inventeurs du monde numérique

Mise en oeuvre du RGPD

Mise en oeuvre du RGPD

Rappel réglementation

Réglementation en vigueur

Réglementation : le Règlement Général sur la Protection des Données (RGPD) du 14 avril 2016, la Loi Informatique et Libertés du 20 juin 2018

Acteur : Commission Nationale de l'Informatique et des Libertés (CNIL)

Obligations

- Renversement de la charge de la preuve (*Accountability)*
- Mesures techniques et organisationnelles *(Privacy by design)*
- Minimisation des données (*Privacy by default*)
- Notification des violations de données perso à la CNIL et aux personnes concernées

Renforcement du droit des personnes

- Transparence / Consentement renforcé / Rectification et effacement / Droit d'opposition

Sanctions

- Administratives / Financières

Mise en oeuvre du RGPD

Actions en cours

Actions en cours

Sensibilisation

- Tour des centres / Réunions avec directions générales et fonctionnelles
- A venir : Mooc formation au RGPD

Conseil pour la mise en conformité

- Expérimentations / Applications du SI / Bases de contacts / Sondages
- Demande avis à la DAJ Inria et à la CNIL
- Inscription dans registre des traitements

Traitement des demandes d'exercice de droit et des signalements de non conformité

- Dialogue avec la direction fonctionnelle concernée
- Demande avis à la DAJ Inria et à la CNIL

Traitements à risque

- Analyse impact initiale / Echelle de sensibilité / Dossier d'homologation
- Réunions avec le Comité d'éthique Inria (COERLE)

Actions en cours

Travail avec la DAJ

- Annexe RGPD pour contrats partenariat de recherche
- Mise en conformité du formulaire de consentement
- Recommandations RGPD pour montage expérimentations

Contact avec DPO des EPST et de SUPDPO

- Réunions / partage d'expérience

Relations avec la CNIL

- Présentation de démarche mise en oeuvre du RGPD chez Inria

Mise en oeuvre du RGPD

Projet de gouvernance de protection des données

Documents Inria de la gouvernance

Politique Générale de Sécurité de l'Information

→ **amendement**

PSSI

Plan annuel de la SSI

Règlement intérieur / Charte informatique

→ **amendement**

Politique de Protection des Données personnelles

→ **rédaction**

Processus internes

→ **rédaction sur intranet**

Plan annuel de protection des données personnelles

→ **rédaction**

Acteurs de la gouvernance

PDG

- **Décision** : Responsable des Traitements d'Inria
  - PDG ?
  - **Ou** Directeur de Centre et Directeur Général et Directeur Fonctionnel ?

DG / ComDir / RSSI / DSI et Ligne SI / Directeur fonctionnel
COSS ISSI / Chefs de projet scientifiques ou Techniques / Partenaire

DPD

- **Décision :** fréquence des audits DPD par an ?

Directeurs de Centre et Directeur Général et Directeur Fonctionnel

- **Décision :** Responsable application politique : Directeur de Centre et DG et DF ?

Comité éthique

- **Décision** : Comité éthique valide étude d'impact pour la vie privée ?

Politique de Protection des Données personnelles

Responsable de Traitement / Sous-Traitant / Responsabilité conjointe

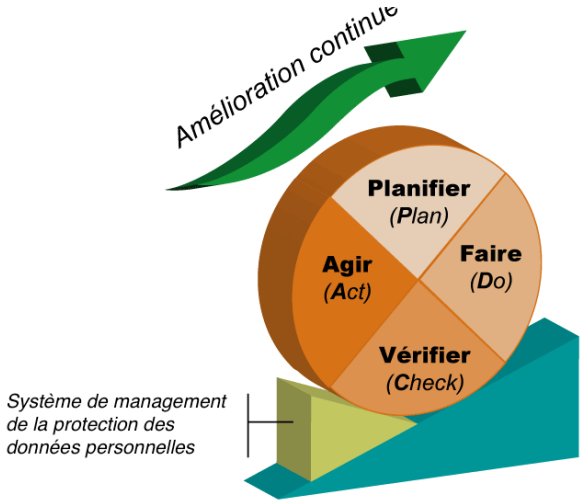
- Obligations

Gestion de la conformité

- Documentation de la conformité
- Conseils sur la conformité
- Contrôles de la conformité
- Gestion des non conformités

Exercice du droit des personnes

- Types de droits



Politique de Protection des Données personnelles

Sécurisation des traitements

- Mesures techniques et organisationnelles / Minimisation des données
- Conservation des données
  - **Décision :** comment les données sont conservées ?

Traitements comportants des risques pour les personnes concernées

- Analyse de conformité (Relais protection des données) + Analyse de risque (CSSI)
- **Décisions :**
  - Dossier d'homologation obligatoire ?
  - Commission d'homologation pour expérimentations avec données sensibles ?
  - Expérimentations passant devant un CPP doivent être soumises au Comité d'éthique ?

Transfert hors UE

- Pays adéquats / Pays non adéquats

Politique opérationnelle

Fiches réflexes

- Violation de données personnelles
- Contrôle de la CNIL
    - **Décision :** qui est le responsable des lieux : Directeur de Centre ?

Processus internes

- Exercice droit des personnes
- Déclaration d'un traitement
- Mise en conformité
    - Expérimentations
    - Applications du SI
- Organisation capacité de démontrer la conformité

Organisation documentation de la conformité

Registres

- Violations de données personnelles
- Demandes exercice des droits
- Signalement de non conformités
- Traitements Responsable de traitement
- Traitements Sous-Traitant

Mises en conformité

- 1 dossier par traitement mis en conformité
  - Déclaration traitement / Suivi conformité / Analyse impact
  - Contrat / Annexe RGPD, etc
- Points de suivi Juristes / DPO

Etudes DPO

- Ex : Inria Alumni

Sensibilisations

- Tour des centres

Merci

Anne Combe - Déléguée à la Protection des Données

Direction Générale