  - informations concernant les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique ou syndicale.

Données sensibles : les données de santé

- Définition : élargie depuis le RGPD

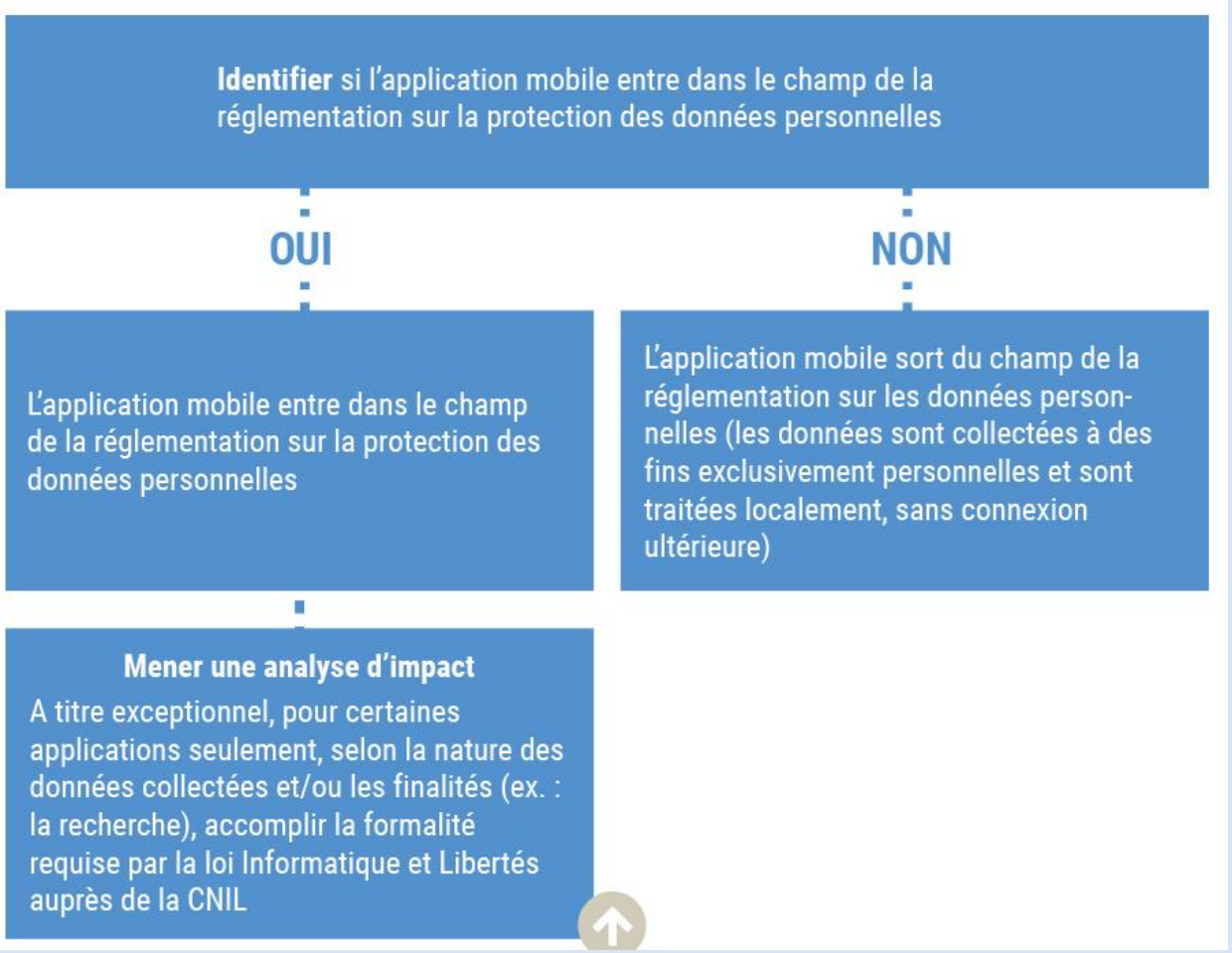
- Comprend l'ensemble des données collectées et produites dans le cadre du parcours de soins mais aussi celles qui, détenues par d'autres acteurs (développeurs d'applications par exemple), constituent une information **sur l'état de santé de la personne**.

Données sensibles : les données de santé



Données sensibles : les données de santé

Mise à disposition d'applications mobiles de santé :



Exemple : non-respect du RGPD en matière de données de santé

- 2 amendes prononcées le 7 décembre 2020 par la CNIL de 3 000 et 6 000 euros à l'encontre de 2 médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL.

