

# **SENSIBILISATION AUX NOUVELLES RÈGLES RELATIVES À LA PROTECTION DES DONNÉES (RGPD/GDPR)**

**CODE STAGE : P-AAMC**

## **OBJECTIFS**

Connaître les évolutions réglementaires imposées par le nouveau règlement européen  
Pouvoir Identifier les impacts sur les aspects organisationnels et sur les procédures internes  
Savoir préparer le plan d'actions de mise en conformité

## **DURÉE**

2 jours

## **PUBLIC**

Dirigeants, responsables juridiques et juristes, responsables informatiques, DSI, RSSI, responsables conformité, responsables RH et toute personne concernée par le traitement des données personnelles ou la mise en conformité des traitements au sein de son organisme

## **PRÉ-REQUIS**

Aucun

## **PROGRAMME**

**1ÈRE PARTIE : LES NOUVEAUTÉS APPORTÉES PAR LE RÈGLEMENT**

### **INTRODUCTION**

Les enjeux du nouveau règlement européen et les objectifs recherchés

Les définitions relatives aux données, aux fichiers et aux traitements

Les définitions relatives aux acteurs impliqués dans les traitements (responsable de traitement, tiers, sous-traitant, destinataire, personne concernée, code2utf('8230',0))

Les nouvelles définitions introduites par le règlement européen (violation de données, profilage, représentant, code2utf('8230',0))

## LES NOUVELLES RÈGLES DE GESTION IMPOSÉES PAR LE RÈGLEMENT

Transparence concernant les traitements de données à caractère personnel

La simplification des démarches administratives auprès de l'autorité de contrôle

Les nouvelles sanctions imposées par le règlement

La gouvernance européenne en matière de protection des données (comité européen, guichet unique, rôle des autorités de contrôle)

## LES OBLIGATIONS DU RESPONSABLE DE TRAITEMENT ET DU SOUS-TRAITANT

Les nouvelles obligations imposées au responsable de traitement (preuve du respect du règlement, sécurité des données, PIA, Privacy by Design, notification de violation de données)

Les nouvelles obligations imposées au sous-traitant et les clauses contractuelles à intégrer dans les contrats

Les actions à mener par l'entreprise pour se mettre en conformité

## LES DROITS DES PERSONNES CONCERNÉES

Les nouveaux droits des personnes concernées et les évolutions des droits existants concernant le traitement de leurs données

Les nouveaux droits de recours des personnes concernées

## LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Son rôle, ses responsabilités et ses missions

Sa désignation et son positionnement

Les contrôles de conformité au règlement

## LES TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL EN DEHORS DE L'UNION

## 2ÈME PARTIE : LES ACTIONS POUR SE METTRE EN CONFORMITÉ

### INTRODUCTION

Descriptions des actions à prévoir pour se mettre en conformité

La démarche méthodologique

### ORGANISATION ET RÉFÉRENTIEL

Les expressions de besoins et finalités des directions métiers Le lien avec le DPO

Le comité de pilotage, arbitrage, suivi et validation des projets

Le respect des politiques protection de la vie privée (interne et usagers) et sécurité des données à caractère personnel, déclinées dans la PSSI (les PSSI par typologie d'entreprise)

Les articulations avec les autres filières, (SSI), protection des installations, conservation des documents,

Les contrats

L'enregistrement dans le registre des traitements de données à caractère personnel

Les procédures SI de respect des obligations liées au consentement et aux devoirs

Informations

Les procédures de gestion des demandes d'accès, rectification, limitation, portabilité, et destruction des données à caractère personnel

La définition des niveaux de dommages sur la vie privée et la notification de violation de données à caractère personnel

La formalisation des points de contacts

LES TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL EN DEHORS DE L'UNION EUROPÉENNE

Les pays adéquats

Les garanties, les contrats, les règles d'entreprise contraignantes

Les dérogations

SÉCURITÉ

Security by default : contrôle d'accès, identification, authentification, habilitation et protection des échanges et des supports de données à caractère personnel

Security by design la méthodologie AIPD : les acteurs, les étapes (la formalisation du périmètre des données, les exigences légales non négociables, les événements redoutés pour la vie privée,

les sources de menaces, les menaces, les vulnérabilités,

les risques, les contremesures, la validation par le responsable des traitements), l'homologation et les outils

Le cas de l'externalisation : les PAS

LA GESTION DE LA PREUVE

Le contrôle

La labélisation

Les agréments

La certification

Les outils