PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

-

SENSIBILISATION À LA MISE EN CONFORMITÉ RGPD

13/03/2020

Déléguée à la protection des données

Sommaire

1

Les enjeux de la protection des données personnelles en France & en Europe

Protection des données à caractère personnel

« Ensemble des règles à respecter pour que la collecte, l'utilisation, la conservation, la divulgation et la destruction de données à caractère personnel d'un individu ne porte pas atteinte à ses droits et ses libertés ».

Pourquoi une nouvelle réglementation ?

QU'EST-CE QUE C'EST ?

Nouveau cadre européen de référence harmonisé en matière de protection des données à caractère personnel pour les résidents de l'Union européenne.

POURQUOI ?

Réponse à un **besoin d'adaptation du cadre légal aux évolutions technologiques** et sociétales.

QUEL EST SON OBJECTIF ?

Donner aux citoyens européens davantage de contrôle et de visibilité sur leurs données personnelles et l'utilisation pouvant en être faite.

QU'EST-CE QU'IL APPORTE ?

- **Plus de droits** pour les individus / Plus de transparence et de clarté
- **Responsabilité partagé** entre Responsable de traitement et sous-traitant
- **Des sanctions plus strictes** *(jusque 20 millions d'€uros d'amende et 4% du chiffre d'affaires)*

Quels sont les enjeux et les risques pour le MNHN de la mise en conformité au RGPD ?

Les enjeux

- Créer la **confiance** de nos clients, étudiants, partenaires et personnels
- **Sécuriser et valoriser** les données
- **Responsabiliser** les acteurs et les sous-traitants
- **Favoriser un développement harmonieux** de l'établissement

Les risques

- **Economiques et opérationnels**
  - Fichier non déclaré = sans valeur
  - Suspension temporaire de l'activité
- Risque « **réputationnel** »
  - Atteinte image
  - Perte confiance clients / partenaires
- **Sanctions** importantes
  - Administratives (CNIL)
  - Pénales (5 ans et 300 000 €)
  - Civiles
- **Action de groupe** *(introduction de Class action)*

2

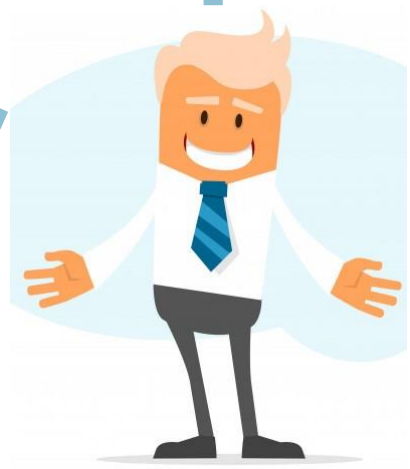
Quelques définitions et principes de la protection des données

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

Toute information, ou toute combinaison d’informations, relative à une personne physique susceptible d’être identifiée, directement ou indirectement.

