e DataPrivacy

Formation
Ateliers

Groupe d'experts en protection de la donnée
spécialistes RGPD
'*DPO as a Service*'

Qui sommes nous ?

eDataPrivacy est née de l'initiative d'un groupe d'**experts séniors**.

Experts ayant de 15 à 25 ans d'expérience dans la protection des données, mise en conformité, certification, gestion de risques, auprès de grands groupes ou de petites structures.
L'approche est celle de l'accompagnement de l'entreprise dans la révision de ses process de gouvernance.
A partir des résultats d'un premier audit, nous établissons un plan d'actions qui s'appuie sur les forces de votre établissement et enrôle ses acteurs. Cette méthodologie vise à une meilleure compréhension du changement par l'ensemble des personnels. Cet audit est réalisé selon les recommandations de IAPP(*) et les modèles proposés par l'AICPA(**), nos experts certifiés maîtrisent l'ensemble de ces modèles et les ont expérimentés chez de nombreux clients.
Notre équipe met également à votre service ses outils et son expérience confirmée sur la mise en conformité au RGPD (Règlement Général de la Protection des Données).

Nous vous proposons ainsi une offre transverse : Diagnostic, gestion de risque, analyse d'impact, analyse de maturité, conduite de projet de mise en conformité.
eDataPrivacy met en place un accompagnement sur mesure à la hauteur des enjeux de votre entreprise et de son environnement.

(*) International Association of Privacy Professional
(**) American Institute of Certified Public Accountants

Ce document ne peut être reproduit sans l'autorisation d' e DataPrivacy

HYPOTHÉSE DE TRAVAIL POUR VOTRE MISE EN CONFORMITÉ AU RGPD

De l'identification des forces et faiblesses de l'entreprise jusqu'à l'accompagnement en routine, BAU (Business As Usual), les experts d'eDataPrivacy sont expérimentés sur l'ensemble des phases du projet. La méthode de travail est pragmatique et au plus près des personnels de l'entreprise. C'est une démarche collaborative qui permet de faciliter le transfert de compétences et donc une appropriation plus rapide par les personnels des nouveaux process mis en œuvre.

Audits de conformité

» Audits de traitements, solutions, procédures
» Analyse de risques
» Analyse de traitements et registres
» Audit du système d'information (cartographie des systèmes)

Programme de mise en conformité

» Liste des actions à mettre en oeuvre
» RACI, Budget
» Cartographie des traitements

Recommandations sur mesure

» Conseils sur la protection des données personnelles
» Stratégie de gouvernance
» Analyse des lois applicables

Développement de livrables

» Création des politiques et procédures de protection des données
» Modèles types de courriers
» Modèles types de clauses de protection des données

Mise en œuvre du programme & formation

» Gestion du programme
» Renégociation de contrats
» Formation du personnel
» Mise en place du registre de traitements

Privacy by Design

» Analyse des solutions
» Conduite des DPIA nécessaires
» Relations avec la CNIL
» Relations avec le groupe

Ce document ne peut être reproduit sans l'autorisation d' e DataPrivacy

SE METTRE EN CONFORMITE AVEC LE REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES

RGPD

En bref

LE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES :

Êtes vous prêt ?

e DataPrivacy

LE RGPD *EN BREF*

Termes et définitions

QUIZ

- Qu'est ce qu'une donnée ?
- Qu'est ce qu'une donnée personnelle ?
- Qu'est ce qu'un traitement ?
- Qu'est ce qu'un sous-traitant ?

Définitions

QUIZ

- Parmi ces données personnelles, quelles sont celles qui constituent des données sensibles ?

  - A - Une photographie
  - B - Une empreinte digitale
  - C - L'appartenance à un parti politique
  - D - La localisation géographique
  - E - La date de naissance
  - F - Le NIR

CONTEXTE LÉGISLATIF

LÉGISLATION SUR LA PROTECTION DES DONNÉES

RGPD
L'Europe s'attaque à la protection des données

Conformité

La loi « informatique et libertés »	La Directive européenne sur la protection des données	La loi pour une République numérique	au Règlement Général pour la Protection des Données
6 janvier 1978	24 octobre 1995	7 octobre 2016	25 mai 2018

27 AVRIL 2016

LE RGPD : CE QUI CHANGE ?

du déclaratif à la responsabilisation

Responsabilité
(« Accountability »)

Avec l'accompagnement du DPO, les entreprises doivent prouver qu'elles sont en conformité

