RGPD

Serez-vous prêts?

Amphithéâtre de la CCISM

Vendredi 7 mars 2019

De 14h à 18h30

esci

CCISM
POLYNÉSIE FRANÇAISE

DGEN
DIRECTION GENERALE DE L'ECONOMIE NUMERIQUE

OPEN
Organisation des Professionnels
de l'Économie Numérique

CLUSIR
TAHITI

TAHITI NUI
FORTRESS

DT
DIGITAL TAHITI

SPILOG
Partner Consulting Services

ACTECIL
RGPD SOLUTIONS

IAORA
systems
SERVICES ET INGÉNIERIE INFORMATIQUES

DPMS
| Data Privacy Management System |

LE DPO Délégué à la Protection des Données

- Dr Eugène SANDFORD
- ESCI Conseil en informatique
- 5 ans d'expérience dans le domaine I&L et RGPD
- DPO externe de plusieurs sociétés
- DPO Certifié par Bureau Veritas Certification
- Partenaire Pacifique du groupe DPMS (AXIL, ANAXIL, PRIVACIL)
- --
- Accompagnement au RGPD,
- Mise en oeuvre vers la conformité au RGPD

LABEL CNIL
FORMATION RGPD
N°2018-278
EXPIRE : 21/06/2021

dpo Délégué à la protection des données

Qualification Formation DPO
BUREAU VERITAS Certification

esci

Le DPO Délégué la Protection des Données

- "Le DPO est au coeur du RGPD" selon la CNIL.
- Il assiste le Responsable de Traitement dans la mise en place de la conformité au RGPD
- Le RGPD est un règlement européen qui renforce la protection des citoyens dans l’utilisation qui est faite de leurs données personnelles

Le DPO - quand est-il obligatoire ?

- Le DPO est obligatoire (art 37) lorsque
  - Vous êtes une **autorité publique** ou un **organisme public** (sauf juridictions),
  - Vous réalisez des traitements qui exigent un **suivi régulier et systématique** à **grande échelle** des personnes concernées; ou
  - Vous réalisez des **traitements à grande échelle** de **données sensibles** (art 9) ou de données relatives à des **condamnations pénales et à des infractions** (art 10).
- En dehors de ces cas, si vous désignez un DPO, vous devrez faire comme si cela vous était obligatoire
- La désignation d'un DPO est fortement conseillé par le EDPB (European Data Protection Board)

Le DPO - Les compétences, ce que dit la CNIL

- une expertise juridique et technique en matière de protection des données personnelles ;
- une bonne connaissance du secteur d'activité, de l'organisation interne, en particulier des opérations de traitements, des systèmes d'information, des besoins en matière de protection et de sécurité des données.
- Ces compétences peuvent être acquises, par exemple, à l'occasion de formations adaptées

Le DPO - Des compétences étendues en

- Juridique en protection des données,
- Informatique et en sécurité informatique,
- Gestion des risques,
- Processus d’entreprise, organisation et amélioration continue,
- Gestion de projet,
- Transfert de compétence

Le DPO - la certification DPO pour s'en assurer

- La certification (art 42) est encouragée par l'UE,
- Examen des compétences et de l'expertise de la mise en œuvre de la conformité au RGPD
- Exemple de Certification Bureau Veritas BV
  - Formation labellisée CNIL pour BV
  - Examen 50% de réussite
  - 120 DPO certifiés sur 15.000 DPO désignés à la CNIL

Le DPO - Conflit d'intérêt

- Le DPO doit être à l'abri des conflits d'intérêt (art 38.3) et c'est au RT d'y veiller.
- Le DPO ne peut être :
  - PDG, DG, Secrétaire Général, DSI, DRH, DAF, Directeur Marketing, Médecin chef, Mandat de représentant du personnel, etc

Le DPO – mutualisation

- Si l'entreprise fait partie d'un groupe (art 37.2, art 37.3), il peut désigner un DPO unique pour toutes les entités du groupe
- Le DPO doit être joignable de chaque lieu d'établissement, afin qu'il puisse exercer ses missions
- Ses coordonnées doivent être communiquées à la CNIL
- Le G29 recommande fortement que le DPO soit établi dans l'UE mais il peut être hors de l'UE

Le DPO - Son role, sa mission

- Le DPO est chargé d'assister le RT dans la mise en œuvre de la conformité au RGPD
- C'est le « Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme

Le DPO - Son role, sa mission

- Le DPO délégué à la protection des données est principalement chargé (1) :
  - **d'informer et de conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
    - Mise en place de formations internes, sensibilisations,
    - Organisation des comités RGPD avec Référents RGPD dans les services
  - **de contrôler le respect du règlement** et du droit national en matière de protection des données ;
    - Vérifier que toutes les mesures ont bien été prises

Le DPO - Son role, sa mission

- Le DPO délégué à la protection des données est principalement chargé (2) :
  - **de conseiller l'organisme** sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
    - Lorsque vous avez des données sensibles mais pas seulement,
  - **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci (voir question ci-après).
    - Lien avec la CNIL pour répondre à ses questions, notamment lors de plaintes de personnes physiques
- Les missions du délégué couvrent l'ensemble des traitements mis en œuvre par l'organisme qui l'a désigné.

Le DPO - interne, externe ?

- Interne ou externe, le RGPD autorise les deux
- Interne
  - Le RT doit lui donner les compétences pour effectuer son boulot
  - Attention au conflit d'intérêt
    - pas de DG, Resp. Informatique, DRH, etc
  - Il ne rend compte qu'au RT et pas à sa hiérarchie
  - Il peut être relevé de ses fonctions mais attention car la suppression de sa désignation alerte la CNIL
  - En général, ce n'est pas un mi temps les 3 premières années

Le DPO - interne, externe ?

- Externe
  - Coût moindre
  - Expert en la matière
  - Pas de conflit d'intérêt, pas un ayatollah
  - Sa relève de fonction est une fin de contrat de prestation de service
  - Il s'organise pour être là le temps qu'il faut

Le DPO – la journée type (1)

- Gérer les Registres pour le Client
  - Registre des Traitements de Données
  - Registre des Traitements en tant que Sous-Traitant
  - Registre des violations de données personnelles
  - Registre des consentements et de leurs retraits
- Lancer et gérer la sensibilisation aux salariés
  - Sensibilisations, formations plus poussées, formations des référents métier, des référents RGPD
- Organiser le comité RGPD, nommer et former les référents internes métier
- Lancer les plans de mesure de conformité avec l'aide des référents métier
- Constituer et mettre à jour la documentation à la conformité (Dossier CNIL)

Le DPO – la journée type (2)

- Être consulté systématiquement pour tout nouveau projet incluant des données personnelles (Privacy by design art 25)
- Maintenir opérationnelle la conformité par des audits internes, des vérifications que les mesures ont bien été prises et restent en place
- Répondre aux questions des personnes physiques (salariés, clients, etc) sur le sujet
- Répondre aux demandes des droits d'accès, de rectification, d'opposition, etc, des personnes physiques
- Répondre aux sollicitations de la CNIL

Merci !

Des questions ?

- Dr Eugène SANDFORD
- +689.89.76.76.57
- Société ESCI
- 5 ans d'expérience dans le domaine
- DPO externe de plusieurs sociétés
- DPO Certifié par Bureau Veritas Certification
- Partenaire Pacifique du groupe DPMS (AXIL, ANAXIL, PRIVACIL)