RGPD Niveau I
NOTIONS FONDAMENTALES

SOMMAIRE

Qu’est ce que le RGPD ?

Le RGPD est le règlement **européen** portant sur la protection des données personnelles.

Il encadre la mise en œuvre des **traitements de ces données**.

Il fixe les **conditions** dans lesquelles de telles données peuvent être **légalement collectées, conservées et exploitées** par les différents organismes.

Ces conditions visent à éviter que l’utilisation des informations en cause ne **porte atteinte aux droits et libertés** des personnes qu’elles concernent.

Qu’est-ce qu’une « donnée à caractère personnel » ?

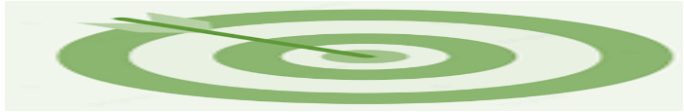
Article 4 RGPD

- **Point 1** Données « **directement identifiables** » (associées à un élément indiquant clairement l’identité de la personne)
  - Fiches de paye, relevés de comptes bancaires, factures, devis, fichiers clients etc…
- **Point 2** Données « **indirectement identifiables** »
  - (les noms et prénoms sont remplacés par des identifiants, des numéros de client, des numéros de téléphone…)
  - En revanche, si ces données sont associées à un autre fichier (par exemple un fichier client) : les données sont susceptibles de devenir des données « **directement** identifiables ».
- **Point 3 Combinaisons d’informations**
  - La combinaison de plusieurs informations peut parfois permettre d’identifier la personne, alors que prises isolément, c’est impossible.

A NOTER ! On peut retrouver des données à caractère personnel sur **différents supports** :

- Une note, un post-it, un document papier, un fichier informatique, une photo, une vidéo, un enregistrement audio etc…

Qu’est-ce qu’un « traitement » ?



- **Article 4 RGPD**

« Toute opération ou tout ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données ».

- La simple **consultation d’un fichier** comportant des données personnelles est considérée comme un « traitement ».

- La notion de traitement s’applique également aux **documents papier**.

- **Exemple d’autres traitements :**
  - Collecte, enregistrement, conservation (hébergement), transmission, modification, extraction, communication, mise à disposition, rapprochement, etc…

La législation : LES GRANDES DATES

1978 *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*
dite : **Loi Informatique et Libertés (LIL) : pour la protection :**

- des données nominatives,
- de la liberté individuelle,
- de l'identité de la personne.

+ Création de la Commission Nationale de l'informatique et des Libertés **(CNIL),**
autorité de contrôle indépendante des pouvoirs publics.

1995 **Directive européenne du 24 octobre 1995** reprend les concepts de la Loi Française pour un socle commun à tous les pays de l'UE. Les pays membres doivent se doter d'une « CNIL »

2004 **:** Réforme de la Loi Informatique et Libertés :

- « *données nominatives* » **deviennent** « *données* ***à*** *caractère personnel* » (plus large)
- la protection s'étend au « papier »
- CNIL : investie d'un **pouvoir de sanctions.**

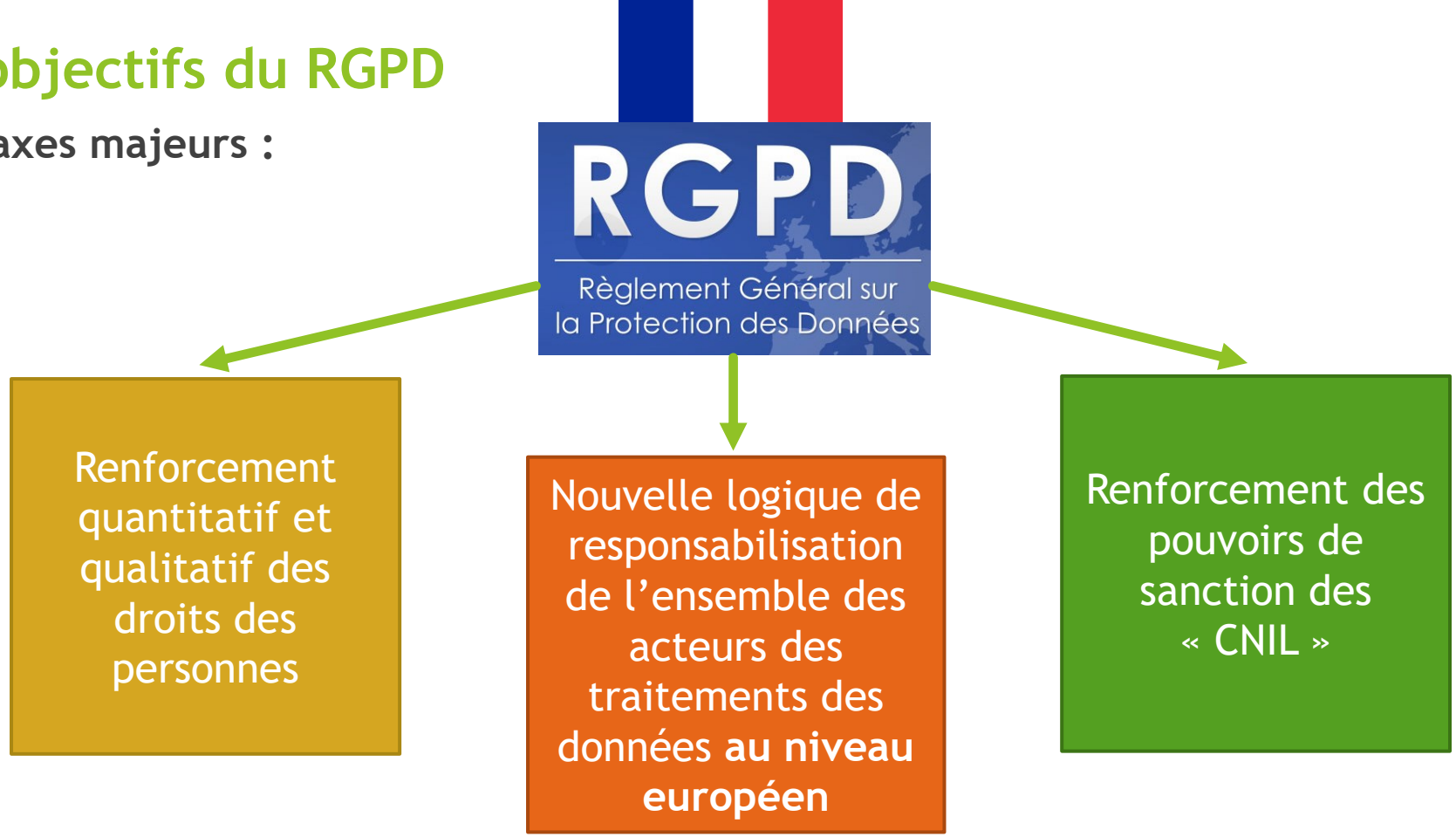
2018 * : RGPD

- Entrée en vigueur du nouveau règlement européen dans l'ensemble des pays de l'UE **- Chaque pays conserve sa propre législation en la matière (exemple en France la loi Informatique et Libertés : LIL) transposant dans celle-ci les grands principes du RGPD.**

