Hôpital
Marie-Lannelongue

Accueil des Internes 02/11/2023

Sensibilisation RGPD
&
Sécurité des données

RGPD : Règlement Général sur la Protection des Données

Hôpital
Marie-Lannelongue

Donnée à caractère personnel / Donnée «Sensible»

- **Les données personnelles :** désignent toutes **données relatives à une personne physique identifiée** ou pouvant être identifiée directement ou indirectement grâce à cette donnée.

- **Les données particulières ou sensibles** : sont celles qui font apparaître, directement ou indirectement pour un individu ***les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuse ou l'appartenance syndicale, ou qui sont relatives à la santé ou à l'orientation sexuelle***.

sont soumises à un
haut niveau de protection

Hôpital Marie-Lannelongue

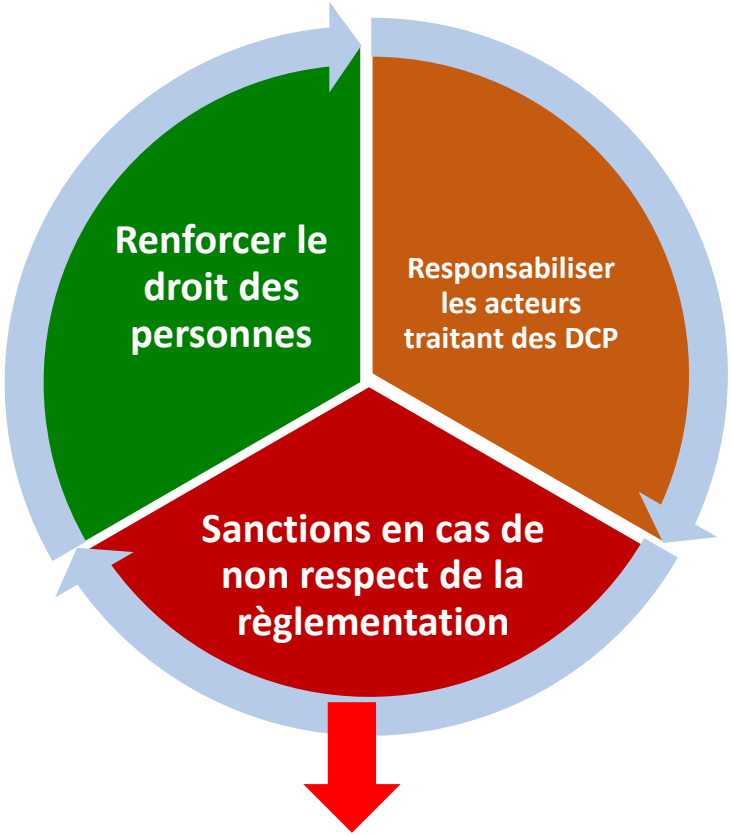
Le RGPD : Règlement Général sur la Protection des Données

- Commission européenne propose en janvier 2012 un nouveau règlement visant à
  - ✓ Adopté en première lecture mars 2014
  - ✓ **Adopté définitivement le avril 2016 par le Parlement européen,**
  - ✓ **Entré en vigueur le 25 mai 2018**

→ **"redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises"**

Le RGPD est placé, en France, Sous l'autorité de la

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS



Amende jusqu'à 4 % du CA mondial ou 20 M€

RGPD
Règlement Général sur la Protection des Données

Le RGPD : Règlement Général sur la Protection des Données

En 2022

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

345 contrôles

dont

- 143 contrôles sur place
- 128 contrôles en ligne

21 sanctions

dont :

