COMITÉ NATIONAL OLYMPIQUE ET SPORTIF FRANÇAIS

CROS AUVERGNE RHÔNE-ALPES

Les principes du RGPD

La Région Auvergne-Rhône-Alpes

Préfet de la Région Auvergne-Rhône-Alpes

Le RGPD, c’est quoi ?

RGPD, KÉSAKO ?

« Règlement Général sur la Protection des Données »

Texte de mai 2018 qui fait évoluer la loi « Informatique et Libertés » de 1978.

Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

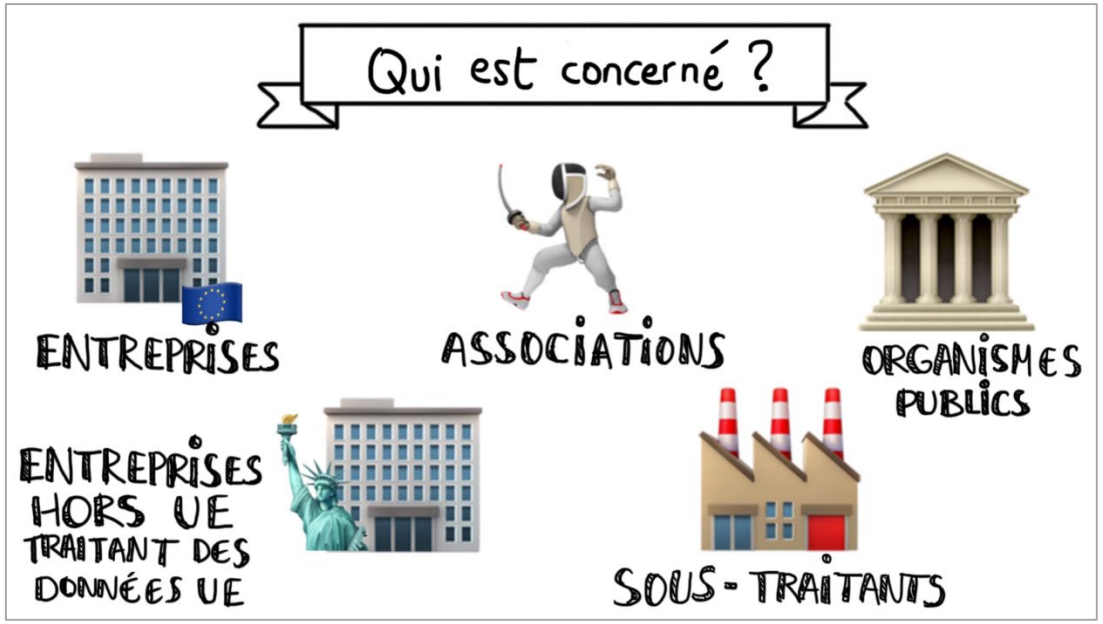
Il octroie de nouveaux droits aux propriétaires des données.

Contrôlé par la **Commission nationale de l'informatique et des libertés (CNIL)**

RGPD, POUR QUI ?