Amendes élevées

→ 2% du CA ou 10 M€
→ 4% du CA ou 20 M€
Sanction du marché
Risque réputationnel

Protection des données dès la conception
(« Privacy By Design »)
La protection est un élément moteur des process de l'entreprise

DPO
Prérogatives renforcées,
rôle de conseil et
de sensibilisation au RGPD
mais aussi rapport privilégié avec la CNIL

L'analyse d'impact (« Privacy Impact Assessment »)
Une analyse d'impact du traitement doit être faite au préalable pour tout traitement de données personnelles présentant un risque important pour la vie privée

Violation de données personnelles
Le délai pour notifier la violation de données personnelles est désormais de 72 heures

LE RGPD : CE QUI CHANGE ?
du déclaratif à la responsabilisation

Responsabilité
(« Accountability »)

Avec l'accompagnement du DPO, les entreprises doivent prouver qu'elles sont en conformité

Internalisation de la censure ?

- Collecte loyale et licite des données
- Données sensibles interdites
- Finalité déterminée, explicite et légitime
- Respect du droit des personnes
- Proportionnalité
- Sécurité et confidentialité des données
- Durée limitée de conservation des données

- Responsabilité personnelle, pénale du dirigeant de l'entreprise
- Amende administrative
- Co-responsabilité
- Risque réputationnel

LE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES :

Êtes vous prêt ?

Les risques

Les sanctions

Outside

- **Pécuniaires :** Amendes.
  - *2% du CA (annuel mondial consolidé groupe) ou 10ME*
  - *4% du CA (annuel mondial consolidé groupe) ou 20ME*
- **Judiciaires :** Poursuites civiles ou pénales
  - *individus (trolling),*
  - *actions collectives,*
  - *autorités*

- **Réputationnel :** Dégradations de l'image
- **Économique :** Perte de clientèle

  Une entreprise en conformité doit exiger la conformité de ses fournisseurs

Inside

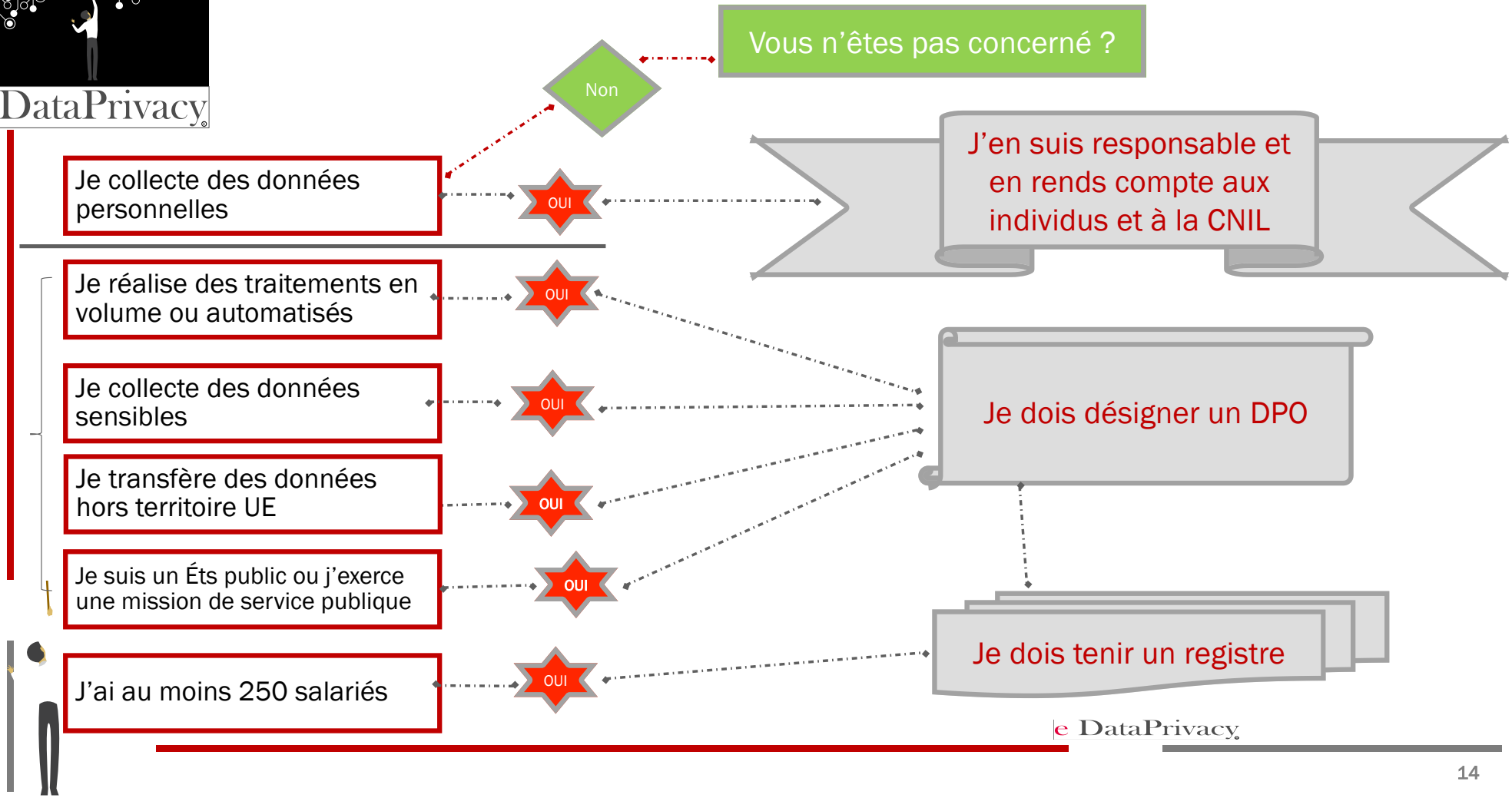
Si vous êtes en conformité, la principale sanction vient de l'intérieur de l'entreprise

