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 incidents de sécurité 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

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

- Dossier d'homologation
- Réunions avec le COERLE (Comité d'éthique Inria)

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

Rédaction d'informations sur intranet

- Déclaration de traitement
- Mise en conformité d'un sondage

Contact avec DPO des EPST

- 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** : RT = PDG **ou** Directeur de Centre **ou** Responsable Equipe / Service ?

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 CSSI et Relais Protection des Données personnelles

- **Décisions :**
  - Responsable application politique = Directeur de Centre **ou** Responsable Equipe / Service ?
  - Relais protection des données sous responsabilité du Directeur de Centre ?

COERLE

- **Décision** : quel rôle pour le COERLE dans la validation étude d'impact pour la vie privée ?

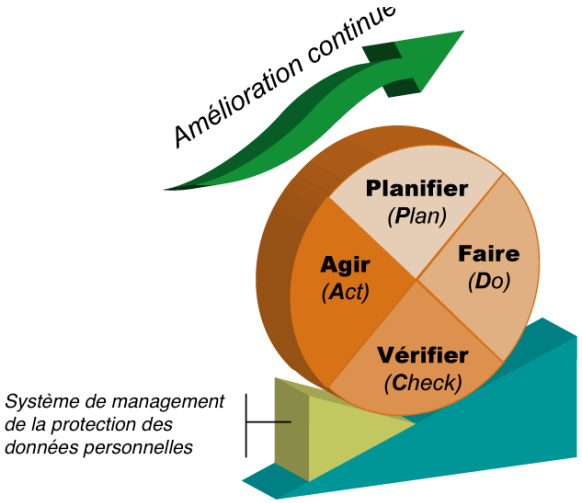
Politique de Protection des Données personnelles

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

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 ?
  - COERLE : commission d'homologation pour expérimentations manipulant données sensibles ?
  - Expérimentations passant devant un CPP doivent être soumises au COERLE ?

Transfert hors UE

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 du droit des personnes
- Déclaration d'un traitement
- Pour les juristes et CSSI des centres
- Organisation de la capacité de démontrer la conformité
- Documentation d'un projet ou d'une expérimentation

Actions septembre - décembre 2018

Septembre - Octobre 2018

- **Rédaction** sur intranet des **fiches réflexes et processus internes**

Novembre 2018

- **Rédaction** sur intranet des objectifs et règles de la **Politique de protection des données personnelles**

Décembre 2018

- **Rédaction** du document de **Politique de Protection des Données personnelles**
- **Rédaction** amendement de la **PGSI**

Actions janvier - mars 2019

Janvier 2019

- **Soumission** Politique de Protection des DCP **/** Amendement PGSI
- **Rédaction** **Lettre de mission pour juristes des centres**
- **Rédaction** **Plan 2019 de protection des données personnelles**

Février 2019

- **Soumission** Lettre de mission pour juristes et Plan 2019 protection des DCP
- **Rédaction** amendement de la **charte informatique**
- **Recensement** à grande échelle des traitements d'Inria
    - priorité : **expérimentations et recrutement**

Mars 2019

- **Soumission** amendement de la **charte informatique**

Merci

Anne Combe - Déléguée à la Protection des Données

Direction Générale