Le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

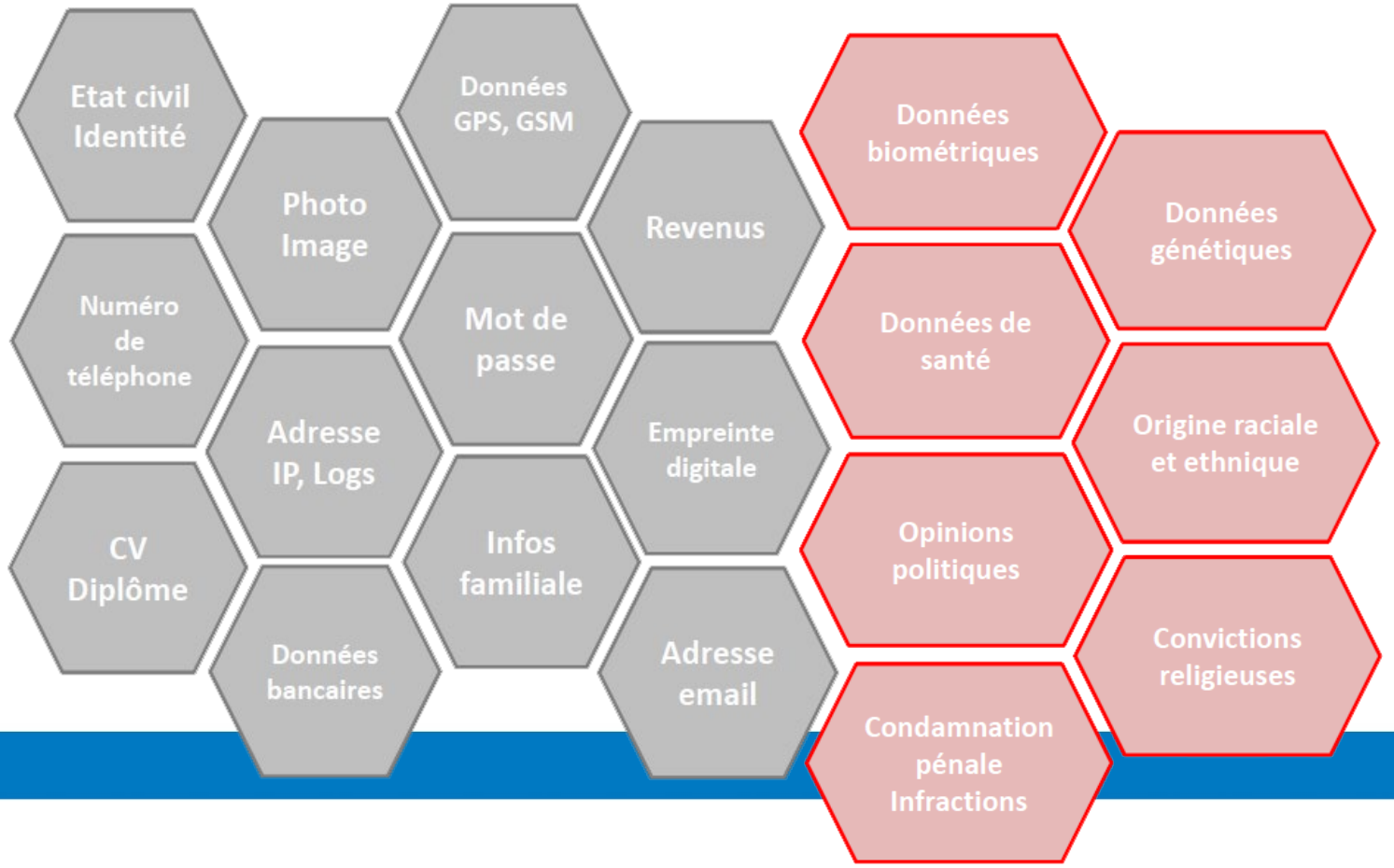
• qu'elle est établie sur le territoire de l'Union européenne ;
• que son activité cible directement des résidents européens.

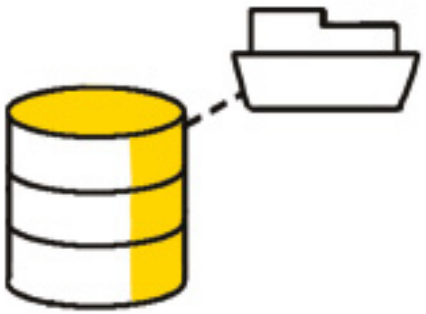


Qu'est ce qu'une donnée personnelle ?

Une donnée personnelle est toute information se rapportant à **une personne physique identifiée ou identifiable directement ou indirectement**.

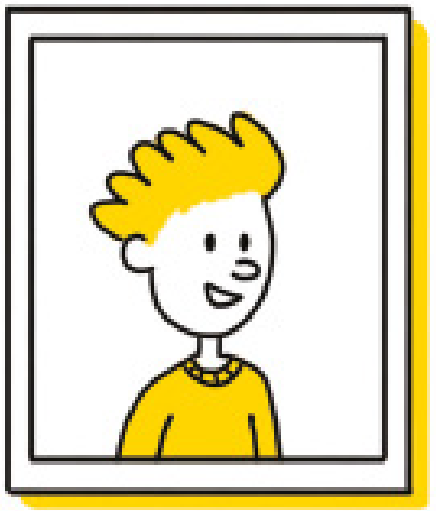
Peu importe que ces informations soient **confidentielles ou publiques.**





- Nom : ?
- Prénom : ?
- Sexe : masculin
- Âge : 19
- Adresse : 5 rue de la gare
  79000 NIORT
- Lycée : Montaigne (Bordeaux)
- Passion : Le jazz

=



Marc PELLETIER

Zoom sur les données sensibles

Il est par principe interdit de recueillir ou utiliser des données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses, données de santé…)

SAUF exceptions : preuve de consentement, informations publiques, sauvegarde de la vie humaine…