- Origine de la violation de données : mauvais choix de configuration de la box Internet + mauvais paramétrage du logiciel d'imagerie médicale (images pas systématiquement chiffrées)

→ Manquement à la sécurité des données

Délégué à la protection des données (DPO)

- Nomination obligatoire si :
  - ✓ Le traitement de données fait partie intégrante de l'activité de l'entreprise
  - ✓ Le traitement a lieu dans le cadre normal des activités d'une société (« grande échelle » : activités de marketing fondées sur les données personnelles collectées, publicité comportementale)
  - ✓ De manière constante suivant un procédé organisé ou un programme général de collecte de données

- Qualités :
  - ✓ un membre du **personnel** de l'entreprise ou **externe à l'entreprise**,
  - ✓ désigné **sur la base de ses qualités professionnelles** : expertise du RGPD, compréhension des traitements effectués, compréhension des technologies de l'information et de la sécurité des données, connaissance du secteur d'activité et de la société, capacité à promouvoir une culture de protection des données au sein de la société,
  - ✓ doté d'un **positionnement efficace en interne** pour être en capacité de faire directement rapport au niveau le plus élevé de la société et animer un réseau de relais au sein des filiales d'un groupe (expert informatique, juriste, expert en communication).

Le DPO a des missions obligatoires, dont l'exécution ne doit pas entraîner de situation de conflit d'intérêts : contrôle du respect du RGPD, contrôle des règles internes de l'entreprise en matière de données personnelles, coopération et point de contact avec l'autorité de contrôle, information des personnes concernées.

Délégué à la protection des données (DPO)

- **Le DPO doit être <u>indépendant</u> et l'exécution de ses missions ne doit pas entraîner de conflits d'intérêts**

  - ✓ le DPO ne peut exercer une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel
  - Ex:
    - directeur général,
    - directeur opérationnel,
    - responsable du département marketing,
    - mais également **responsable du service informatique**.

- **Impossible de transférer au DPO, par délégation de pouvoir, la responsabilité incombant au responsable de traitement.**

  - ✓ toute délégation de pouvoir au DPO reviendrait à lui confier un pouvoir décisionnel sur la finalité et les moyens du traitement, ce qui serait constitutif d'un conflit d'intérêts contraire au RGPD.

  - ✓ le DPO n'est pas responsable en cas de non-respect du règlement, mais c'est bien le responsable de traitement ou le sous-traitant qui doivent s'en assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD.

  - ✓ en cas de poursuites pénales envers la personne morale, c'est le représentant de la société qui sera poursuivi.

Manquements à la législation applicable en matière de données personnelles

Exemple : usage de drones par les forces de police et la gendarmerie

Décision en formation restreinte de la CNIL du 12/01/2021 à l'encontre du Ministère de l'intérieur

Objet : utilisation de drones par les forces de police pendant le confinement pour vérifier le respect des mesures, et par ailleurs pour des missions de maintien de l'ordre.

- Traitement de données personnelles : captation d'images par les drones en haute résolution et capacité de zoom entre 6 et 20 fois. Les personnes sont filmées dans des conditions permettant leur identification (pas de mise en place d'un dispositif de floutage), donc il y a bien traitement de données personnelles

  → l'image constitue donc une donnée personnelle

- Manquements :

  - ***Licéité du traitement*** : lorsque le traitement est mis en œuvre pour le compte de l'Etat, il doit être découler d'une disposition légale et si les risques pour les personnes sont élevés, faire l'objet d'une analyse d'impact. En l'occurrence, pas d'analyse d'impact
    → La CNIL a considéré que le traitement ne répondait pas aux conditions de licéité des traitements de données personnelles

  - ***Information des personnes*** : aucune information relative au traitement de données n'a été fournie aux personnes concernées (un message vocal des drones invitant les personnes à se disperser ne permet pas de remplir les exigences légales liées à cette obligation).

Sanction : rappel à l'ordre, injonction de mise en conformité et publicité de la décision.

Autres exemples

Autres exemples :

- Le **8 octobre 2018** : mise en demeure de l'association « 42 » pour vidéosurveillance excessive. Des caméras filmaient en permanence les espaces de travail et lieux de vie, et images accessibles sur l'intranet (*déc. n° MED 2018-041, 8 oct. 2018*)

- Le **15 septembre 2021 :** sanction de 3 000 euros de la Société nouvelle de l'annuaire français pour non-respect des droits des personnes concernées, en ne prenant pas en compte les demandes d'effacement ou de rectification des données personnelles. Cette sanction prend en compte la taille et la situation financière de la société. La publicité de la décision se justifier par l'importance de traiter les demandes de rectification et d'effacement.

Encore quelques exemples

➢ **<u>Première mise en demeure publique de la CNIL se fondant sur le RGPD (Singlespot).</u>**

Absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire. Singlespot avait recours à des outils techniques dénommés « SDK » installés dans des applications mobiles (*MED-2018-043 du 8 octobre 2018*).

Les fondements :

- **<u>défaut d'information</u>** : la seule mention du nom du responsable de traitement dans les politiques de confidentialité des applications de ses partenaires sans information des finalités du traitement et des droits des personnes.
- **<u>défaut de consentement spécifique</u>** : l'utilisateur devait accepter un bloc de finalités.
- **<u>défaut de consentement univoque</u>** : le seul choix laissé à l'utilisateur entre « j'accepte » et « plus tard » ne lui permettait pas de refuser la collecte.
- **<u>durée de conservation disproportionnée aux finalités du traitement</u>**: données de géolocalisation conservées 13 mois, couplées avec les centres d'intérêts et identifiants publicitaire (identifiant du terminal de l'utilisateur de façon stable) conservé 13 mois.
- **<u>manquement à la sécurité des données</u>:** du fait de l'utilisation de données personnelles réelles pendant les phases de test et de développement.