LE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES :

Êtes vous prêt ?

RGPD ? SUIS-JE CONCERNÉ ?

Suis-je concernée par le RGPD ?



LE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES :

Êtes vous prêt ?

Mener son programme de mise en conformité

Partie 2 : Mener son programme de mise en conformité

1) Désigner une équipe projet du programme de mise en conformité

2) **Support de la direction** (ou des directions si programme mutualisé) : lettre de mission

3) Créer son équipe projet, quelques compétences clés :
   - CIL
   - Juridique / règlementaire
   - Informatique / sécurité

Partie 2 : Évaluer les risques

Quelques questions préliminaires :

Comment définir une méthodologie

Quel le périmètre prendre en compte ? Nb de services concernés, les personnes, les établissements partenaires ? Les autres administrations ?

Quelle maturité des services à la règlementation actuelle ?

Quelle maturité des services à la nouvelle règlementation ?

Comment cartographier les traitements ?

Comment cartographier les systèmes d'exploitation impactés ?

Comment recenser l'ensemble des pratiques actuelles de mon établissement ?

Partie 2 : Auditer ses services et traitements

Quel périmètre ?

Comment définir le périmètre du programme ? Nb de services concernés, les personnes, les établissements partenaires ? Les autres administrations ?

- Qui utilise des données personnelles dans l'établissement ?
- Pourquoi ?
- Quelques pistes : les activités qui nécessitent cette utilisation, des licences logicielles de BDD, des missions attribuées, une politique de droits d'accès, une arborescence dans les systèmes d'exploitation.

- Une définition : toute personne ou entité qui collecte, utilise, sauvegarde, héberge, vérifie, transfère, ou de quelque façon que ce soit directement ou indirectement traite une données personnelle est dans ce périmètre.

Partie 2 : Mesurer la maturité

Cartographier ?

Comment cartographier les traitements ?
Comment cartographier les systèmes d'exploitation impactés ?
Comment recenser l'ensemble des pratiques actuelles de mon établissement ?

- Préparer son registre :
- Recenser auprès de chaque service toutes les informations requises pour la tenue de ce registre
- Croiser les informations obtenues avec d'autres sources de recensement :
  - interrogation des systèmes d'information
  - Interrogation CNIL ou CIL (demande d'extraction)

- Attention 2 registres à tenir et recenser :
  - Registre du responsable de traitement
  - Registre du sous traitant

Partie 2 : Définir son plan d'actions

- Analyse des risques :
- Conclusions de l'audit : il permet d'identifier les points de force et de faiblesse de l'établissement.