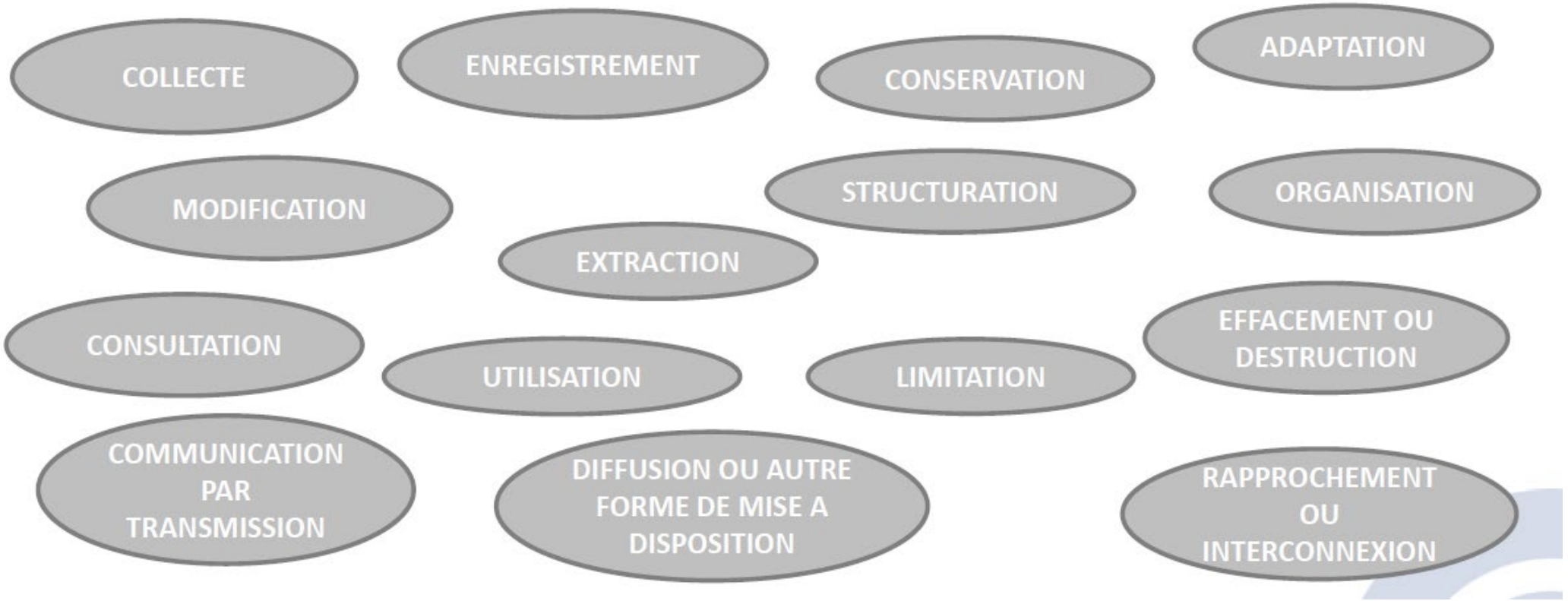
En pratique : il convient d'éviter la collecte excepté si l'activité l'exige, auquel cas vous devrez vous assurer de la licéité du traitement.

NB : Ne collectez que les données strictement nécessaires, avec une gestion spécifique d'accès restreint et de sécurité pour une durée limitée

Qu'est-ce qu'un traitement ?

Un « traitement de données personnelles » **est une opération, ou ensemble d'opérations**, portant sur des données personnelles, quel que soit le procédé utilisé.

Qu'est-ce qu'un traitement ?



Qui traite les données et qui est responsable ?

Le responsable de traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Le sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

Le Délégué à la Protection des Données (DPD ou DPO)

Le DPO : la personne physique externe ou interne à la structure qui organise la mise en conformité : il conseille le responsable de traitement, contrôle le respect du RGPD et coopère avec l'autorité de contrôle.

Le DPO n'est pas obligatoire dans toutes les structures. Néanmoins, la CNIL conseille fortement d'en désigner un.

Il peut être bénévole ou salarié et sa mission doit faire l'objet d'une désignation officielle, via une lettre de mission pour le salarié, une convention pour le bénévole.

Attention, la désignation d'un DPO auprès de la CNIL soumet le responsable de traitement à plusieurs obligations comme : la formation continue, donner l'accès aux informations de la structure, fournir une indépendance fonctionnelle et les ressources nécessaires à la mission du DPO… En retour, le DPO a aussi des obligations.

Ce qui a changé avec le RGPD

L'esprit avant le RGPD	L'esprit avec le RGPD
▪ Régime de formalités préalables ▪ Les autorités de contrôle doivent prouver la non-conformité	▪ Absence de formalités préalables *(sauf cas particuliers*)* ▪ Les organismes doivent prouver leur conformité aux autorités de contrôle

Quels droits possèdent les propriétaires de données personnelles ?