La procédure a été <u>clôturée</u> le 29 novembre 2018, la société s'étant mise en conformité avec le RGPD

➢ **Les sociétés FIDZUP et TEEMO avaient également été mises en demeures** le 25 juin 2018 sur les mêmes fondements selon le droit applicable au 7 juin 2017 et 11 janvier 2018 (dates des opérations de contrôle). **Les procédures ont été clôturées, les sociétés s'étant depuis « mises en conformité avec le RGPD ».**

Suite des exemples

➢ **<u>Première sanction par la CNIL sur le fondement du RGPD</u> (21 janvier 2019**) sanction de **50 millions d'euros** à l'encontre de la société **GOOGLE LLC.**

Cette sanction intervient suite aux plaintes collectives des de l'association None Of Your Business (« NOYB ») et de l'association La Quadrature du Net.

La CNIL a constaté <u>deux séries de manquements</u> au RGPD :

- **Un manquement aux obligations de <u>transparence et d'information</u>** : la CNIL relève que les informations essentielles fournies par GOOGLE (telles que les finalités pour lesquelles les données sont traitées, la durée de conservation des données ou les catégories de données utilisées pour la personnalisation de la publicité) ne sont pas aisément accessibles pour les utilisateurs et ne sont pas toujours claires et compréhensibles.

- **Un manquement à l'obligation de <u>disposer d'une base légale</u> pour les traitements de personnalisation de la publicité** : la CNIL estime que le consentement des utilisateurs n'est pas suffisamment éclairé et qu'il n'est pas « spécifique » et « univoque ».

La CNIL précise enfin que cette sanction prend notamment en compte l'ampleur des traitements en cause, le fait qu'il s'agit de violations continues, la place prépondérante qu'occupe le système d'exploitation Android sur le marché français et le modèle économique de la société qui repose en partie sur la personnalisation de la publicité.

→ La sanction prononcée sur le fondement du RGPD à l'encontre de Google est 125 fois supérieure à la sanction la plus élevée rendue par la CNIL en 2018 (400 000 euros - UBER).

➢ **Le 28 mai 2019**, autre sanction sur le fondement du RGPD : sanction de **400 000 euros** sur le fondement du RGPD à l'encontre de la société **SERGIC** pour avoir insuffisamment protégé les données des utilisateurs de son site web et mis en œuvre des modalités de conservation des données inappropriées.

Durée de conservation des données personnelles

« Cycle de vie » d'une donnée personnelle

- **Conservation en base active** : durée nécessaire à la réalisation de l'objectif poursuivi (finalité du traitement) = données facilement accessibles aux services qui en ont besoin

  Exemple : données d'un candidat non retenu conservées pendant 2 ans maximum par le service des ressources humaines.

- **Archivage intermédiaire** : les données ne sont plus utilisées pour réaliser l'objectif mais qui conservent un intérêt pour l'organisme ou relèvent d'une obligation légale

  Exemple : gestion de contentieux, données de facturation pendant 10 ans

« Cycle de vie » d'une donnée personnelle

- **Archivage définitif** : archivage de façon définitive et pérenne

= les deux dernières étapes ne sont pas obligatoires : évaluation selon les traitements concernés. Tri opéré entre les données.

- Détermination de la durée de conservation :
  - ❑ par le responsable de traitement au regard de l'analyse conformité
  - ❑ par la règlementation, exemple : le code du travail impose la conservation du bulletin de salaire du salarié pendant 5 ans

« Cycle de vie » d'une donnée personnelle

- En pratique : pour de nombreux traitements de données, pas de durée de conservation fixée par un texte.

- Donc durée à fixer par le responsable du fichier de données personnelles (cf. référentiels CNIL notamment)

- <u>Questions à se poser pour fixer la durée de conservation :</u>

  - Jusqu'à quand ai-je vraiment besoin des données pour atteindre l'objectif fixé ?
  - Ai-je des obligations légales de conserver les données pendant un certain temps ?
  - Dois-je conserver certaines données en vue de me protéger contre un éventuel contentieux ? Lesquelles ?
  - Jusqu'à quand puis-je faire valoir ce recours en justice ?
  - Quelles informations doivent être archivées ? Pendant combien de temps ?
  - Quelles sont les règles de suppression des données.
  - Quelles sont les règles d'archivage des données ?

Exemples de manquements en matière de durée de conservation

- **Sanction de la société PERFORMECLIC le 7 décembre 2020** : plusieurs fondements, dont notamment la durée de conservation.

- Contexte : TPE avec 2 salariés. Activité : envoi de prospection commerciale par courrier électronique pour le compte d'annonceurs.

- Suite à une information de l'association SIGNAL SPAM (réception de signalements d'internautes), la CNIL a procédé à un contrôle et a identifié plusieurs manquements.