- 19 amendes pour un montant cumulé de **101 277 900 euros**

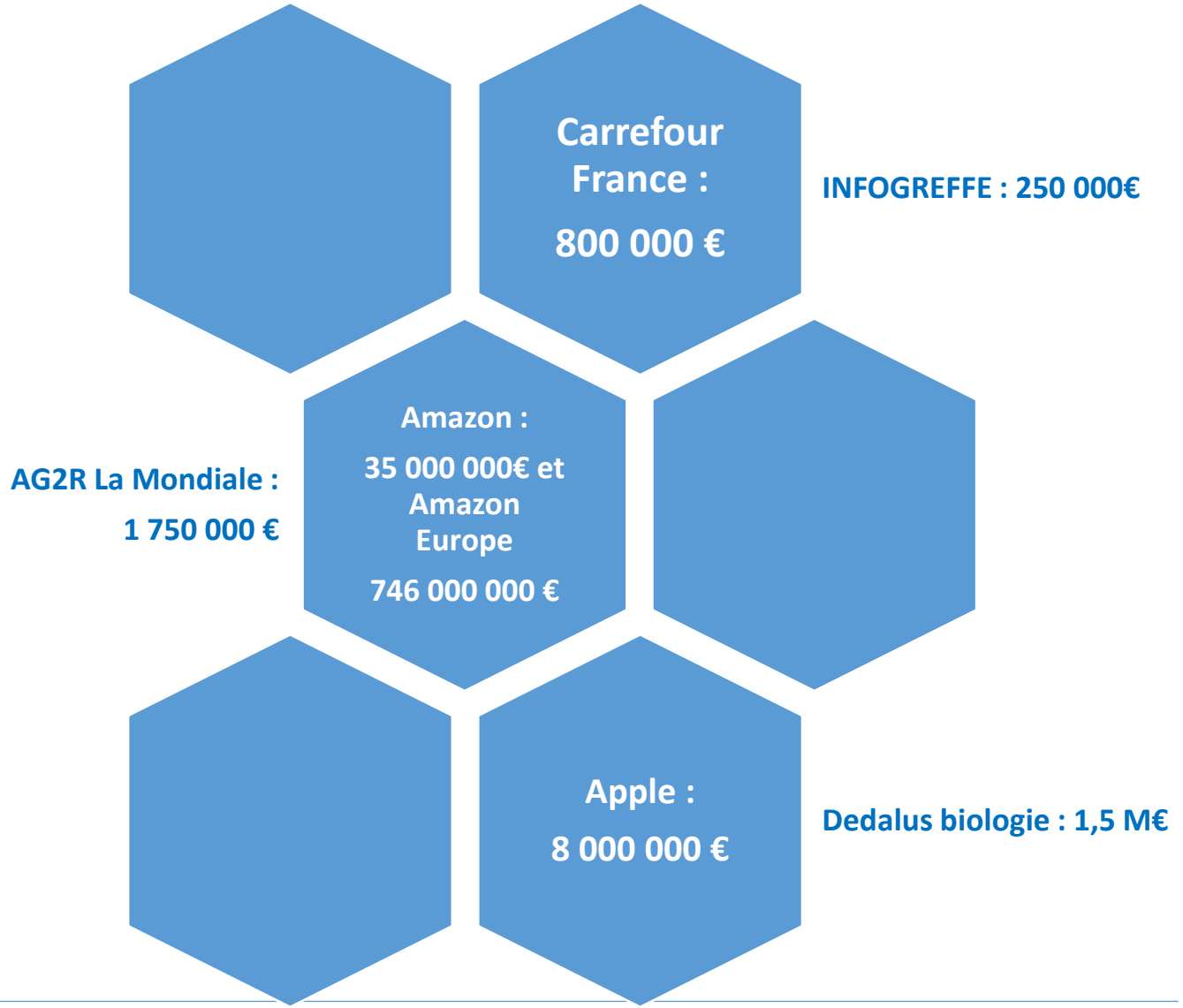
(214 106 000 euros en 2021)

A FHSJ contrôle de la CNIL
→ 03/07/2020
Contact tracing
2 juristes, 1 ingénieur, 1 auditeur des SI, 1 médecin