** 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/CE, dispositions, entré en vigueur dans l'ensemble des 27 États membres de l'Union européenne à compter du 25 mai 2018.*

Les objectifs du RGPD

- 3 axes majeurs :



Le RGPD garantit un niveau de sécurité adéquat aux informations traitées et donne aux personnes la possibilité de mieux comprendre et de mieux contrôler l'usage qui est fait de leurs données.

Le but est donc de générer la confiance des usagers des secteurs publics et privés et de limiter le risque contentieux.

Quel organisme est concerné par le RGPD ?

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

  - Les **entreprises privées** quelle que soit leur taille,

  - Les **administrations** (d'état, hospitalières, territoriales),

  - Les **associations**.

  - **Exception domestique** : Dans la sphère privée, les données personnelles peuvent être utilisées pour un usage strictement personnel (exemple : répertoire de contacts sur un téléphone). Mais ici le code civil s'applique (article 9 : droit au respect de la vie privée).

Quel organisme est concerné par le RGPD ?

Les règles :

S'applique à toutes les structures dont l'offre de biens et/ou de services cible des personnes qui se trouvent **sur le territoire de l'UE, même si leur siège social se trouve en dehors de ses frontières**

S'applique aux organismes qui traitent **depuis le sol d'un Etat membre de l'UE des données de personnes physiques quelle que soit leur nationalité**

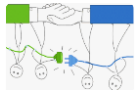
QUIZ : OUI ou NON ?

- **Une entreprise Japonaise vend un logiciel à un étudiant Italien travaillant à Rome. L'entreprise Japonaise est-elle soumise au RGPD ?**
  - La réponse est **OUI** : L'entreprise Japonaise vend des services à un ressortissant de l'Union Européenne qui habite au sein de l'Union Européenne. Le RGPD s'applique.
  - **Une entreprise Japonaise met en œuvre un dispositif de gestion du personnel de ses salariés au Japon parmi lesquels figurent des expatriés italiens. Ce traitement est-il soumis au RGPD ?**
  - La réponse est **NON** : L'entreprise Japonaise est établie hors de l'Union Européenne. L'expatrié de l'Union Européenne est soumis aux règles du pays d'accueil : Le Japon puisqu'il a quitté les frontières de l'Union Européenne. L'entreprise Japonaise n'est soumise au RGPD que si la « cible » est une personne résidant sur le sol Européen.
- **Une entreprise Italienne vend de l'huile d'olive au Japon. L'entreprise Italienne est-elle soumise au RGPD ?**
  - La réponse est **OUI** : L'entreprise Italienne est basée sur le sol de l'Union Européenne. Elle est soumise au RGPD au même titre que toutes les autres entreprises européennes, même si ses clients sont hors du territoire européen.

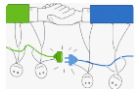
Qui sont les autorités assurant le respect du RGPD ?

- 3 acteurs complémentaires :

- La CNIL (Commission Nationale de l'Informatique et des Libertés) :
  - Autorité administrative indépendante Française. Régulateur des données personnelles. Accompagne, informe, protège, contrôle les professionnels et les particuliers. Pouvoirs de sanctions.



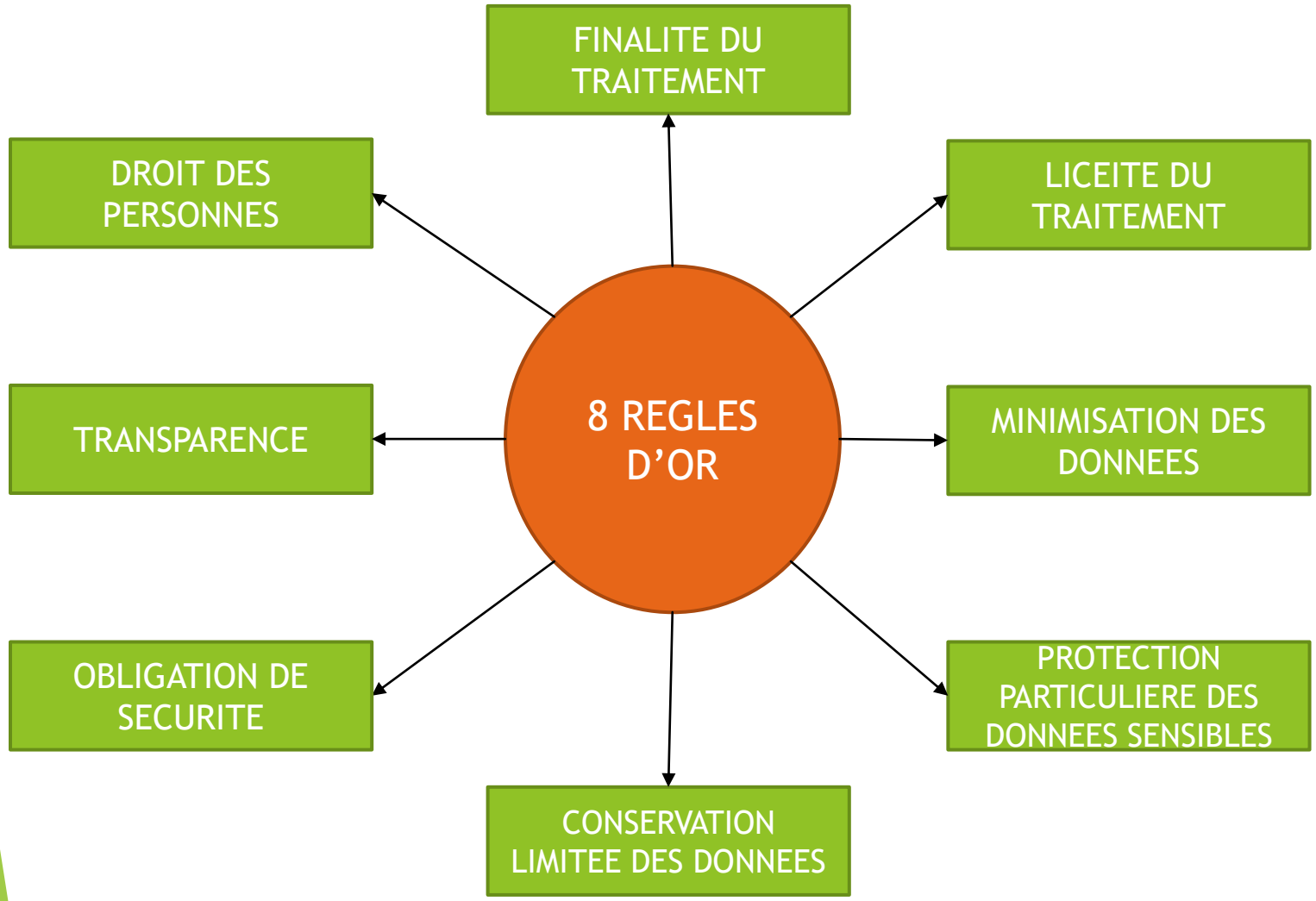
- Le CEPD (Comité Européen de la Protection des Données)
  - Coordonne l'action des « CNIL » de l'ensemble des pays de l'UE. Conseille la Commission Européenne, publie les lignes directrices. Se prononce sur les litiges transfrontaliers.