Exemples de manquements en matière de durée de conservation

- Concernant la durée de conservation : conservation de données de prospects pendant une durée excessive, à savoir plus de trois ans à compter de la simple ouverture des courriels de prospection, sans une autre action de la part des personnes concernées (par exemple sans clic sur un des liens présents dans les courriels de prospection)

- **Amende de 7 300 euros** : la CNIL a pris en compte la taille de l'entreprise et sa situation financière pour prononcer une amende dissuasive et proportionnée.

Sécurité des données personnelles

Objectifs

- **Sécurité de l'information :**

  → protection de l'organisme des atteintes relatives à son patrimoine informationnel

- **Protection de la vie privée :**

  → protection des personnes des atteintes liées à leurs données personnelles

Ces objectifs sont complémentaires et devraient être menés en parallèle.

Niveau 1 : 12 règles essentielles pour une entreprise (établies par l'**ANSSI** : Agence nationale de la sécurité des systèmes d'information, et la **CPME** : confédération des PME)

- Règle 1 : choisir avec soin ses mots de passe
- Règle 2 : mettre à jour régulièrement les logiciels
- Règle 3 : bien connaître ses utilisateurs et ses prestataires
- Règle 4 : effectuer des sauvegardes régulières
- Règle 5 : sécuriser l'accès wi-fi de l'entreprise
- Règle 6 : être aussi prudent avec son smartphone et sa tablette qu'avec son ordinateur
- Règle 7 : protéger ses données lors de ses déplacements
- Règle 8 : être prudent lors de l'utilisation de sa messagerie
- Règle 9 : télécharger ses programmes sur les sites officiels des éditeurs
- Règle 10 : être vigilant lors d'un paiement sur internet
- Règle 11 : séparer les usages professionnels des usages personnels
- Règle 12 : prendre soin des informations personnelles, professionnelles et de son identité numérique

Règles et plus encore à retrouver dans le guide publié par l'ANSSI et la CPME :
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

Niveau 2 : mesures d'hygiène pour protéger le SI

Principes :

- sécurité proportionnée aux risques : plus de protection pour les données médicales que pour un fichier de parents d'élèves
- notion de risques :
  - accès non autorisés
  - modifications non désirées
  - disparitions de données
- source des risques : interne, externe, accidentelle ou délibérée (employés, concurrents, pannes, sinistres (inondations ou incendies, etc.)
- bonnes pratiques : pseudonymisation, chiffrement, etc.

→ mesures insuffisantes en cas de risque élevé pour les droits et libertés des personnes

Niveau 3 : protéger les données sensibles de façon spécifique

Questions à se poser :

- Quels pourraient être les impacts sur les personnes concernées en cas :
  - ❑ d'accès illégitime à des données ?
  - ❑ de modification non désirée de données ?
  - ❑ de disparition de données ?

- Qui (ou quoi) pourrait être à l'origine de telles violations (sources de risques) ?

- Comment chacune de ces violations pourrait-elle arriver ?

- Quelles mesures (de prévention, de protection, de détection, de réaction…) devrait-on prévoir pour réduire ces risques à un niveau acceptable ?

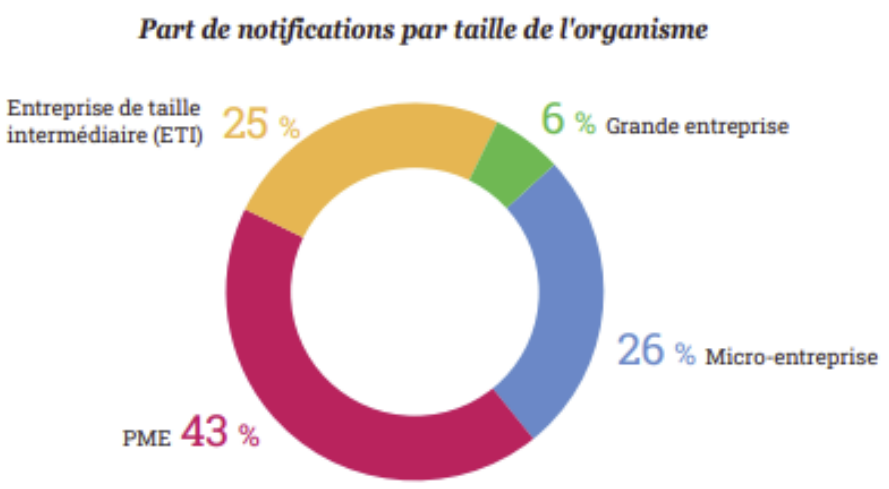
- Serait-ce grave (compte tenu des mesures existantes ou prévues) ?

