TP 1 : Comment mettre en place ces 6 mesures ?

COURS : REGLEMENT EUROPÉEN GENERAL SUR LA PROTECTION DES DONNEES

BLOC 3 : CYBERSECURITE DES SERVICES INFORMATIQUES

Durée du travail : 04H00 – Travail de groupe

En vous rendant sur cette page du site internet de la CNIL, répondez par écrit

et **de manière structurée** au sujet suivant :

Comment, dans les faits, mettre en place ces 6 mesures ?

Voici une liste de questions permettant de vous aider à la réponse du sujet principal. Ces questions subsidiaires doivent-elles aussi trouver réponses dans votre travail de recherches. Si vous souhaitez effectuer des recherches sur des sites internet annexes c'est votre choix, mais sachez que toutes les réponses aux questions ci-dessous sont disponibles sur le site susmentionné.

La désignation d'un délégué à la protection des données

- Qui peut être délégué ?
- Quels sont les rôles du délégué ?
- Est-il toujours obligatoire d'élire un délégué ? Existe-il des cas particuliers ?
- Comment devenir délégué à la protection des données ?
- Quelles sont les étapes de désignation d'un DPO ?
- Comment se passe la fin de mission d'un DPO ?
- Quel est le statut du DPO ?
- Chaque organisme doit-il avoir un délégué différent ?
- Quels sont les moyens d'action du délégué ?
- Existe-il des certifications de compétences pour les DPO ? ○ Quels organismes sont agréés pour dispenser ces formations ?

Cartographier vos traitements de données personnelles

- Quels sont les recensements précis à effectuer ?
- Quels sont les différents traitements pouvant être effectués ?
- Existe-il différentes catégories de données personnelles ? ○ Quels sont les objectifs de cette cartographie ?
- Développez les acteurs qui rentrent en jeu.
- Développez les flux de données qui rentrent en jeu.
- Développez le QQOCQP.
- À quoi ressemble un registre de base ?

Durée du travail : 04H00 – Travail de groupe

Prioriser les actions à mener

- Quelles sont les actions à mettre en place pour vous conformer aux obligations ?
- Quels sont les éléments de priorisation ?
- Quels sont les points d'attention sur lesquelles vous devez travailler ?
- Existe-il des points d'attention particuliers ?
- Quelles sont les particularités de la sous-traitance ?

Gérer les risques

- Qu'est-ce qu'un risque ?
- Qu'est-ce qu'une analyse d'impact ?
- Quels sont les piliers d'une AIPD ?
- Quand réaliser une AIPD ?
- Quels sont les 9 critères de définition du risque ?
- Quelles sont les personnes qui participent à l'élaboration d'une AIPD ? ○ Qu'est-ce que PIA ? Comment fonctionne-t-il ?

Organiser les processus internes, violations de données et demandes d'accès

- Qu'est-ce qu'un processus ?
- Quels processus doivent être mis en place lors de la collecte ? ○ Quelles sont les informations à fournir lorsque des données personnelles sont collectées ?

- Qu'est-ce qu'une violation de données à caractère personnel ?
- Que doit-il se passer en cas de violation de données ? ○ Qu'est-ce qu'une notification ?
- Quels sont les délais légaux de notification d'une violation ?
- Quelles sont les 5 étapes d'une notification ?
- Que va faire la CNIL après votre notification ?
- L'obligation de notifier à l'autorité de contrôle peut-elle être confiée au sous-traitant ?
- Quels sont les pouvoirs de la CNIL en matière de violation de données ?
- Quelle est la plateforme Nationale d'assistance aux victimes d'actes de cyber malveillance ?
- Qu'est-ce qu'une demande de droit d'accès ?

- Quelles sont les 4 étapes de la demande d'un droit d'accès ?
- Peut-on refuser de répondre à une demande de droit d'accès ?
- Qui peut exercer une demande de droit d'accès ?
- Une justification d'identité doit-elle être obligatoirement demandé ?
- Qu'est-ce qu'un « doute raisonnable » concernant la vérification d'identité ?
- Quel est le coût d'une demande d'accès ?
- Une fois la demande d'accès réalisée, de quelles manières les données peuvent-elles être communiquées ?
- Que faire lors d'une demande d'accès si la gestion des données personnelles est sous-traitée ?

Documenter la conformité

- Quels sont les éléments qui doivent être documentés ?
- Quels sont les éléments qui doivent apparaître dans ce registre ?
- Qu'est-ce qu'un registre de traitement ?
- Un registre concernant les violations de données doit-il être tenu ?

Le site « Have I been pwned » disponible ici vous permet de savoir si vos données personnelles (adresse électronique, numéro de téléphone…) ont été trouvées dans une base de données piratée.

Le site « KASPERSKY Password Checker » disponible ici vous permet de connaître la robustesse de votre mot de passe ainsi que le temps nécessaire à sa résolution. Ce site vous indique également si votre mot de passe a déjà fait l'objet d'une fuite.

Dans le cours, nous avons évoqué le concept de **DATA GOUVERNANCE**. Prenez le temps qu'il vous reste pour ce travail afin de développer ce qu'est la DATA GOUVERNANCE.

➢ Pour aller plus loin dans ce chapitre, la CNIL à réalisé un MOOC gratuit et accessible à tous, disponible ici.