- La CJUE (Cour de Justice de l'Union Européenne).
  - Autorité judiciaire de l'UE. Sanction de toute entité (état membre ou entreprise) qui ne respecte pas la législation européenne. Arrêts juridiquement contraignants. Se prononce sur les demandes d'interprétation de la législation européenne à la demande des états membres.

Les Grands Principes de la protection des données

- **8 règles d'or :**



Ces principes doivent être assurés **à tout moment** et ce **même si les données sortent de l'Union Européenne**

Règle 1 : Licéité du traitement

- **Article 6.1 du RGPD : Le traitement n'est licite et ne peut être mis en œuvre que si l'une des 6 conditions suivantes est remplie :**
  - 1/ La personne concernée a **consenti au traitement de ses données : le consentement doit être :**
    - **Eclairé : Le responsable de traitement doit mettre en avant (avant tout consentement) : l'identité du responsable de traitement, les finalités du traitement, les catégories de données collectées, l'existence d'un droit de retrait du consentement.**
    - **Libre : Sans contrainte, peut accepter ou refuser ou retirer à tout moment son consentement.**
    - **Spécifique : En cas de modification de la finalité, un nouveau consentement sera nécessaire.**

      En cas de besoin de 2 traitements différents, il faut obtenir 2 consentements différents.
    - **Univoque : sans ambiguïté par une déclaration ou un acte positif clair. (nécessité d'un écrit pour preuve). Le responsable de traitement doit être en mesure de prouver le recueil le consentement à tout moment.**
  - 2/ Soit le traitement est **nécessaire à l'exécution d'un contrat, (exemple : inscription au conservatoire)**
  - 3/ Soit le traitement est nécessaire au **respect d'une obligation légale** à laquelle le responsable de traitement est soumis,
  - 4/ Soit le traitement est nécessaire à la **sauvegarde des intérêts vitaux de la personne** concernée ou d'une personne physique,
  - 5/ Soit le traitement est nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de **l'autorité publique** dont est investi le responsable de traitement,(exemple : plaque FPS)
  - 6/ Soit le traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable de traitement.
  - **EXEMPLE : Consentement à la publication de résultats nominatifs de concours en ligne : il faut avoir obtenu au préalable l'accord écrit et signé du concerné ou du représentant légal (si mineur).**

CITER LES SOURCES REGLEMENTAIRES

Règle 2 : Finalité (objectif) du traitement

- **Article 6 RGPD. LA REGLE :**

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

- La finalité est l'objectif en vue duquel les données sont collectées, enregistrées, transmises, conservées, (…) par l'organisme.

Exemple : la finalité d'un traitement peut-être la gestion des recrutements, des usagers d'un service public, la protection des biens et des personnes…

- Il est IMPOSSIBLE de collecter les données « à toutes fins utiles », ou « dans l'éventualité de ».

- Sa justification pourra être remise en cause si la finalité est considérée comme peu justifiée ou trop intrusive pour les personnes.

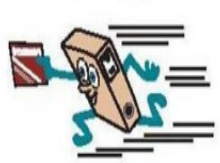
- La finalité doit être suffisamment claire et explicite pour la personne qui donne son accord.

- Le détournement de finalité sera sanctionné.

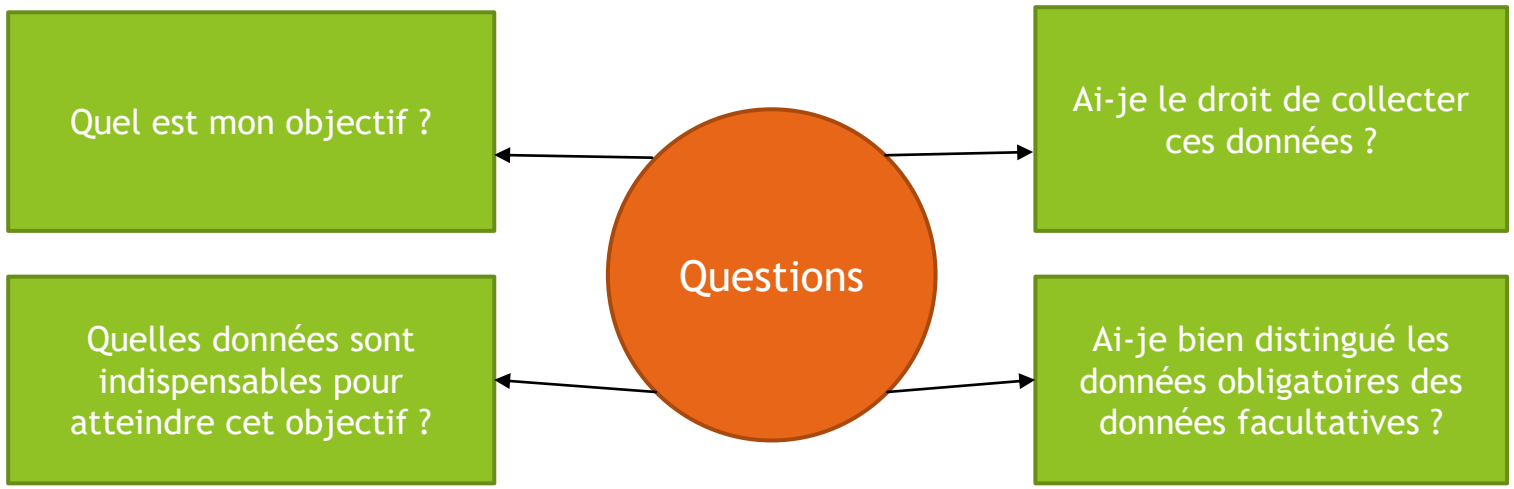
- Une finalité pourra être considérée comme « compatible » en cas d'évolution de celle-ci, mais elle devra se faire en toute transparence et dans le respect des droits de la personne, notamment le droit de s'y opposer et de nouveau consentement.