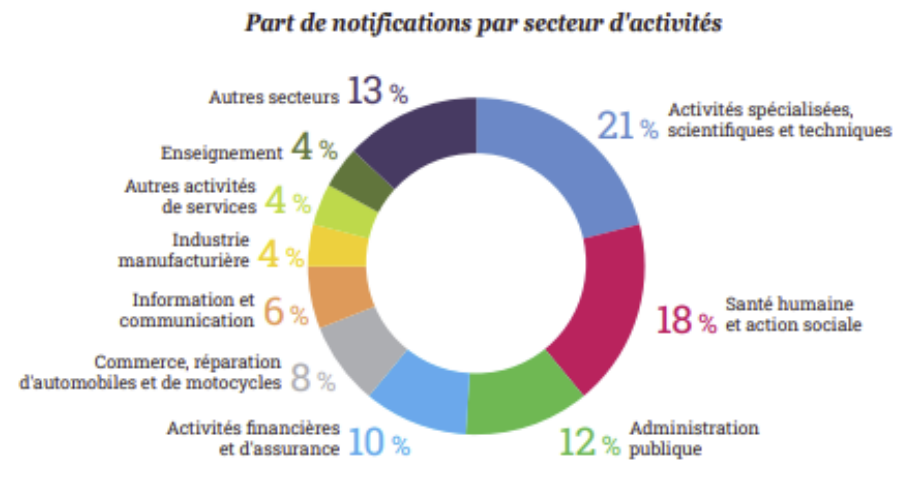
- Serait-ce vraisemblable (compte tenu des mesures existantes ou prévues) ?

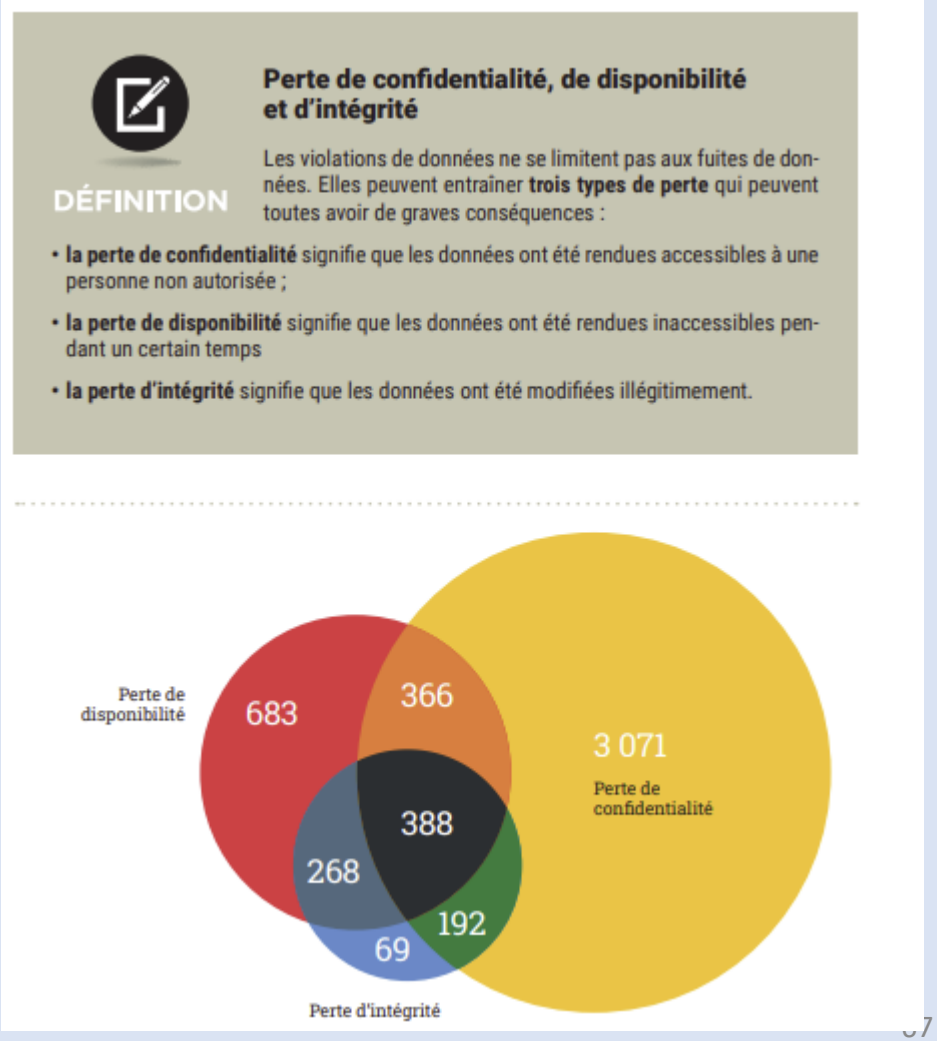
Notifications de violations de données personnelles

En chiffres

En 2021, la CNIL **a reçu 5 037 notifications (+ 79% par rapport à 2020, qui avait connu 2 821 notifications)** de violations de données.







Notification et information

- **La violation de données personnelles entraîne** :

➢ de manière accidentelle ou illicite la perte de données à caractère personnel conservées

➢ l'accès non autorisé à de telles données

- **La notification** :

❑ doit être faite à l'autorité de contrôle compétente dans un délai de 72h, s'il existe un risque pour les droits et libertés des personnes concernées.

❑ le risque se détermine selon : un dommage physique, matériel, une perte de contrôle sur les données, une limitation des droits des personnes, un vol ou une usurpation d'identité etc.

