Le DPO dans l'organisation et sa relation avec le CISO

Alain De Maght

Dpocircle.eu

DPO CIRCLE

Rôle et responsabilités du DPO

- **Le DPO** (Data protection officer) - *défini par le RGPD*
  - *conseiller* de **manière indépendante** le responsable du traitement et
  - *s'assure*r que les principes du RGPD sont bien respectés dans l'organisation.
  - Il doit tenir compte en particulier des *risques* associés aux opérations de traitement compte tenu des données traitées et de la manière dont elles sont traitées.

Les missions du DPO (définies dans les art. 38 et 39 du RGPD) sont :

- *d'informer et conseiller* le responsable du traitement quant aux obligations en matière de protection des données personnelles ; cela implique de mener des actions de sensibilisation et de formation
- de *contrôler* le respect du RGPD - au travers d'audit de mise en conformité
- dispenser des conseils sur demande - notamment en ce qui concerne la PIA
- *gérer les interactions* avec l'autorité de protection des données belge (APD), fait office de point de contact avec elle

Dpocircle.eu

Autres acteurs et responsabilités associés au RGPD

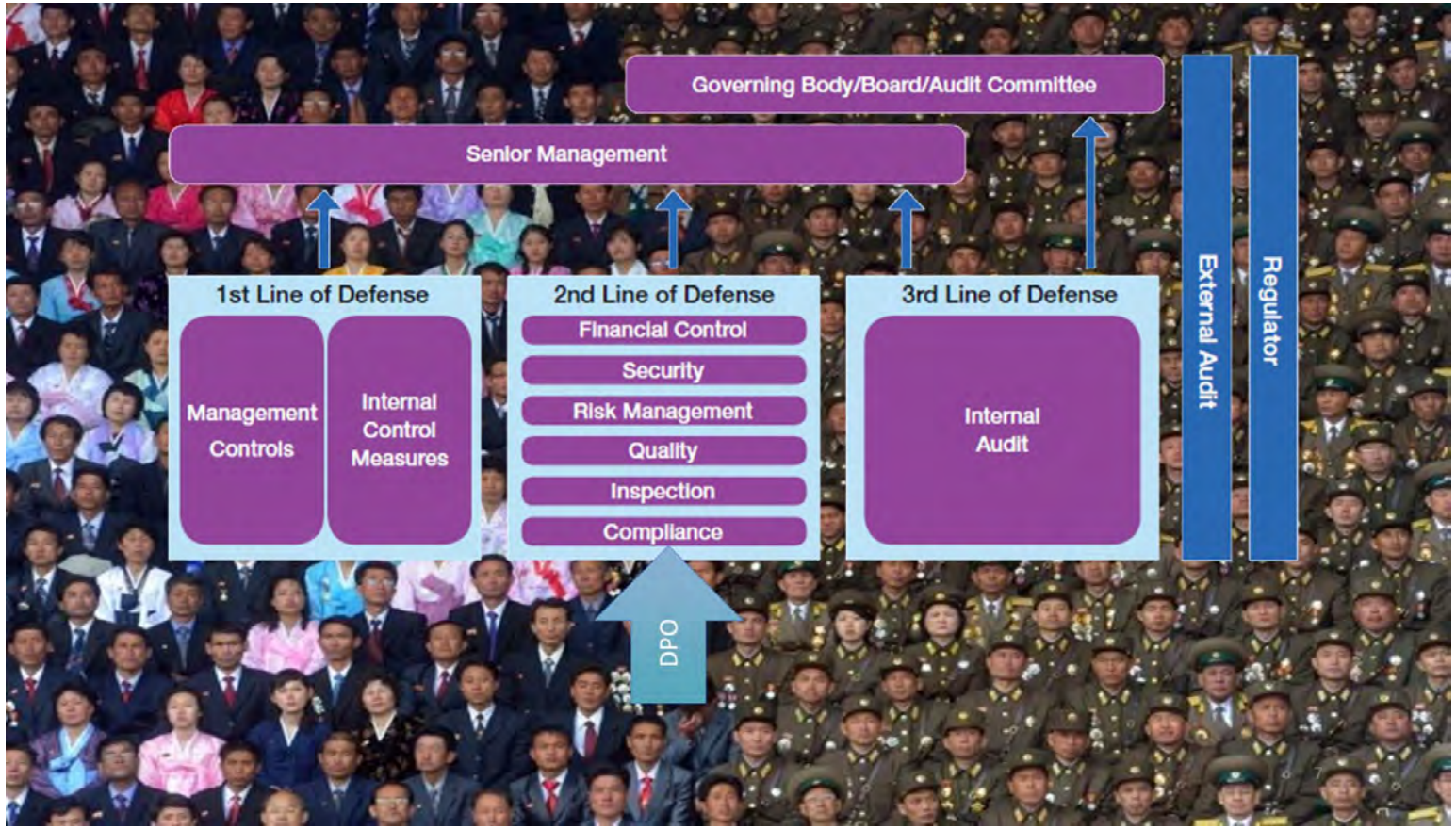
- **Le conseil d'administration** a la responsabilité finale de s'assurer que les obligations relatives au respect de la vie privé soient bien gérées et qu'elles soient conformes à la stratégie et au respect de la législation

- **Chaque responsable de traitement** de données à caractère personnel est responsable pour les traitements définis.