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

Règle 3 : Minimisation des données



- **Article 5-1 du RGPD.**
- Les données collectées doivent être **limitées,**
- **Est-ce que ma donnée est pertinente ? : lien direct avec la finalité du traitement.**



On ne recueille que ce dont on a strictement besoin !

- Les données doivent être **exactes et actualisées** (Article 5-1.d. du RGPD).
- Toute donnée erronée peut porter préjudice à la personne. Il faut donc prévoir une **mise à jour régulière** et le cas échéant **renouveler le consentement** si la finalité a changé.

QUIZ : Plusieurs solutions possibles

- **Question** : Parmi ces informations personnelles, lesquelles ne peuvent pas être collectées par un centre sportif lorsque la finalité du traitement est la gestion des cotisations de ses membres.

Identité	Numéro de sécurité sociale
Adresse postale	Adresse email
Coordonnées bancaires	Régime alimentaire

- **Réponse** :
- Le **numéro de sécurité sociale** n'est pas nécessaire dans le cadre de la gestion des cotisations.
- Il en est de même pour le **régime alimentaire**.
- Ces deux données ne sont pas **pertinentes** dans le cadre de la gestion des cotisations.

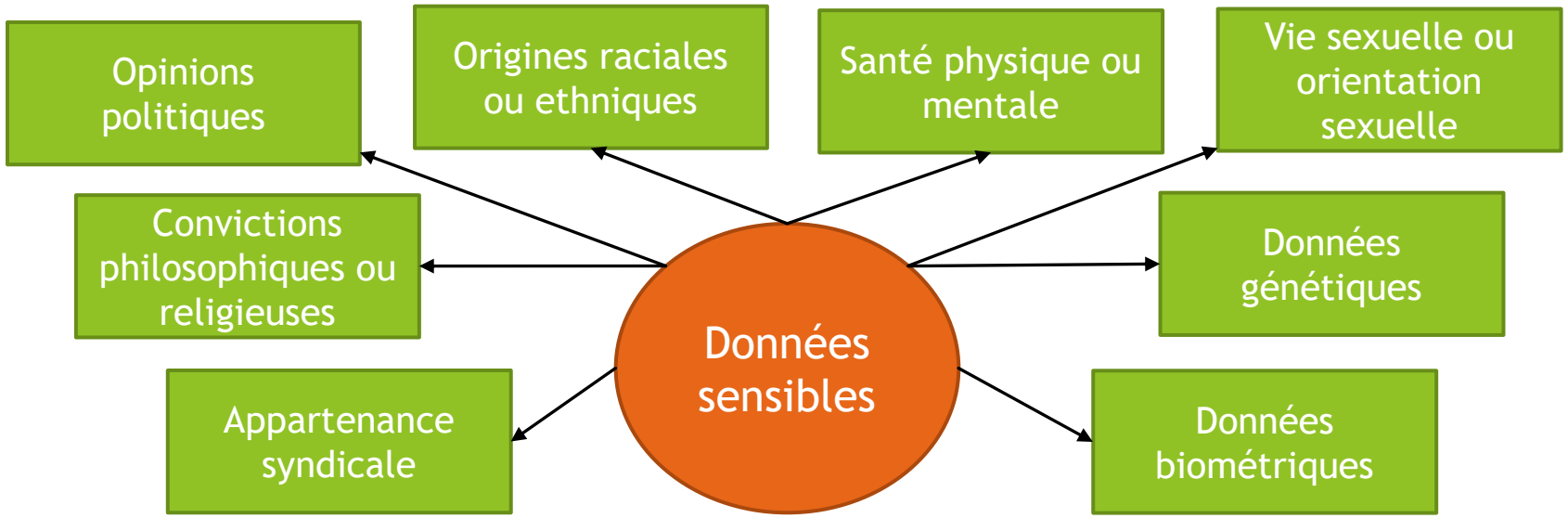
BONNES PRATIQUES :

- **Toujours s'interroger** sur la possibilité d'obtenir une **donnée alternative moins invasive**. Bien cerner la cible.
  - *Exemple* : pour une enquête, plutôt que de demander l'âge de la personne, on peut demander sa tranche d'âge.
- **Bannir** toute collecte de données à titre « préventif ».
- **Pseudonymiser** les données toutes les fois où leur conservation sous forme directement identifiante n'apparaît pas nécessaire.
- **Limiter** au maximum les zones de commentaires libres et privilégier autant que possible les menus déroulants pour limiter les réponses qui pourraient être jugées trop intrusives.
- **Faire régulièrement le tri** : Se questionner sur la nature des données collectées, la finalité du traitement, leur quantité, leur précision, leur durée légale de conservation. Archiver, faire détruire après validation.

Règle 4-1 : Protection de données « particulièrement sensibles » :

Art. 9-1 RGPD

- Il s'agit des données qui touchent à l'**intimité** de la personne voire à **l'identité humaine** et dont un mauvais usage représente un risque **élevé** pour l'individu.



