

Fiche mémo CYBER

RGPD = Règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE)

DPIA = il s'agit d'une analyse d'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Le PIA en revanche est le logiciel open source délivré par le CNIL qui facilite la conduite et la formalisation d'analyses d'impact relatives à la protection des données en toute conformité telles que prévues par le RGPD.

- Dans quel cas ?

On effectue ces traitements lorsque les données personnelles sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Qui est en charge de la protection des données au sein de l'entreprise ?

C'est le DPO qui a pour responsabilité la protection des données personnelles collectées et traitées par l'entreprise qui l'emploie. La CNIL met à disposition un guide pratique du DPO.

Def = Data Protection Officer

Mise en conformité

- Identifier les données personnelles
- Cartographier les traitements de données
- Évaluer les risques
- Nommer un DPO si nécessaire
- Mettre en place des mesures de sécurité
- Obtenir un registre des activités de traitement
- Élaborer des politiques de confidentialité
- Former le personnel
- Répondre aux demandes des personnes concernées

CNIL = La commission nationale informatique et liberté est chargée du contrôle de l'application du RGPD en France.

Obligations CNIL=

- Informer les personnes de leurs droits (mentions légale CNIL)

Droit de savoir ce qui est fait de mes données et si elles seront ou non partagées à des tiers.

Droit d'accès à une copie de mes données, aux modalités de traitement et finalités

Droit de s'opposer pour motif légitime au traitement de mes données en retirant mon consentement initial

Droit de rectifier mes données sans contraintes, ni délais excessifs

Droit à l'oubli quand mes données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées

Droit de regard sur le traitement automatisé de mes données

Droit à la portabilité de mes données pour les réutiliser à mes propres fins.

Droit à la limitation temporaire du traitement de mes données en cas de contestation

- Assurer la sécurité des données

- Respecter les règles spécifiques aux données sensibles

- Recenser

permet d'avoir une vision claire et globale des activités de la collectivité qui nécessitent la collecte et le traitement de données personnelles

- faire le tri des données

- Respecter

informer les personnes dont vous traitez les données

organisez et facilitez l'exercice des droits des administrés et des agents

-sécuriser les données

l'accès illégitime aux données

leurs modification non désirée

disparition

- Analyse d'impact

Installer xxd :

Sur linux cliquer en hauts a gauche sur application
sélectionner système gestionnaire symstuc de paquet

configuration depot selectionet les paquet de Nantes
chercher xxd et cliquer sur sélectionner pour installation installer le et appliquer

echo pour convertir de binaire

```
root@debian-xfce:~# echo "obase=2;54" | bc |
```

Numero de conversion

numero a convertir

Hashing-blowfish

<-c> pour chiffrer symétriquement avec paraphrase

<.gnupg> le point ici avant le ,, sert à indiquer que c'est un répertoire caché

passPhrase:phrase secrète

commande linux : file [nom du fichier] → nous donne l'info de comment il est chiffrer

gpg --decrypt aes256 nom du fichier

AES

gpg -c --cipher-algo aes256 NomFichier

gpg --decrypt aes256 NomFichier.gpg

disque SANDISK 1 TO SSD EXTERN

gpg --full-gen-key → Génère une nouvelle clé

Exportation de la clé public

gpg --output <la chaine qui vous convient le mieux.asc> --armor --export <le nom que vous avez saisi pendant la génération des clés>

2 SSH Secure SHell

shell = programme=automatise les taches

Vérifiez si un serveur ssh est déjà installé sur votre système → systemctl | grep ssh

1. d=serveur installé sur la machine =daemon

windows commande : arp → savoir l'adresse ip de connection de notre ordinateur

tracert googl

Certificat possède :

clés privé

certificat → auto-certifié

→ certifier par une autorité (WAN)

TLS pour Transport Layer Security

L'intérêt est de garantir la confidentialité des données notamment en cas de vol d'un ordinateur portable ou simplement pour mettre en place une politique de moindre privilège renforcée par le chiffrement. (less privilege)

cœur de réseaux → plein de routeur connecter entre eux

IDS → Intrusion detection systeme

-Faille

- *\$*
- *Opinion*
- *Piège à miel*

-pour éviter cela

- *Least privilege*
- *Defense in depth*
- *Open Security*