- Conclusions de la cartographie : elle permet d'identifier les risques pour l'établissement et les points et secteurs à remédier prioritairement.
- Il faut définir le budget et le calendrier du programme de mise en conformité

- Plusieurs solutions :
  - Logiciel de mise en conformité
  - Embaucher
  - Conseil d'experts
  - Accompagnement d'experts
  - Mutualiser la démarche

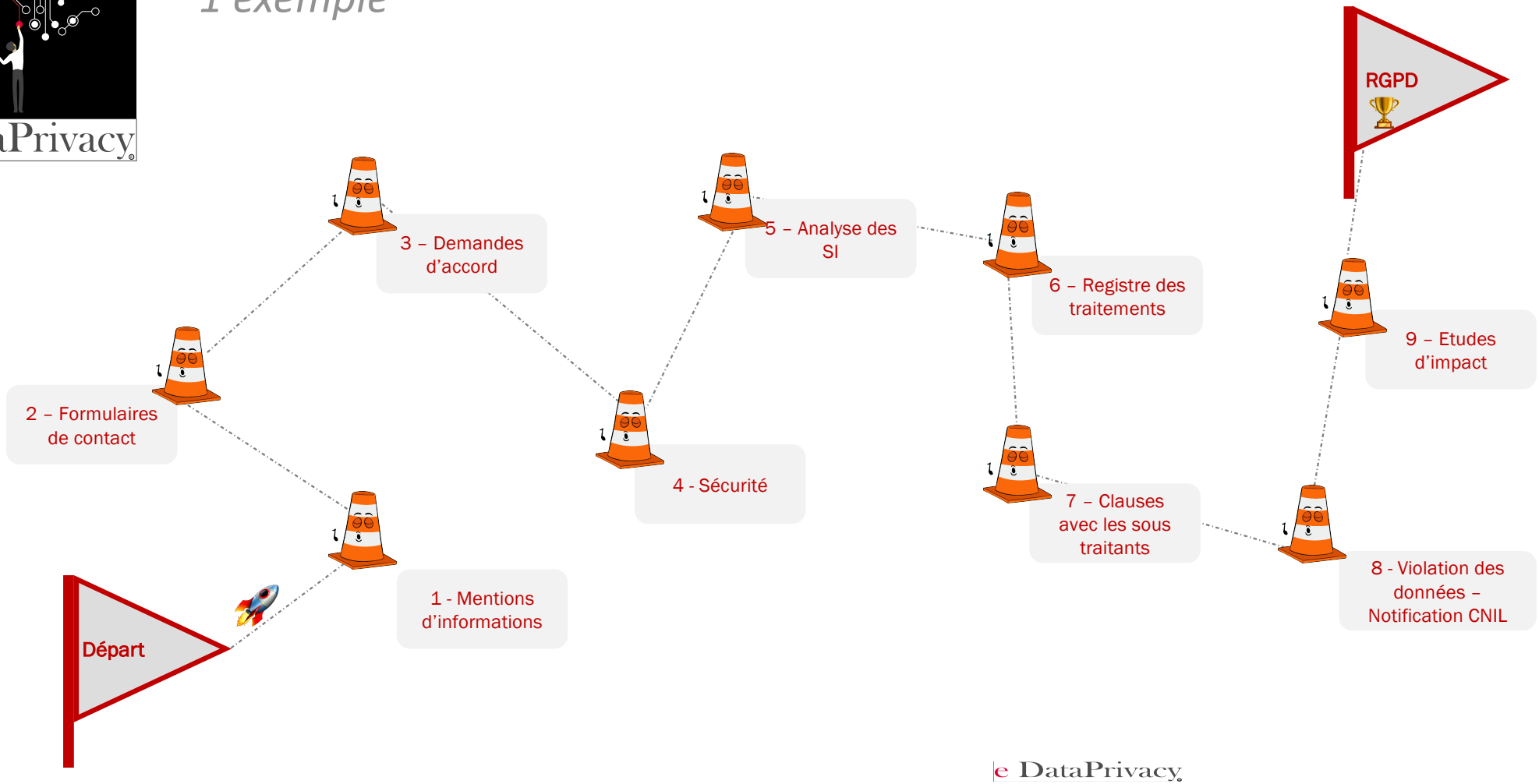
Partie 2 : Prioriser

- Les critères de priorisation sont établis :
- à partir des conclusions de l'audit, (forces / faiblesses)
- Du calendrier de ce règlement
- De l'exposition au risque de l'établissement

- Le règlement prévoit certaines procédures nouvelles à mettre en place et pour lesquelles la CNIL vérifiera non pas l'existence mais la mise en œuvre
  - Désignation d'un DPO
  - Registres
  - Qualité des consentements
  - DPIA
  - Politique de conservation des données
  - Formation des personnels
  - Politique de sécurité des données
  - Procédure de gestion des failles

Partie 2 : Prioriser les actions de sa mise en conformité

1 exemple



LE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES :

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le data Protection officer

- ✓ Désignation obligatoire notamment si :
  - -suivi “régulier et systématique” de personnes
  - -traitement à grande échelle de données sensibles
  - -En pratique, il est fortement recommandé dès lors qu’aucune fonction experte n’est disponible dans l’entreprise et celle-ci réalise des traitements directement ou indirectement sensibles.