147 mises en demeure

Hôpital Marie-Lannelongue

Sanctions de la CNIL

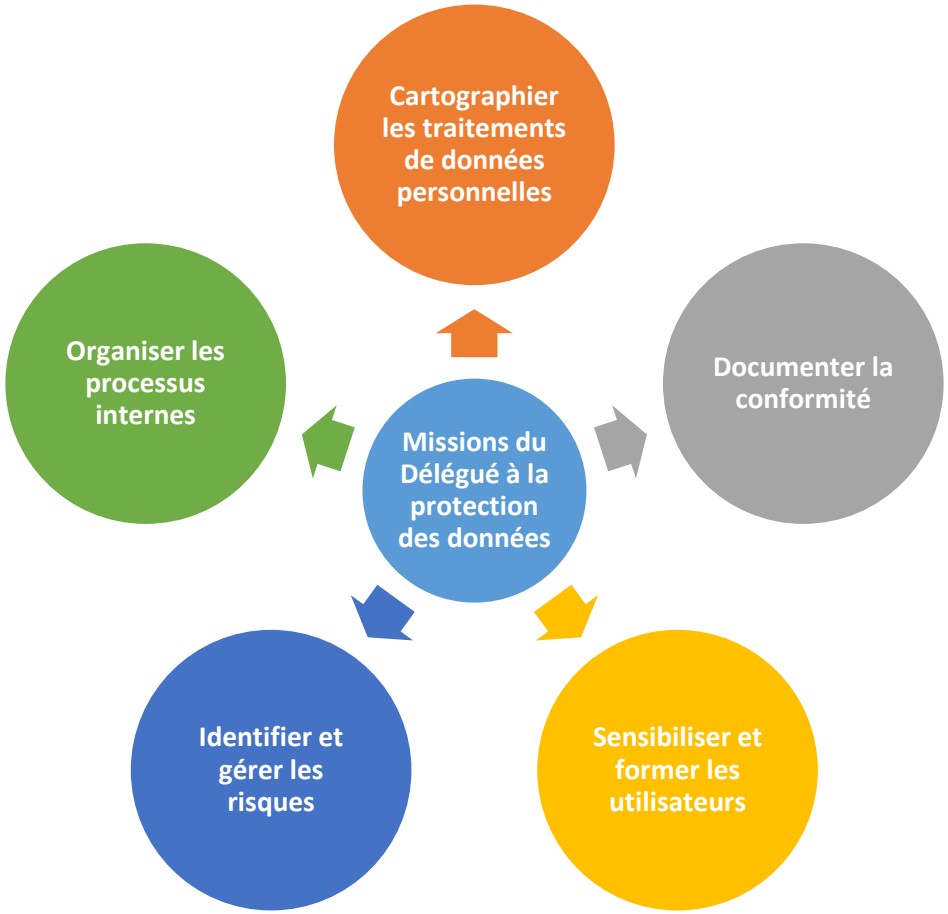


Les acteurs de la conformité

Hôpital
Marie-Lannelongue

Les acteurs de la conformité

- **Les acteur internes**
  - **Le DPO dpo@ghpsj.fr**
    - Nomination obligatoire lorsqu'il s'agit d'un **traitement à grande échelle de données dites « sensibles »** (données de santé, données biométriques, opinions politiques, convictions religieuses…)
  - **Les référents RGPD**
    - Dans les Pôles et Directions sur les 2 sites
      - Participent au « Comité projet RGPD »
  - **La Direction de Services Numériques (DSN)**
  - **Tous les salariés**



- **Les acteurs externes**
  - **Les sous-traitants**
    - Sont également soumis à la même obligation règlementaire

Hôpital Marie-Lannelongue

Sécurité des données
→ implication de tous

Hôpital
Marie-Lannelongue

Pourquoi faut-il vous impliquer dans la protection des données sensibles ?

Données médicales, que vous allez vous-même saisir et consulter, font partie des données les plus personnelles et les plus sensibles ! Touchent à l'intime des individus

→ Responsabilité forte vis-à-vis des patients

Parce que vous allez travailler en France !

→ La France est rentrée dans le top 10 des pays les plus touchés par le piratage informatique… :-(

Sécurité des données → implication de tous

- En 2022 → 18 attaques ont touché des hôpitaux français
- Depuis le début de la crise sanitaire, les cybermenaces ont explosé de 400%

- **90%** de toutes les brèches de cyber sécurité sont causées par une **erreur humaine**
- **94%** des cyber-attaques se déclenchent à partir d'un **email**

- 2 types de cybercriminels
  - Groupes criminels très organisés → **€**
  - Les Etats → **cyber-espionnage (OIV)**

*OIV : Organisme d'Importance Vitale

Des incidents de plus en plus fréquents et graves…

CH Cahors → septembre 2022
Rançon demandée : 10 M€
Dommages : plus d'accès internet

Maternité des Bluets → octobre 2022
Rançon demandée : 900.000€
Dommages : consultations annulées, plus d'e-mail, logiciels endommagés

Hôpital de Castellucciu → mars 2022
Rançon demandée : 50.000€
Dommages : suspension des activités d'oncologie et de radiothérapie

GHT Cœur Grand Est → avril 2022 (Alerte du service cyber-veille du Ministère de la santé)
Vente des données sur le dark net pour 1,3 M$
Dommages : coupure de la totalité du système. + 7 mois fonctionne encore en mode dégradé

CHSF…

Hôpital Marie-Lannelongue

QUE FAIRE POUR SE PREPARER

Hôpital
Marie-Lannelongue

Formation RGPD et cybersécurité → en santé

OBLIGATOIRE → vous avez reçu une invitation dans votre boîte professionnelle

Hôpital Marie-Lannelongue

Le phishing ou hameçonnage

- - Définition
  - **forme d'escroquerie par email** qui consiste à prendre l'identité d'une entreprise connue et reconnue sur un email pour inciter les destinataires à faire une action