Règle 4-2 : Protection données particulièrement sensibles Art. 9-1 RGPD

- **Exceptions : Art. 9-2 RGPD**
  - Données fournies par la personne concernée **avec son consentement explicite** (libre, spécifique, univoque, éclairé et révocable) ou **nécessaire à la sauvegarde des intérêts vitaux** de la personne,
  - Données nécessaires à **l'exécution des obligations** (par exemple droit du travail),
  - Données manifestement **rendues publiques par la personne concernée**,
  - Données nécessaires à la constatation, l'exercice ou la défense d'un **droit en justice**,
  - Données nécessaires pour des motifs d'**intérêt public importants** (par exemple des données de santé publiques, nécessaires à des fins médicales (médecine préventive, diagnostics médicaux, gestion des services de santé),
  - Données nécessaires à **l'intérêt public** (archives dans l'intérêt public ou recherche scientifique ou historique ou statistique),

Les données relatives aux condamnations pénales et aux infractions des individus ne peuvent être traitées que par les juridictions, les autorités publiques et les personnes agissant dans le cadre de leurs attributions légales dans le cadre du service public.

Il faudra donc pouvoir justifier la base légale du traitement et user de l'exception la plus pertinente

Règle 5 : Conservation limitée des données :

- Les données doivent être traitées pendant une **durée limitée et cohérente avec l'objectif** poursuivi. Le but est **d'éviter une utilisation détournée** de l'objectif initial et d'assurer le « **droit à l'oubli** ».
- Vérifier les dates si le recueil des données se fait en vertu d'une **obligation légale**, (et la citer),
- Vérifier les dates si la finalité est atteinte, les données doivent être **détruites (en suivant les règles d'archivage), anonymisées, ou archivées**.

En cours : Création d'une charte de l'archivage et d'un tableau de gestion de durée des données

ARCHIVES : 3 types de conservation

ARCHIVES COURANTES
-> dossiers vivants, d'utilisation habituelle pour l'activité des services, conservées sur le logiciel, le réseau, un disque dur, des armoires -> **le temps nécessaire à la mission**

ARCHIVES INTERMEDIAIRES
-> l'objectif initial justifiant la collecte est atteint mais la donnée doit être conservée à proximité jusqu'à la durée légale de conservation.

ARCHIVES DEFINITIVES
-> les données qui ne peuvent faire l'objet d'aucune destruction en vertu de leur valeur légale, historique ou stratégique.

NE PAS CONSERVER LES DONNEES TROP LONGTEMPS
…
MAIS ATTENTION DE NE PAS DETRUIRE TROP TOT !

Règle 6 : Obligation de sécurité de traitement et conservation des données

- **Article 32-1 :** Le responsable de traitement et le sous-traitant mettent en œuvre des **mesures techniques et organisationnelles** appropriées afin de garantir un niveau de sécurité adapté au risque.
  - **Pseudonymisation** et **chiffrement** des données à caractère personnel
  - Mettre en place des moyens permettant de garantir la **confidentialité et l'intégrité** constantes des systèmes et des services de traitement. Attention de bien cloisonner le partage de données sur les serveurs.
  - Mettre en place des moyens permettant de rétablir la **disponibilité** des données à caractère personnel et l'**accès** à celles-ci dans des délais appropriés en cas d'incident physique ou technique, (erreur technique, incendie, cyber-attaque…)
  - Mettre en place des procédures visant à **tester, analyser et évaluer** régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Principes et but des mesures de sécurité

Confidentialité	**Les données ne sont accessibles qu'aux seules personnes autorisées**
Intégrité :	**Eviter l'altération ou la modification des données**
Disponibilité :	**Les données doivent être accessibles aux personnes concernées par le recueil de leurs données**

La source de ces risques peut être interne, externe, accidentelle ou délibérée

Règle 6 : Obligation de sécurité : Bonnes pratiques

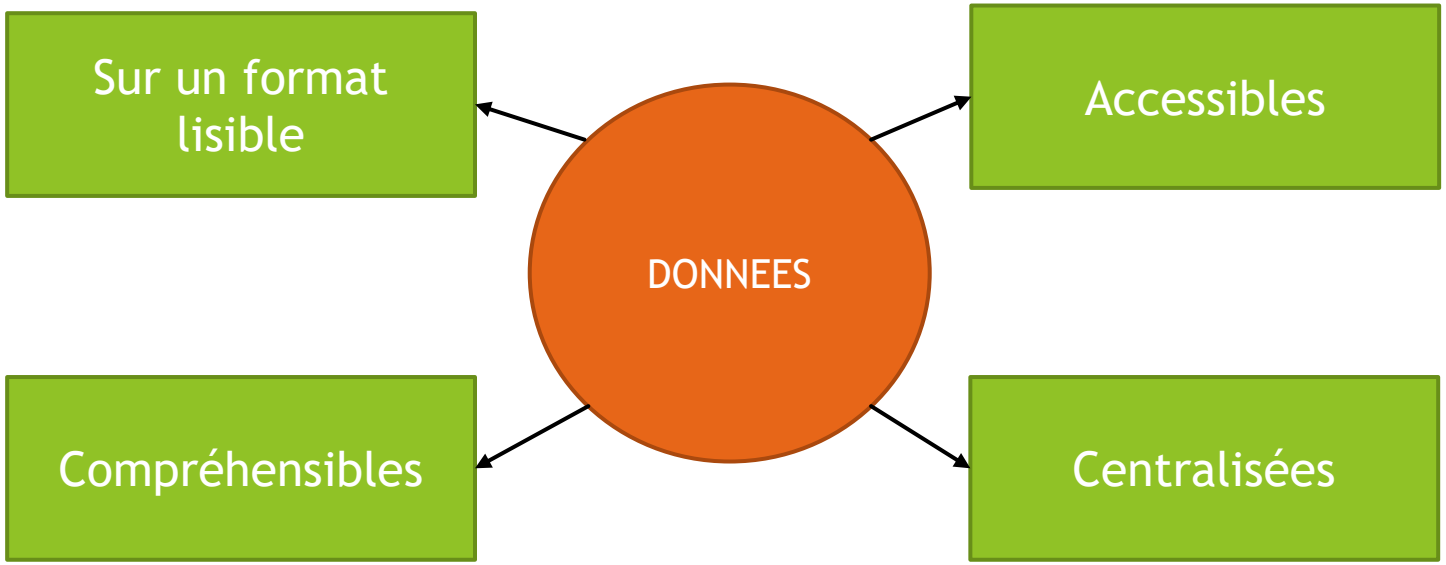
- **Mesures physiques :** alarmes anti-intrusion, badges - contrôle d'accès à certains locaux collectant des données sensibles, armoires fermées à clef…

- **Mesures logiques :** identifiant unique, mots de passes sécurisés, bloquer temporairement l'accès au compte après plusieurs échecs d'identification, verrouillage automatique du poste passé un certain délai de pause, etc.