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

Cartographie des données personnelles



Nom / Email / N° téléphone / Pseudo / Adresse IP

Identifiants

Age / Sexe / ADN

Biométrie

Intérêts / Opinions / Religion

Idéologie

Condamnations pénales et infractions

Criminologie

Identité

Soins / Traitements

Dossier médical

Santé

Contexte

Géolocalisation

Déplacement / Habitudes

Navigation

Consommation

Comportement

Finances

Transaction

Revenu

Communication

Relations

Famille / Amis / Contacts

Réseaux sociaux

Intérêts / Groupes / Opinions

Contenus

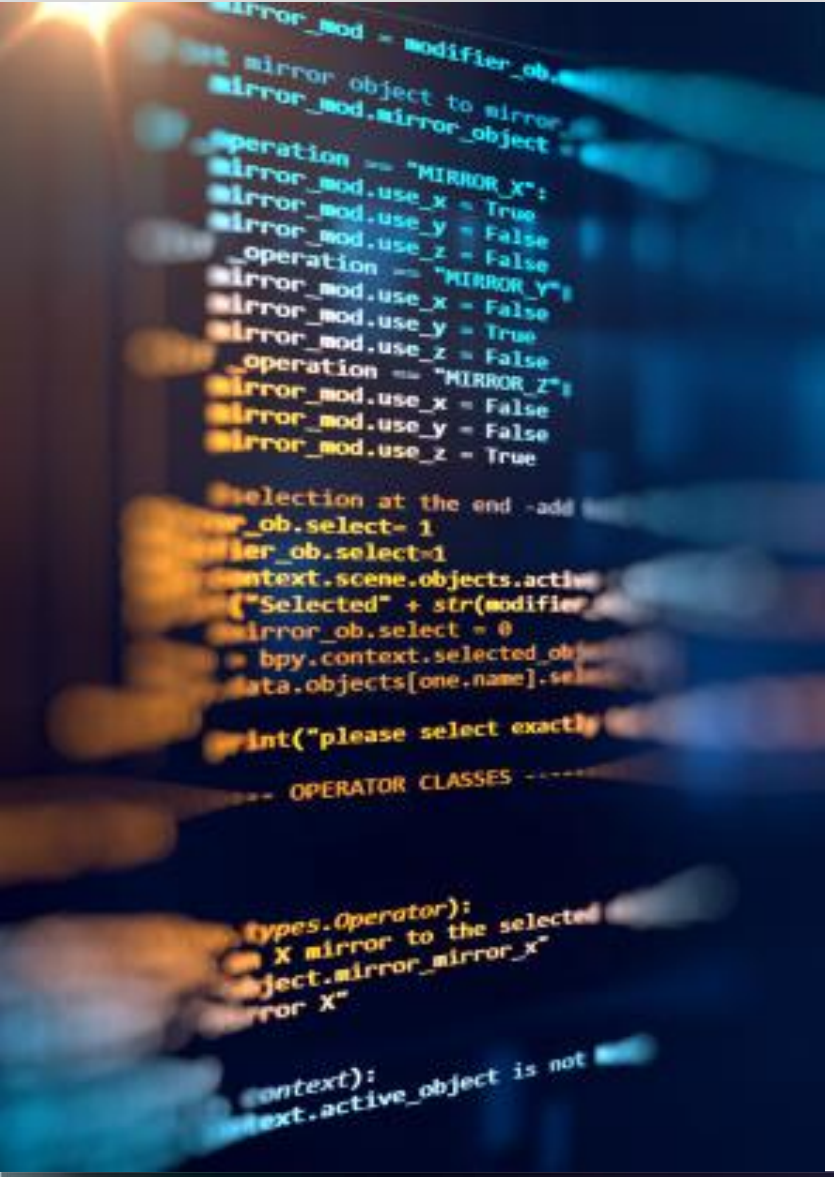
Conversation

Métadonnées / SMS / Appels

Médias

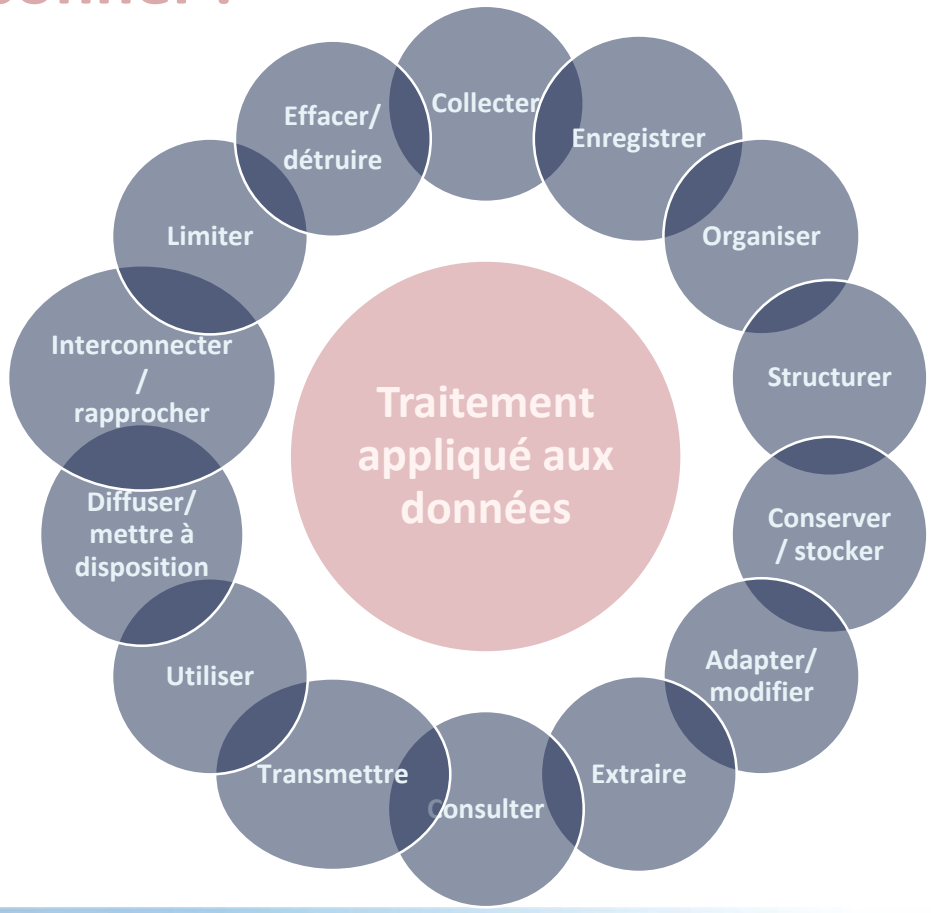
Photos / Vidéos / Podcast

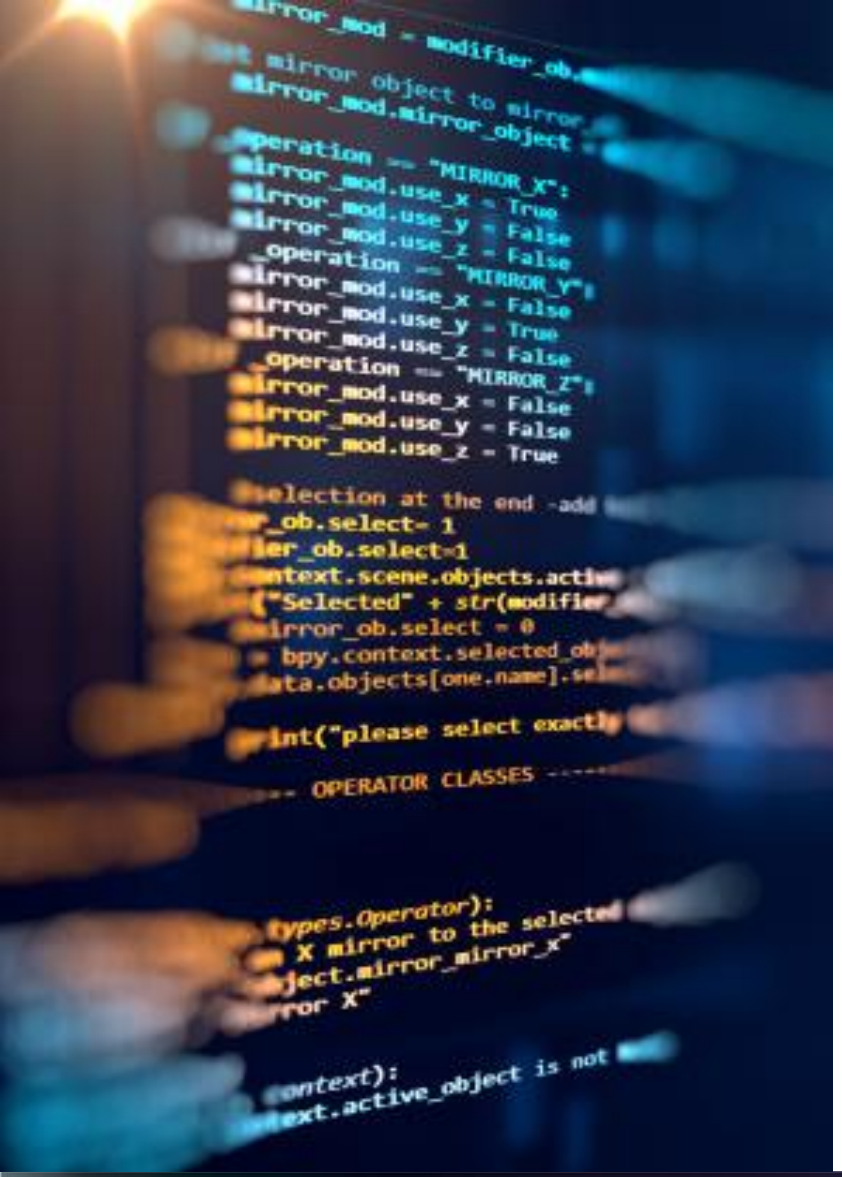
Source : serdaLAB