❑ en cas de risque élevé pour les droits et libertés de personnes, le responsable de traitement doit, dans les meilleurs délais, en informer les personnes concernées (description de la nature de la violation, recommandations pour atténuer les effets négatifs etc.).

➢ L'appréciation du risque se fait au regard:

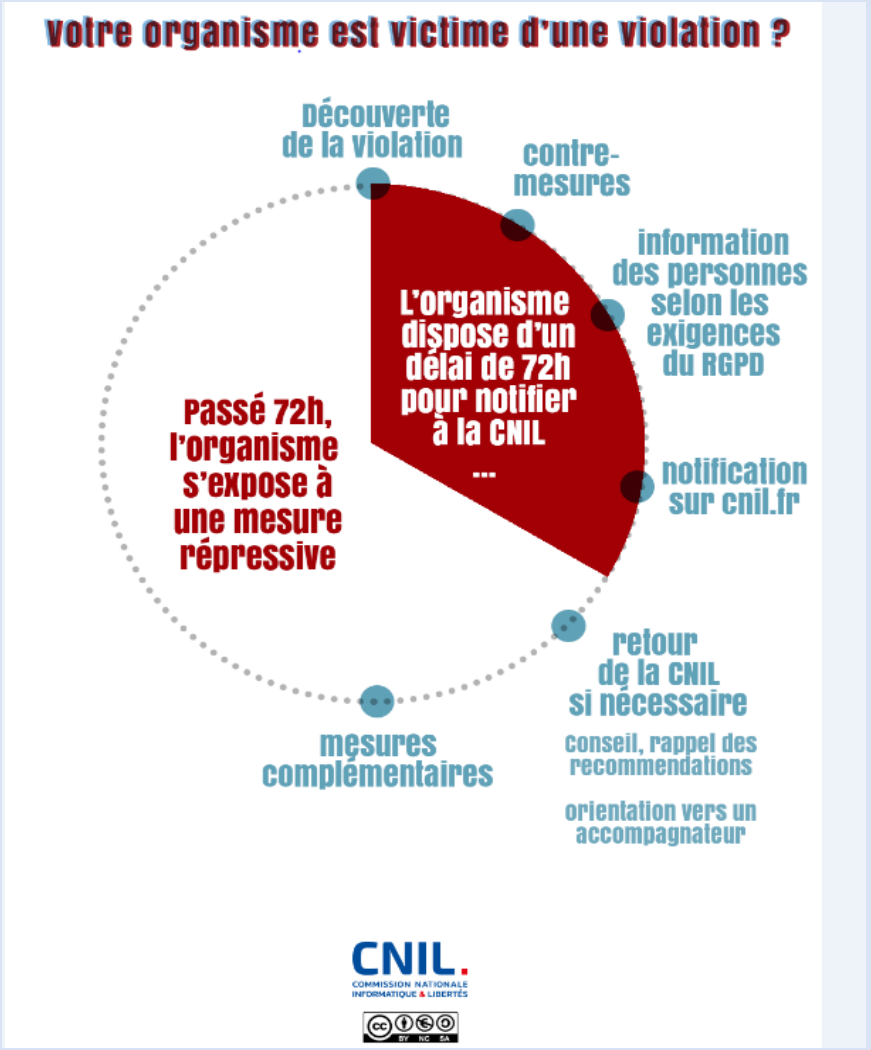
- Du type de données ;
- De la nature, la sensibilité et le volume des données ;
- De la facilité avec laquelle les personnes concernées peuvent être identifiées ;
- De la sévérité des conséquences de la violation pour les personnes concernées;
- Du nombre de personnes concernées ;
- Des caractéristiques spécifiques des personnes concernées et du responsable de traitement.

- **Il convient d'inscrire la violation des données dans le registre du traitement dans tous les cas.**