Quels droits ?

Droit à l'information

Avoir une information claire sur l'utilisation de vos données et sur l'exercice de vos droits

Droit d'opposition

S'opposer, **pour des motifs légitimes,** au traitement de ses données, sauf si celui-ci répond à une obligation légale

Droits d'accès

Obtenir les données détenues sur soi et savoir si elles font l'objet d'un traitement

Droit de rectification

Demander la rectification des informations inexactes ou incomplètes

Droit à l'effacement

Demander à un organisme l'effacement de données (selon conditions)

Quels droits ?

Droit au déréférencement

Ne plus être associé à des contenus en ligne.

Droit à la limitation du traitement

Gel de l'utilisation de certaines données

Droit à la portabilité

Obtenir une copie des données ou demander au RT de les transmettre à un autre RT

Droit à l'intervention humaine

face à un profilage ou une décision individuelle automatisée

Comment traiter des données personnelles dans les règles ?

7 principes clefs à respecter

Principe 1 : Traitement licite, loyal et transparent

Un traitement de données personnelles ne peut être mis en œuvre sans base légale.

En détails :

- **Sur le principe de collecte loyale** :

Il interdit la collecte de données personnelles « *par un moyen frauduleux, déloyal ou illicite* », car une information ne peut être librement réutilisée, et constitue, sans consentement et hors cas d'exception, une atteinte au principe de loyauté.

- **Sur l'obligation de transparence** :

Elle consiste à permettre à l'utilisateur de demander à tout moment d'être informé sur les traitements dont ses données personnelles font l'objet, ainsi que de pouvoir être informé de la finalité et des modalités du traitement.

- **Sur la licéité du traitement** :

Le principe consiste en une liste précisant les cas de licéité, le premier impliquant que l'utilisateur ait donné son consentement positif pour une ou plusieurs finalités définies et spécifiques.

En tant que clubs, comités, ligues… quelles bases légales utiliser ?

Licenciés ou adhérents
Base légale : contrat

Salariés
Base légale : obligation légale

Newsletter
Base légale : consentement

Partenaires, prestataires
Base légale : contrat

Prospects
Base légale : consentement

Zoom sur l'intérêt légitime

Justification d'un traitement de données personnelles s'il ne porte pas une atteinte importante aux droits et intérêts des personnes concernées, dans le **respect de 3 conditions** :

1. L'intérêt poursuivi par l'organisme doit être « *légitime* »

2. Le traitement de données doit être « *nécessaire* »

3. Le traitement ne doit pas heurter les droits et intérêts compte tenu des attentes raisonnables

Il convient donc d'opérer une balance entre les intérêts à effectuer un traitement et les droits et intérêts des personnes concernées en identifiant toutes les conséquences

7 principes clefs à respecter

Principe 2 : Limitation des finalités

Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

- Le responsable de traitement devra déterminer la finalité de ce traitement clairement et précisément afin de prévenir tout détournement ultérieur.

- La finalité devra être légitime, c'est-à-dire répondre à un objectif du responsable de traitement et ne pas porter atteinte aux droits fondamentaux des personnes (même autres que la vie privée).

- Les données ne devront pas être traitées ultérieurement pour une finalité incompatible

7 principes clefs à respecter

Principe 3 : Minimisation des données

Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Peu importe que la donnée soit intrusive ou non, si elle n'est pas nécessaire au traitement, elle ne devra pas être collectée.

7 principes clefs à respecter

Principe 4 : Exactitude

Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

7 principes clefs à respecter

Principe 5 : Limitation de la conservation

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

Attention, une même donnée peut connaitre plusieurs durées de conservation différentes en fonction de la finalité du traitement mis en œuvre.

Exemple : Géolocalisation des véhicules (norme simplifiée n°51 de la CNIL)

Durée de base : 2 mois

Optimisation des tournées : 12 mois maximum

Suivi du temps de travail : 5 ans (uniquement pour les horaires et non les trajets)

7 principes clefs à respecter

Principe 6 : Sécurité

Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées

3 types de sécurité :

- Physique (ex : mesures de protection des locaux, d'accès aux salles informatiques) ;
- Logique (ex : mesures de protection des données et de l'accès à ces données, mots de passe, politique d'habilitation, chiffrement);
- Juridique (ex : contrat avec les sous-traitants).

7 principes clefs à respecter

Principe 7 : Responsabilité et preuve

Le responsable du traitement est responsable du respect du paragraphe 1 (donc les 6 principes précédents) et est en mesure de démontrer que celui-ci est respecté.