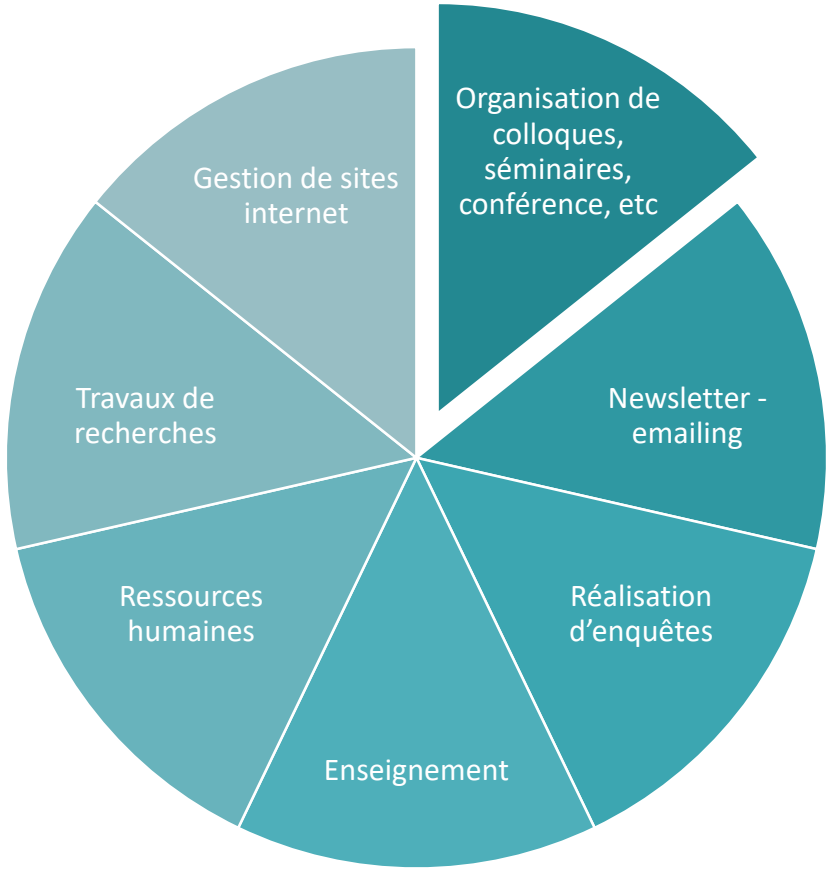
Qu’est-ce qu’un traitement de donnée à caractère personnel ?

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, […].





Quelques unes de vos activités de traitement



Qu’est-ce qu’un fichier de donnée à caractère personnel ?

Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

De quoi parle-t-on ?

Cela peut être une base de données, un tableau Excel, un listing Word, un classeur

Informatisés mais pas uniquement

Ficher papier organisé selon un plan de classement, formulaires papier nominatifs, dossiers classés par ordre alpha ou chrono

Exemples

Annuaire, Feuille d’émargement, Fichier de suivi de candidatures, Fichier Excel de suivi de demandes de formation

Les principes clés de la protection des données personnelles

1 - Licéité du traitement

2 - Finalité du traitement

3 - Minimisation des données

4 - Conservation limitée des données

5 -Obligation de sécurité

6 - Transparence

7 - Droits des personnes

8 - Accountability

Avoir une logique de questionnement RGPD avant toute activité de traitement de données, avant de déterminer si on utilise un outil ou une donnée

Les acteurs de la protection des données à caractère personnel

Responsable de traitement (RT)

Détermine les finalités du traitement et les moyens utilisés

- Les finalités de traitement sont les objectifs du traitement : pour quelles raisons traite-t-on les données ?
- Les moyens de traitement sont les mesures techniques et matérielles mises en œuvre (stockage, sécurisation, …)

Le RT est **celui qui en porte la responsabilité**.