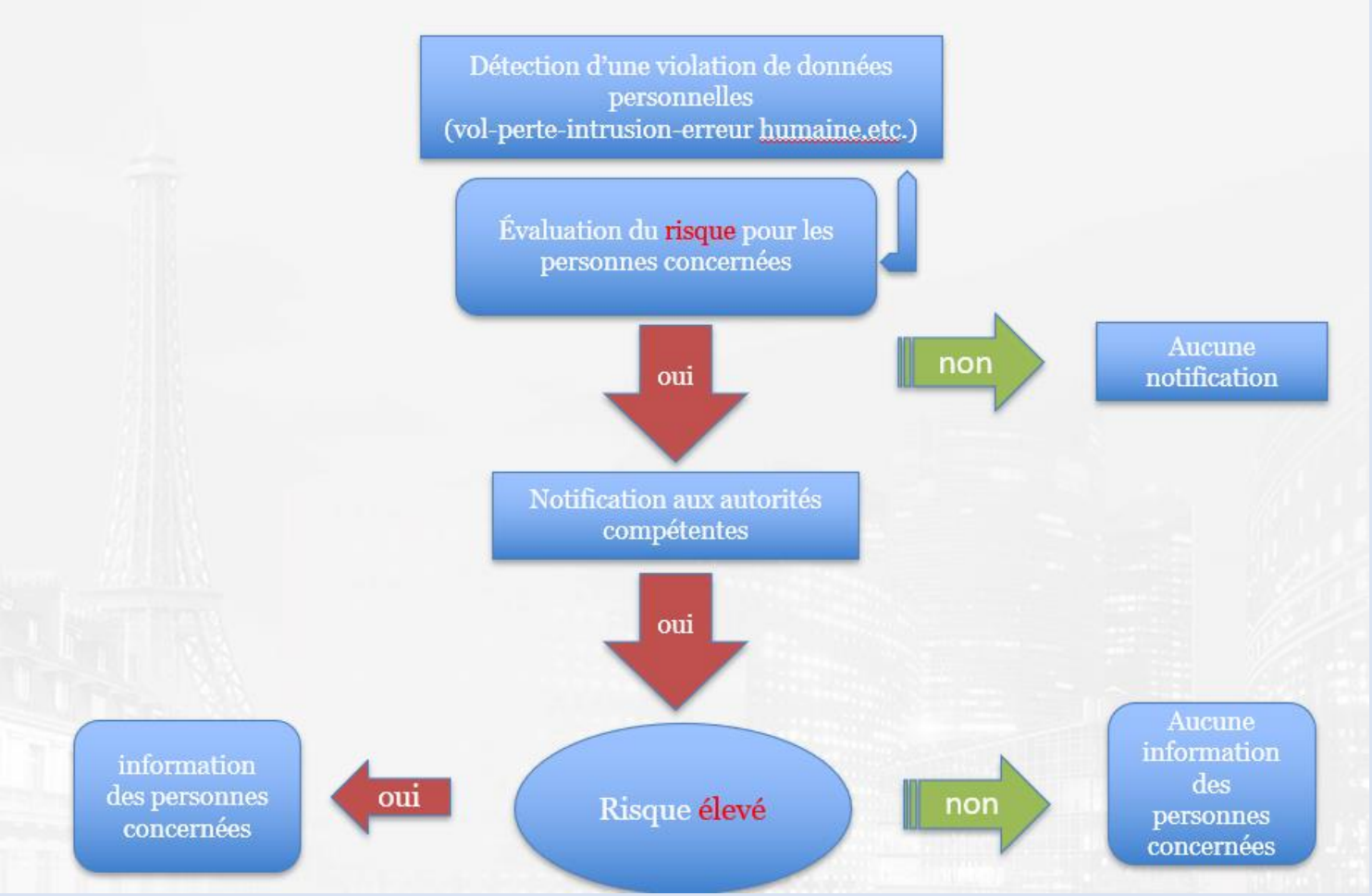
Modalités des notifications de violations de données personnelles

- Des sanctions sont possibles en cas d'absence de notification dans un délai de 72h.

- La CNIL peut mettre en demeure un responsable de traitement de notifier une violation de données aux personnes concernées.



Processus des violations de données personnelles



En toute hypothèse : Inscription de la violation au registre

Exemple 1 : en matière de notification de violation de données personnelles

Perte ou vol d'un matériel informatique contenant des données à caractère personnel : les données concernent plus de 1 000 clients ou utilisateurs et sont relatives à l'état civil, aux coordonnées voire aux données d'identification ou d'accès (identifiant, mot de passe):

- ✓Il y a un risque pour les droits et libertés des personnes concernées en ce qu'elles peuvent subir une perte de contrôle sur leurs données. Ce risque nécessite qu'une notification soit faite à l'autorité de contrôle.

- ✓Ce risque est négligeable si les personnes concernées ne sont pas vulnérables, les données traitées ne relèvent pas de la catégorie des données sensibles. Le responsable de traitement peut estimer qu'il n'y a pas de risque élevé, et donc ne pas informer les personnes concernées.

- ✓L'autorité de contrôle pourra prendre contact avec le responsable de traitement et si elle l'estime nécessaire, lui enjoindre, sous astreinte (100 000 euros) de procéder à l'information des personnes concernées.

Exemple 2 : récupération de numéros de CB par injection SQL sur un site e-commerce

Aspects pratiques : que faire en cas d'attaque de ce type ?

- **Etape 1** : informer les personnes concernées, dès lors l'accès illégitime à des informations bancaires fait courir un risque important. Il faut donc informer les personnes pour qu'elles puissent prendre des mesures de leur côté :

  - ❑ modifier leur mot de passe associé à leur adresse courriel sur le site victime ;
  - ❑ modifier leur mot de passe sur les autres sites où les mêmes identifiants et mots de passe seraient utilisés ;
  - ❑ faire opposition à leur carte bancaire, afin de rendre les données subtilisées inopérantes.

Aspects pratiques : que faire en cas d'attaque de ce type ?

- **Etape 2** : le responsable de traitement doit documenter la violation et notifier la CNIL

  - ❑ enregistrer la violation dans son registre des violations
  - ❑ notifier la CNIL dans un délai de 72h
  - ❑ possibilité de déposer une plainte auprès des autorités compétentes (police, gendarmerie), avec toutes les informations dont il dispose.

Aspects pratiques : que faire en cas d'attaque de ce type ?