- ✓ Son rôle :
  - -Informer, former et conseiller les opérationnels et la direction
  - -Mener des études de risques et d’impact (notamment les PIA obligatoires)
  - -Assister dans la mise en conformité au RGPD
  - -Contrôler/auditer le respect des process RGPD (accountability)
  - -Tenir le registre des traitements
  - -Être le point de contact des autorités

- ✓ Son statut :
  - -Expert en droit et informatique, interne ou externe
  - -Indépendant
  - -Reporte directement au plus haut niveau de direction

La désignation obligatoire d'un DPD/DPO

Une obligation du RGPD (Article 37)

Le RGPD impose aux organismes publics (collectivités, établissements publics, etc.) de désigner un délégué à la protection des données (ou Data Protection Officer en anglais) et ce quelque soit leur taille.

Article 37 - Désignation du Délégué à la Protection des Données

Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

La désignation obligatoire d'un DPO

La mutualisation/l'externalisation du DPO

- Mutualisation
  - *structures de mutualisation informatique (SMI)*
  - *exemples de CIL mutualisés (CNIL)*
  - *établissements publics de coopération intercommunale (EPCI)*
  - *mutualisation des politiques de sécurité informatique*

- Externalisation
  - *l'externalisation du rôle de DPO à un prestataire extérieur peut apparaître comme une solution stratégique tant au niveau de la gouvernance interne qu'au niveau des coûts.*

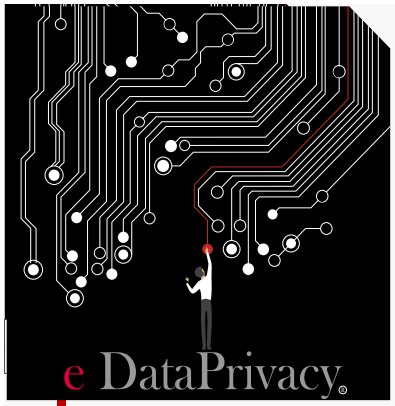
Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.

Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

e DataPrivacy



Patricia CHEMALI-NOEL

pchemalinoel@edataprivacy.fr

Expert senior protection des données - *RGPD*
25 ans d'expérience

- Conseil en protection des données (*dont règlementaire, patrimoine immatériel et optimisation certification ISO*)
- Audit de conformité – analyse de risques et de maturité
- Mise en conformité (*dont règlement européen RGPD*)
- DPO externalisé - conseil
- Formateur expert (*référencé Comundi*)

Compétences clés :
- Protection et qualité des données (25 ans exp.)
- Propriété intellectuelle
- Conformité
- NTIC
- Gestion de projet

Références :
Co-auteur

Diplômes :
- Master II Droit de propriété intellectuelle, Données et NTIC
- DEA Droit international privé
- DEA droit des affaires.

PSA GROUPE · AXA TECHNOLOGY SERVICES redefining / service · comundi compétences · TRACEONE accelerate innovation · cnrs · irstea · AXA ASSISTANCE réinventons / le service

e DataPrivacy

Suite à votre demande, vous trouverez ci-joint les éléments de notre réponse. Nous vous invitons à nous contacter, si nécessaire, pour avoir des précisions concernant cette proposition.

Votre contact commercial est :
Patrick JEAN-BAPTISTE
Adresse courriel : pjeanbaptiste@edataprivacy.fr
Mobile : 06 75 17 69 86

Votre Directeur de Projet :
Patricia CHEMALI NOEL
Adresse courriel : pchemalinoel@edataprivacy.fr
Mobile : 06 28 71 63 59

Ets administratifs : 09 84 39 43 16

Ce document ne peut être reproduit sans l'autorisation d' e DataPrivacy

MERCI DE VOTRE ATTENTION

Avez-vous des questions?