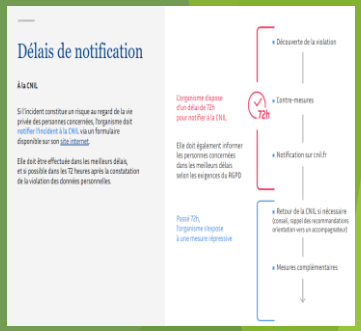
- **Mesures organisationnelles** : Définir les procédures à suivre à chaque changement de personnel, revoir régulièrement les droits accordés aux utilisateurs, créer une politique de contrôle d'accès aux données, sensibiliser les utilisateurs sur les conditions de sécurité et d'utilisation des données dès les premiers entretiens, définir une politique de gestion des incidents, prévoir des audits réguliers des procédures et des traitements.

Règle 7 : Transparence à l'égard des personnes concernées par les données

- **Article 12-1 RGPD**
- **Principe de loyauté et de transparence vis-à-vis des personnes concernées par les traitements de leurs données personnelles => Assurer le droit à l'information.**
  - **L'obligation de transparence pèse sur les responsables de traitement**
  - **But : les personnes concernées par les traitements doivent garder la maitrise de leurs données**



Règle 7 : Transparence à l'égard des personnes concernées par les données



- **Droit à l'information : qui doit être claire simple, concise, et aisément accessible NOUS DEVONS POUVOIR DONNER A TOUT MOMENT :**
  - **Identité et coordonnées de l'organisme responsable du traitement,**
  - **Finalité du traitement et base juridique,**
  - **Le caractère obligatoire de la donnée, le fondement juridique du caractère obligatoire,**
  - **Le destinataire des données,**
  - **La durée de conservation des données, ou les critères utilisés pour la déterminer,**
  - **Les droits de la personne sur les données traitées (accès, rectification, opposition, limitation, effacement),**
  - **Les droits de la personne d'introduire une réclamation auprès d'une autorité de contrôle**
  - **Toute information pertinente concernant les projets et les traitements ultérieurs pour une finalité différente.**

Ces informations doivent être transmises dans un délai **d'un mois**, si déjà contact, ou **à la première communication** avec l'intéressée.

Exception : La personne a déjà ces informations (mais il faut pouvoir apporter la preuve) ou bien il y a couverture par le secret professionnel.

Règle 8 : Droits des personnes sur leurs données

RGPD considérants 7 et 11 (droits préexistants au RGPD)

Art. 15 Droit d'accès à ses données	Art. 16 Droit à rectifications de ses données	Art. 21 Droit d'opposition au traitement de ses données	Art. 17 Droit à l'effacement (oubli) de ses données
Suis-je encore inscrite dans vos fichiers ? (accès à toutes les informations et droits sur mes données)	Je souhaite corriger des données inexactes et les compléter.	Je m'oppose à recevoir vos publicités et vous demande de me sortir de vos fichiers,	Je n'ai plus de contrat chez vous, merci de supprimer mes données de votre base.

Nouveaux droits (apparus avec le RGPD)

Art. 20 Droit à la portabilité de ses données	Art. 18 Droit à la limitation du traitement de ses données	Art. 22 Droit de ne pas faire l'objet d'une décision automatique
Ex : Merci de transmettre mes données à votre concurrent chez qui je viens de conclure.	Ex : En attendant la suppression d'un compte, demander la limitation de pub de la photo	Ex : Votre candidature a été refusée (automatisation de la réponse sans explication)

Responsables de traitement et réflexes à avoir

- **Tous les acteurs intervenant dans un traitement de données sont responsables de la garantie des 8 principes garantissant la sécurité du RGPD.**

- **Tous les organismes, qu'ils soient responsables de traitement ou sous-traitants, doivent s'inscrire dans une posture de mise en conformité dynamique.**
- **Réflexes lors de la conception du projet,**
  - Dès la création du projet, les responsables de traitement doivent prendre les mesures adéquates pour garantir une protection maximale des données personnelles.
- **Réflexes lors de la diversification et la mise en œuvre du projet de façon à ce que la collecte de données se limite au strict minimum.**
  - Gérer les habilitations et droits d'accès, purger automatiquement et sélectivement les données d'une base active à l'issue d'une certaine durée …
- **Les acteurs doivent conserver tout élément permettant de prouver que le traitement des données est conforme (registre des activités de traitement, contrats de sous-traitance, mentions d'information, formulaires de recueil du consentement etc…)**

Le cas du responsable de traitement et du sous-traitant

RESPONSABLE DE TRAITEMENT	SOUS-TRAITANT
ORGANISME POUR LEQUEL LE TRAITEMENT EST MIS EN ŒUVRE, QUI DEFINIT LA FINALITE DU TRAITEMENT DES DONNEES PERSONNELLES	TRAITE LES DONNEES PERSONNELLES POUR LE COMPTE ET SUR INSTRUCTIONS DU RESPONSABLE DE TRAITEMENT

Dans le cadre d'une violation de données, la responsabilité est partagée et chacun a des obligations respectives

Règles entre responsable et sous-traitant :

Le responsable de traitement ne doit faire appel qu'à des organismes qui présentent des **garanties suffisantes** quant à la sécurisation du traitement des données,

Une **clause spécifique** doit être contenue dans le contrat explicitant **qui** est responsable du traitement des données.

Le responsable de traitement doit être informé par **écrit de tout changement**, y compris si le sous-traitant fait lui-même appel à un autre sous-traitant de façon à pouvoir renoncer à la sous-traitance s'il considère que les mesures de sécurité ne sont pas garanties.

Le sous-traitant doit aider le responsable de traitement à s'acquitter de ses obligations (notamment consultation, droit de modification, droit d'effacement…).

-> Le sous-traitant doit notifier à son client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

-> Le responsable de traitement devra quant à lui notifier cette violation de données

* à l'autorité de contrôle (CNIL)
* à la personne concernée par la violation.

Les sanctions en cas de violation aux principes du RGPD et les recours

- **La CNIL a le pouvoir de contrôler et sanctionner tout contrevenant aux principes de la protection des données.**

- La CNIL reçoit et traite les plaintes des particuliers ;
- Elle dispose de pouvoirs de **contrôles sur place, en ligne, sur pièce ou sur audition**
- Elle peut prononcer des mises en demeure de se mettre en conformité, des rappels à l'ordre, des injonctions de mettre le traitement en conformité y compris sous astreinte, des limitations temporaires ou définitives du traitement…
- **Les recours :**
  - **Toute personne** considérant que le traitement de données à caractère personnel la concernant constitue une violation du RGPD peut saisir une autorité de contrôle pour déposer une réclamation.