- - Campagne de phishing mars 2022 → 5% des salariés

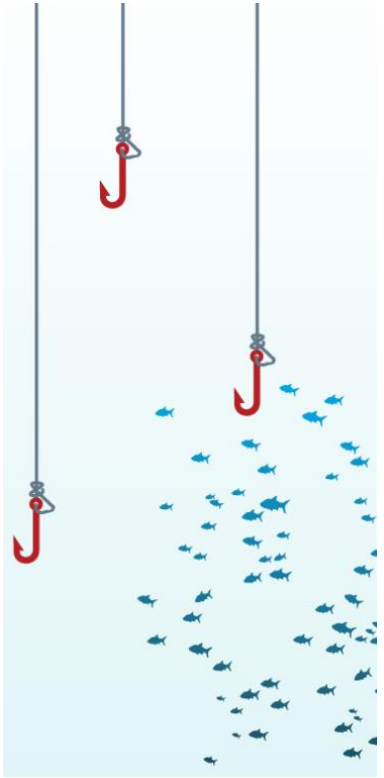
ont cliqué sur le mail et renseigné leurs informations personnelles

- - Campagne de phishing octobre 2022 → 14% des salariés

ont cliqué sur le mail et renseigné leurs informations personnelles

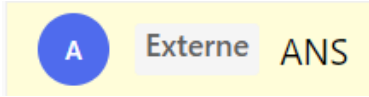
- - Campagne de phishing avril 2023 → 5% des salariés

ont cliqué sur le mail et renseigné leurs informations personnelles



Bonnes pratiques

- **Vos mots de passe**
  - Recommandations CNIL :12 caractères minimum et au moins 4 types suivants majuscule / minuscule / chiffre / caractère spécial
- **Phishing**
  - Ne jamais transmettre votre mot de passe après avoir cliqué sur le lien d'un mail (phishing…)



→ le service informatique ne vous demandera jamais votre mot de passe par mail

- **Utilisation des ordinateurs et logiciels**
  - Sur un poste individuel : toujours verrouiller le PC quand vous vous absentez de votre poste

  - Sur un poste de travail partagé : **toujours se déconnecter des applications quand vous avez fini**
  - **Ne pas conserver de données sensibles sur le C: de son PC Portable, risque de violation de données en cas de vol ou perte. Les données ne sont pas sauvegardées → 72h pour déclarer à la CNIL**
  - Signaler sans délai les problèmes informatiques **securite.informatique@ghpsj.fr**
- **Utilisation de vos smartphones ou équipement personnels**
  - Ne pas divulguer de données d'un patient, d'un salarié : message sur les réseaux (whatsApp, facebook, …), prise de photo (attention aux copies dans le cloud, envois à des tiers…)
  - En télétravail ne pas laisser le VPN ouvert si vous n'en avez pas l'utilité.

Bonnes pratiques

- **Supports externes**
  - **N'utilisez pas de supports externes (clé USB, disque dur externe)**
    - **Entre la maison et le travail → sur les postes de travail de l'hôpital (plus grand vecteur de virus…)**
  - **Ne jamais connecter à un PC, une clé USB trouvée (si elle n'a pas de propriétaire)**
  - **Ne pas recharger son téléphone portable directement sur un PC**

- **Vos communications vers l'extérieur**
  - L'utilisation de Bluefiles pour vos envois contenant des DCP, par mail hors @ghpsj.fr. Maryline Fleury mfleury@ghpsj.fr

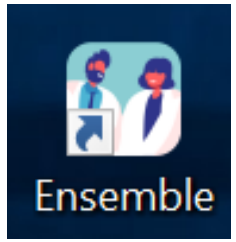
- **L'utilisation du Wifi à l'extérieur → perso**
  - Ne pas utiliser de connexion wi-fi publique (gare, bar, restaurant…)
    - « N'ouvrez jamais vos emails ou vos comptes bancaires sur une connexion internet publique » dit le hacker expert Frank Abagnale, « certains fraudeurs créent de fausses connexions qui semblent réelles afin de vous inciter à vous connecter et partager vos informations ».

- **« Juice jacking » → perso**
  - Danger des stations de recharge USB publiques (hôtels, centres commerciaux, aéroports, gares…). Les criminels peuvent introduire des logiciels malveillants et des logiciels de surveillance et voler les données de votre smartphone.

    → votre propre chargeur et cordon USB

Bonnes pratiques

- ✓ **Les documents relatifs à la protection des données et au règlement de de l'établissement :**
  - ✓ Le règlement intérieur
  - ✓ Le guide des réseaux sociaux
  - ✓ La charte d'utilisation des systèmes d'information



- ✓ **« l'Espace métier RGPD »**
  - ✓ Ensemble GHPSJ
  - ✓ Support de sensibilisation/formation dans l'espace **« Formations »**
  - ✓ Lien d'accès aux **MOOCs** Tableau de bord | GHPSJ Formations (moocit.fr)

- ✓ **Trait d'union**
  - ✓ Informations sur le RGPD

Hôpital Marie-Lannelongue