Co Responsable de traitement (co-RT)

Décide conjointement des finalités et moyens de traitement des données

- Les co-RT doivent définir de manière transparente leurs obligations respectives aux fins d'assurer le respect des dispositions légales en matière de protection des données via un accord dont les grandes lignes seront mises à la disposition de la personne concernée par le traitement

Sous-traitant (ST)

Participe à la mise en œuvre du traitement pour le compte du responsable de traitement

- doit se conformer aux instructions et exigences du RT
- partage la responsabilité avec le RT en cas de violation de sa part de ses obligations légales et contractuelles

Délégué à la protection des données (DPO /DPD)

Pilote la conformité en matière de protection des données au sein de son organisme, en charge de :

- informer et conseiller le RT ou le ST, ainsi que leurs employés ;
- contrôler le respect du règlement et du droit national en matière de protection des données ;
- coopérer avec la CNIL et être le point de contact de celle-ci.

3

Les principaux outils de la conformité au RGPD

Les principaux outils de la conformité

Registre des activités de traitements

Outil de pilotage majeur

- **Recense** les différents traitements existants
- Permet de connaitre le **niveau de conformité** de chaque traitement

Privacy by design / by default

- **Respect de la vie privée dès la conception :** prendre en compte dès le début les exigences en matière de protection de la sphère privée/protection des données

et

- **intégrer les outils de protection directement dans le produit**, au lieu de les ajouter ultérieurement sous forme de compléments.

Analyse d'impact sur la vie privée

Outil de gestion des risques d'un traitement pour :

- décrire le traitement,
- en évaluer la nécessité & la proportionnalité
- aider à gérer les risques sur droits et libertés
- déterminer les mesures nécessaires pour y faire face

Notification des violations de données

Obligation de notifier une violation

- **A la CNIL** au plus tard dans les 72h après en avoir eu connaissance
- **À la personne concernée** lorsque cette violation est susceptible d'entrainer un risque élevé pour les droits et les libertés de la personne

Une violation peut être due à une faille de sécurité, un accident, une erreur, une malveillance

4

Mise en conformité : Comment conformer vos activités au RGPD ?

Comment conformer vos activités au RGPD ?

Structure des fichiers : des bases : savoir si je suis en présence de données à caractère personnel (DCP) ?

Non :
la réglementation ne s'applique pas

Oui :
un traitement de données est-il mis en œuvre ?
Exemple : connexion à une base de données avec authentification pour accéder au contenu de la base

Je suis donc concerné et je dois donc appliquer les principes de la réglementation.

Point de départ de la mise en conformité de vos activités au RGPD

Avant de mettre vos traitement et leur environnement en conformité,
2 points importants :

1. Savoir localiser les données : cartographier vos données personnelles
2. Établir la responsabilité des différents acteurs

Approche Privacy by design de la mise en conformité de vos activités au RGPD

Pour se conformer, il faut partir ou repartir sur de bonnes bases :
S'assurer du respect des principes de la protection des données à caractère personnel

Dans quel objectif je collecte les DCP ?	Toutes les données que je collecte sont-elles nécessaires ?	Sur quelle base légale je collecte ces DCP ?
Est-il nécessaire d'obtenir un consentement ?	Ai-je informé les personnes ?	Leur ai-je donné les moyens de pouvoir exercer leurs droits ?
Ai-je défini une durée de conservation pour ces données ?	Ai-je limité l'accès aux données et sécurisé les transferts ?	Ai-je sécurisé mes contrats avec mes prestataires ?

5

Checklist de la mise en conformité avec le RGPD

Check-list de la mise en conformité avec le RGPD

- Cartographier / recenser les traitements
- Réviser les contrats avec les prestataires / sous-traitants
- Réviser les formulaires de collecte et les mentions d'information
- Sécuriser et gérer les habilitations
- Définir des durées de conservation des données
- Sensibiliser les collaborateurs
- Mettre en place des procédures et politiques

MUSÉUM NAL HIST NATURELLE

MERCI !
DES QUESTIONS ?

Déléguée à la protection des données
Estelle Bervas-Clerc
dpo@mnhn.fr