Quelles sont les sanctions ?

Les organismes publics peuvent-ils être sanctionnés en cas de non respect du RGPD ?

OUI : Les organismes ayant une personne morale de droit public comme les établissements publics ou les collectivités territoriales peuvent être sanctionnés :

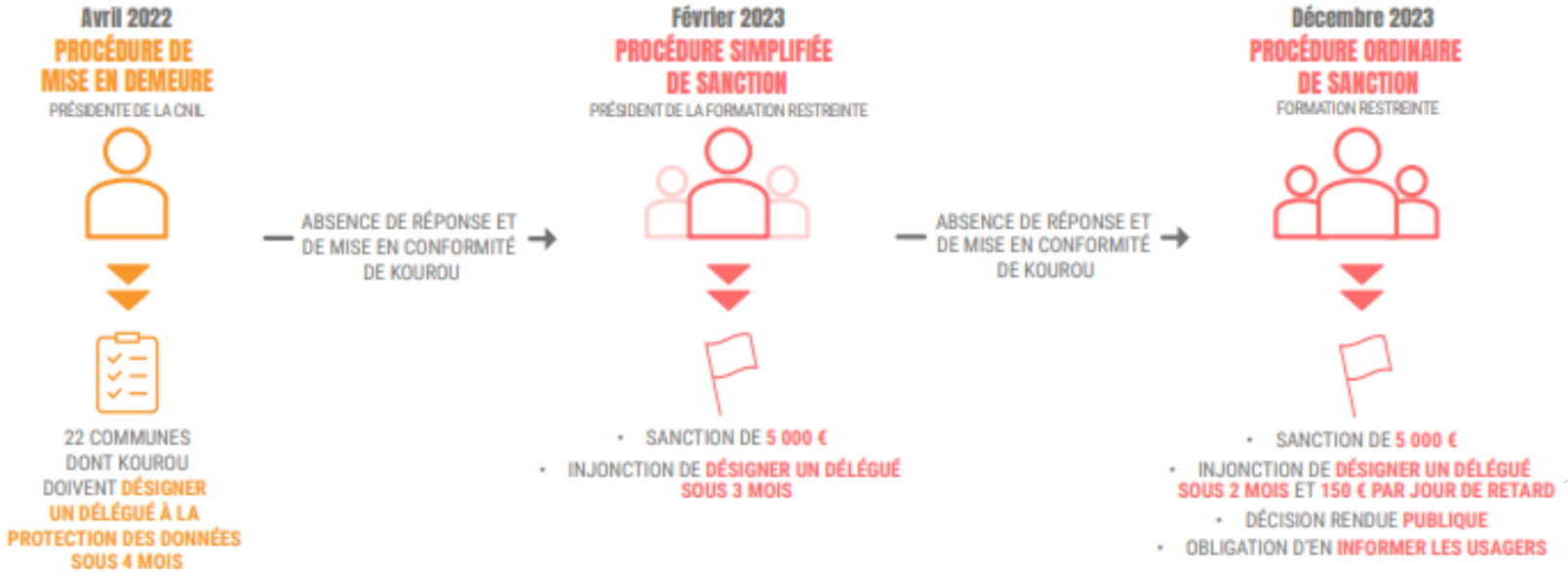
EXEMPLE :

Avril 2022 : La CNIL met en demeure publiquement 22 communes de désigner un délégué à la protection des données.

-> Absence de réponse de KOUROU -> Condamnation : Amende de 5000 € + injonction de se mettre en conformité sous 3 mois.

-> Absence de réponse : Nouvelle condamnation de 5000 euros + 150 euros d'astreinte par jour + injonction de se mettre en conformité sous 2 mois + décision rendue publique + obligation d'en informer les usagers

Ces **mises en demeure publiques** non suivies peuvent donner lieu à une **amende rendue également publique ou d'une injonction sous astreinte.**



Les outils de la conformité : Le registre

- **Un registre des activités de traitement est obligatoirement mis en place par tout responsable de traitement ou sous-traitant.**

Il permet d'avoir une vue d'ensemble des traitements pour piloter la conformité au RGPD.

Forme et contenu :

-> Sous forme écrite (papier ou électronique)

-> Renseigne :

- **les parties prenantes,**
- **les catégories de données traitées et leurs finalités,**
- **le nom (ou service) de ceux qui ont accès aux données,**
- **la durée de conservation des données,**
- **les modalités de sécurisation des données.**

L’analyse d’impact relative à la protection des données (AIPD ou PIA)

- **Outil central permettant de considérer les risques encourus pour les droits et libertés des individus, la responsabilisation des organismes utilisant des données personnelles, (GPSO : outil mis en place par la Direction des Affaires Institutionnelles, le responsable de traitement et la DSI).**
- **C’est un outil permettant de démontrer la conformité des traitements au RGDP à la demande de la CNIL en cas de contrôle.**
- **3 cas**

1. **- Une liste de critère qui rendent l’AIPD quoi qu’il en soit obligatoire,**
2. **- Une liste de critères qui rendent l’AIPD non nécessaire,**
3. **- Le traitement contient cumulativement au moins 2 de ces 9 critères :**
   - **- évaluation des personnes (y compris le profilage)**
   - **- prise de décisions automatiques avec effet légal ou similaire**
   - **- surveillance systématique**
   - **- collecte de données sensibles ou données à caractère hautement personnel**
   - **- croisement de données (statistiques)**
   - **- présence de personnes vulnérables (patients, personnes âgées, enfants etc.)**
   - **- mise en place d’usage innovant (utilisation d’une nouvelle technologie)**
   - **- exclusion du bénéfice d’un droit ou d’un contrat.**
   - **- collecte de donnée à grande échelle.**

L’analyse d’impact relative à la protection des données (AIPD ou PIA)

Cas spécifique de la vidéo protection ou vidéo surveillance des agents :

-> collecte à grande échelle + surveillance systématique + personne vulnérable

-= 3 critères

-=> AIPD nécessaire.