- **Etape 3** : prévenir les attaques en réalisant des audits réguliers des sites internet afin d'identifier les vulnérabilités et les combler. Les failles les plus classiques concernent :

  - ❑ vulnérabilité à l'injection SSL
  - ❑ répertoires disponibles en écriture
  - ❑ mots de passe hachés avec MD5 sans sel

  → Un enchaînement de petites vulnérabilités peut suffire à ce qu'une attaque réussisse, il faut donc les anticiper le plus possible.

Exemple 3 : attaque par credential stuffing (bourrage d'identifiants) sur un site web

- Définition : soudaine et très forte affluence, liée à un grand nombre de requêtes envoyées aux serveurs d'authentification des clients.

- NB : le credential stuffing est différent d'une attaque par force brute (bruteforce attack), dans le cadre de laquelle l'attaquant va essayer des combinaisons de mots de passe à partir de « dictionnaires » ou en utilisant les mots de passe les plus simples (« 123456 », « azerty », etc.).

Mode opératoire d'une attaque par credential stuffing

La violation du trimestre

Le *credential stuffing*

1. Des listes d'identifiants et de mots de passe sont publiées, généralement suite à une violation de données.

2. L'attaquant récupère ces listes, en partant du principe que les utilisateurs se servent souvent du même mot de passe et du même identifiant (l'adresse courriel) pour différents services.

3. Par l'intermédiaire de « robots », l'attaquant cible des sites souvent peu sécurisés et tente une grande quantité de connexions.

Les sites peu sécurisés peuvent avoir des difficultés à distinguer un robot d'un véritable utilisateur.

4. L'attaquant, qui a réussi à se connecter à un compte, peut alors changer de mot de passe pour que l'utilisateur ne puisse plus utiliser son compte, faire des achats (si la carte bancaire est enregistrée), etc.

Aspects pratiques : que faire en cas d'attaque de ce type et comment s'en prémunir ?

- **Etape 1** : comprendre l'origine de l'attaque et limiter ses effets
  - ❑ organiser une cellule de crise (DPO, DSI, RSSI, etc.) : communication avec les équipes internes et externes
  - ❑ analyser les journaux d'accès et bloquer les flux suspects
    - ✓ Analyse régulière des logs pour repérer les usages suspects
    - ✓ Limiter le volume du trafic réseau : limitation du flux pour les IP des zones identifiées comme suspectes, mise en place d'un captcha pour limiter les flux suspects

- **Etape 2** : informer les personnes concernées
  - ❑ le service peut envoyer une alerte aux utilisateurs dès qu'un terminal inconnu se connecte (ex : Netflix, applications bancaires) : le site peut proposer la suspension immédiate possible + changement du mot de passe si nécessaire + possibilité de faire opposition à sa CB

Aspects pratiques : que faire en cas d'attaque de ce type et comment s'en prémunir ?

- **Etape 3** : documenter et notifier la violation à la CNIL (enregistrement dans le registre des violations + notification dans les 72h)

- **Etape 4** : se prémunir contre ce type d'attaque
  - ❑ utiliser une connexion multifacteurs : renseigner l'identifiant et le mot de passe + confirmation par un code envoyé par SMS par exemple
  - ❑ veille des équipes sur les méthodes d'attaques afin d'adapter les mesures et de prévoir un dispositif de défense efficace
  - ❑ mesures de sécurité type captcha et couple identifiant / mot de passe avec un identifiant qui n'est pas l'adresse mail de l'utilisateur.

Processus de sanction de la CNIL

Signalement

- Plaintes (signalements sur le site de la CNIL)
- Auto-saisine : par rapport à des thèmes identifiés comme prioritaires
- Presse : faits remontés par la presse ou le web
- Coopération : signalements reçus d'autres CNIL européennes

Types de contrôles

- **Sur place** : accès aux traitements de données personnelles
- **En ligne** : manquements identifiables en ligne
- **Sur convocation** : audition des acteurs concernés
- **Sur pièces** : questions écrites et demande de documents

Suites des contrôles

- **Pas / peu de manquements :**
  - ❑ clôture du contrôle et envoi d'un courrier

- **Manquements sérieux** :
  - ❑ Présidente peut adresser une mise en demeure : délai de 6 à 12 mois pour se conformer
    - ➢ Si mise en conformité dans les délais : clôture
    - ➢ Sinon : sanction
  - ❑ une plainte peut également aboutir à une mise en demeure sans passer par un contrôle préalable
  - ❑ formation restreinte : possibilité de sanction directement, sans mise en demeure préalable

Publicité des mises en demeure et sanctions de la CNIL

- Publicité des mises en demeure :
  - ❑ non publique
  - ❑ publique : communiqué sur les sites de la CNIL et Legifrance

- Publicité des sanctions :
  - ❑ publique
  - ❑ non publique : communiqué sur les sites de la CNIL et Legifrance
  - ❑ pécuniaire : maximum 4% du CA mondial ou 20 millions d'euros
  - ❑ non pécuniaire : rappel à l'ordre, injonction sous astreinte, etc.