- Être conforme à la règlementation ;
- Démontrer la conformité à la règlementation.

Exemples : Contrats sous-traitants, clause de confidentialité dans les contrats, politique de confidentialité, registre des activités de traitements, codes de conduite, procédures diverses…

Quelles sont les sanctions ?

CROS AUVERGNE RHÔNE-ALPES

Quelles sont les sanctions ?

Cas de sanction	Sanction maximale
Le **délit d'entrave** en cas de contrôle est une volonté manifeste du RT de ne pas coopérer ou de dissimuler des informations.	1 an d'emprisonnement et 15 000€ d'amende
Sanction administrative niv. 1 en cas de : - Faille de sécurité (Art. 32 à 34) - Traitement impliquant le consentement des enfants (Art. 8) - Traitement ne nécessitant pas l'identification (Art. 11) - Analyse d'impact et DPO (Art. 25 à 39) - Certification (Art. 42 et 43) - Suivi des codes de conduite (Art. 83 §4)	2% du chiffe d'affaire annuel mondial ou 10M€ (Les Etats membres fixent les amendes pour les organismes publics.)
Sanction administrative niv. 2 en cas de : - Non respect des droits des personnes concernées - Les transferts de données hors UE - Non respect d'une injonction ou d'une limitation temporaire ou définitive d'un traitement - Refus de donner accès à un traitement à l'autorité de contrôle	4% du chiffre d'affaire annuel mondial ou 20M€ pour les organismes privés (Les Etats membres fixent les amendes pour les organismes publics.)

CROS AUVERGNE RHÔNE-ALPES

Quelles sont les sanctions ?

Sanctions pénales relatives au non-respect des dispositions relatives...	Art.s du Code pénal	Amende max	Emprisonnement
Au caractère loyal et licite de la collecte de données	Art. 226-18	300 000 €	5 ans
Aux droits d'accès, de rectification ou d'opposition de la personne	Art. 226-18-1 (opposition prospection) Art. 226-19-1 (traitement à des fins de recherches dans le domaine de la santé) Art. R. 625-11 (droit d'accès) Art. R. 625-12 (droit de rectification)	300 000 € 300 000 € 3 000 € 3 000 €	5 ans 5 ans NA NA
À l'information des personnes	Art. R. 625-10	3 000 €	NA
Aux formalités préalables	Art. 226-16	300 000 €	5 ans
À la sécurité des données	Art. 226-17	300 000 €	5 ans
À la durée de conservation des données	Art. 226-20	300 000 €	5 ans
À la finalité des données	Art. 226-21	300 000 €	5 ans
À la conversation de données sensibles en l'absence de consentement exprès des personnes concernées	Art. 226-19	300 000 €	5 ans
À l'obligation de notification des failles de sécurité	Art. 226-17-1	300 000 €	5 ans

Exemples concrets de sanctions

La CNIL sanctionne chaque année entreprises et institutions pour leurs manquements au RGPD avec un montant de **sanctions pécuniaires** pouvant s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du CA annuel mondial.

#Cybersécurité *: l'autorité britannique de protection des données, en coopération avec la CNIL, inflige deux amendes record - 02 novembre 2020*

#Sanctions *de 2 250 000 euros et de 800 000 euros pour les sociétés CARREFOUR FRANCE et CARREFOUR BANQUE - 26 novembre 2020*

#Cookies *: sanction de 35 millions d'euros à l'encontre d'AMAZON EUROPE - 10 déc. 2020*

#Violations *de données de santé : la CNIL sanctionne deux médecins - 17 déc. 2020*

#Prospection *commerciale : sanction publique de 7 300 Euros à l'encontre de la société PERFORMECLIC - 31 décembre 2020*

Bilan du RGPD 3 ans après

Les chiffres clés : Rapport d'activité 2020 de la CNIL

13 585 plaintes de la part d'internautes et 38 799 depuis la mise en place du RGPD.
40% des contrôles suite à une plainte ou signalement
Un montant total d'amendes de **138 M €** en 2020
61% des organismes soumis au RGPD collectent plus ce que la loi leur permet
77% des organismes ne sont pas sûrs d'avoir que des données clients nécessaires

Les principales évolutions réglementaires **:**

1- Invalidation du Privacy Shield en Juillet 2020
2- Nouvelle directive sur les cookies en Octobre 2020
3- Fin du délai de tolérance pour l'Analyse d'Impact au 25 mai 2021
4- Une intensification et simplification des contrôles
5- Et l'augmentation corrélative des sanctions amendes

CONCLUSION

- Questions réponses

- Autodiagnostic

- Questionnaires d’évaluation et de satisfaction