- **Les dispositifs de vidéoprotection** filment la voie publique et les lieux ouverts au public : rue, gare, centre commercial, zone marchande, piscine etc.
- **Les dispositifs de vidéosurveillance** filment les lieux non ouverts au public : réserve d'un magasin, entrepôts, copropriété fermée etc.

L’analyse d’impact relative à la protection des données (AIPD ou PIA)

- **Contenu :**
- **-> Description systématique des opérations de traitement et leurs finalités**
- **-> Evaluation de la nécessité et la proportionnalité du traitement**
- **-> Evaluation des risques**
- **-> Mesures envisagées pour faire face aux risques**

- **Quand ?**
- **Avant la mise en œuvre du traitement (ou après si pris en cours).**

La Direction des Affaires Institutionnelles va se rapprocher de vous pour préparer ensemble votre Analyse d’Impact en cas de collecte de données à risque

Notification des violations de données

Le RGPD impose à tous les responsables de traitement

-> de documenter en interne les violations de données

-> de notifier à la CNIL les violations de données personnelles induisant un risque élevé pour la personne

-> de notifier aux personnes concernées les violations de données personnelles susceptibles d'engendrer un risque élevé.

Quelle peut être la violation ? Ce peut être :

- Faille ou vulnérabilité de sécurité
- Accident (incendie, inondation, panne matérielle etc.)
- Une erreur de saisie
- Une action de malveillance (piratage, vol de matériel etc).

Documentation obligatoire :

- La nature de la violation
- Les conséquences probables de la violation
- Les catégories et le nombre de personnes concernées
- Les mesures prises ou envisagées
- Les catégories et le nombre approximatif d'enregistrements de données personnelles concernées.

Notification des violations de données

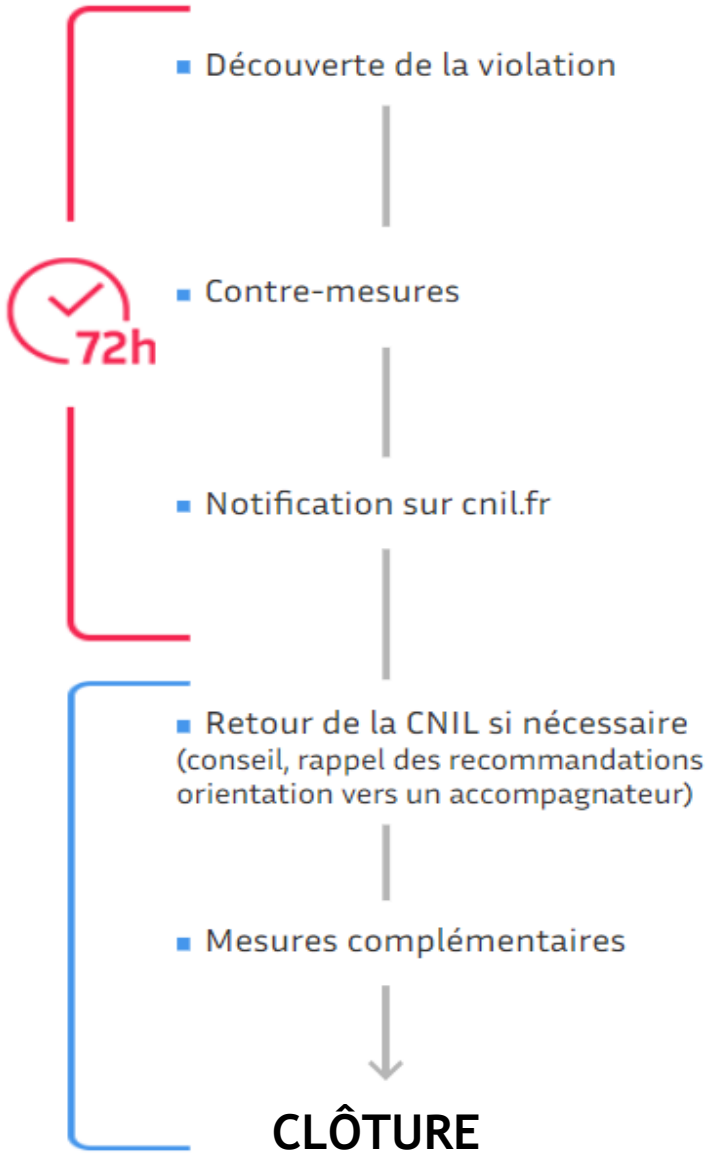
Délais de notification :

à la CNIL :

L'organisme dispose d'un délai de 72h pour notifier à la CNIL

Elle doit également informer les personnes concernées dans les meilleurs délais selon les exigences du RGPD

Passé 72h, l'organisme s'expose à une mesure répressive



Dès la découverte d'une faille dans le système de sécurité du traitement de vos données, en informer immédiatement Caroline LARCHEVEQUE (DAI) ainsi que la DSI (si problème informatique)

Notification des violations de données

EN PARALLELE :

Délais de notification aux personnes concernées :

- **« dans les meilleurs délais ».**
  - **Nature de la violation**
  - **Conséquences probables de la violation**
  - **Coordonnées de la personne à contacter**
  - **Mesures prises pour remédier à la violation ou limiter les conséquences**

EXCEPTION A CETTE OBLIGATION :

- **-> si l'organisme a mis en œuvre des mesures techniques et organisationnelles de protection pour ôter le caractère élevé du risque**
- **-> si l'organisme a mis en œuvre des mesures techniques et organisationnelles qui rendent les données incompressibles (mots de passe, cryptage, chiffrement…)**
- **-> si la notification nécessite un effort disproportionné (une communication publique sera alors obligatoire mais évitera une information individuelle).**

Les acteurs de la conformité en interne

- **Le Délégué à la Protection des données de GPSO :**

Caroline LARCHEVEQUE, Directrice Direction des Affaires Institutionnelles

Chef de service : Eric SCHUBERT

Juriste : Anne-Sophie APARICIO

- **Contact :** rgpd@seineouest.fr

Rôle n° 1 : Informe et conseille les services

Rôle n° 2 : Contrôle la conformité de l'utilisation des données avec la réglementation RGPD

Rôle n° 3 : Interface entre GPSO, la CNIL, et les personnes concernées

- **Plus généralement, tous les agents dans le cadre de leur activité sont garants de la protection des données personnelles qu'ils utilisent dans le cadre de leur(s) missions(s).**

LA DIRECTION DES AFFAIRES INSTITUTIONNELLES EST A VOTRE ECOUTE !

rgpd@seineouest.fr