Dpocircle.eu

Position du DPO

Le modèle des 3 lignes de défense



Assurance, Permettre une gestion efficace des risques contre toute menace.

Objectif:

- Evaluer,
- répondre et
- surveiller

les risques et les menaces afin d'atténuer les pertes opérationnelles, les sanctions réglementaires, la fraude et les cyberattaques

Dpocircle.eu

Position du DPO

RGPD : Art 38.3

« Le DPO fait directement rapport au niveau le plus élevé de la direction du responsable de traitement ou du sous-traitant »

Possibilités de reporting:

- Board of directors (indirect report)
- Chief executive officer (CEO)
- General counsel or chief legal officer (CLO)
- Chief information officer (CIO)
- Chief financial officer (CFO)
- Chief risk officer (CRO)
- Chief technology officer (CTO)
- Chief marketing officer (CMO)
- Chief operating officer (COO)

Dpocircle.eu

Board of directors (indirect report)

Avantages

Le risque d'atteinte à la vie privée est élevé au plus haut niveau dans l'entreprise

Désavantages

Les plans de gestion des risques liés à la protection de la vie privée doivent être présentés sous une **forme compréhensible pour les membres du conseil d'administration**, ce qui risque de les rendre trop ambitieux pour être efficaces.

En outre, la **responsabilité pourrait être diluée** entre tous les membres du conseil d'administration.

Dpocircle.eu

Chief executive officer (CEO)

Avantages

Le risque d'atteinte à la vie privée est élevé au plus haut niveau dans l'entreprise. La gestion de la vie privée, lorsqu'elle est communiquée de manière claire et efficace, peut se traduire par **un soutien visible et fort de la part du PDG.**

Ce soutien se traduira par une **adoption plus cohérente des pratiques** de protection de la vie privée dans l'ensemble de l'entreprise.

Désavantages

Étant donné la multitude de responsabilités du PDG, le risque d'atteinte à la vie privée peut être surveillé et géré à un **niveau d'abstraction trop élevé** ou ne pas être pleinement compris dans ses détails pertinents.

Dpocircle.eu

General counsel or chief legal officer (CLO)

Avantages

Il faut bien comprendre les exigences juridiques en matière de vie privée. Cette voie de signalement contribue à garantir que toutes les **obligations légales en matière de respect de la vie privée sont correctement prises en compte.**

Désavantages

Le risque d'atteinte à la vie privée qui n'est pas couvert par des exigences légales **peut ne pas être pris en compte**. La mise en œuvre de protections de la vie privée dans l'ensemble de l'entreprise peut être inefficace ou irréalisable si la vie privée n'est gérée que selon la "lettre de la loi".

Dpocircle.eu

Chief information officer (CIO)

Avantages

Les questions et les solutions relatives à la gestion des informations personnelles peuvent être alignées sur toutes les initiatives informatiques. Cela permet de garantir une mise en œuvre efficace du principe **"privacy by design"** et l'utilisation de technologies appropriées de protection de la vie privée.

Désavantages

Il se peut que le risque d'atteinte à la vie privée **ne soit pas traité en raison d'autres initiatives et délais informatiques** qui priment sur les besoins de gestion de la vie privée.

Il existe un conflit d'intérêts potentiel. Le travail effectué par les professionnels de la protection de la vie privée désignés pourrait être axé sur les TI et non sur la protection de la vie privée. En outre, les exigences légales peuvent ne pas être prises en compte de manière appropriée.

Dpocircle.eu

Chief financial officer (CFO)

Avantages

Les questions et les risques liés à la protection de la vie privée sont abordés **sous l'angle de l'impact financier** sur les entreprises.

Désavantages

Le risque de violation de la vie privée peut ne pas être pris en compte en raison **d'initiatives financières** et de délais qui priment sur la protection de la vie privée. Il existe un conflit d'intérêts potentiel.

Dpocircle.eu

Chief risk officer (CRO)

Avantages

Le risque d'atteinte à la vie privée est élevé à une position qui permet également **d'examiner le risque d'un point de vue stratégique, financier, opérationnel, de réputation et de conformité.**

Désavantages

Ce rôle n'existe souvent pas dans les entreprises. Il se retrouve le plus souvent dans les entreprises de services financiers.

Dans les entreprises où il n'y a pas de CRG, les décisions relatives au risque d'entreprise peuvent être prises par le PDG ou le conseil d'administration.

Dpocircle.eu

Chief technology officer (CTO)

Avantages

La gestion de la vie privée fait l'objet d'un partenariat et est **incluse dans les futures feuilles de route technologiques**.

Désavantages

La gestion de la vie privée peut ne pas être prise en compte en raison des orientations technologiques qui priment sur la sécurité de l'information

Dpocircle.eu

Chief marketing officer (CMO)

Avantages

L'utilisation d'informations personnelles dans le cadre d'activités de marketing vise à atténuer le plus efficacement possible les risques et les exigences associés à la protection de la vie privée.

Désavantages

Le risque pour la vie privée qui est **en dehors des activités de marketing peut être négligé**. En outre, étant donné que les activités de marketing impliquent une grande quantité d'informations personnelles, il pourrait **y avoir un conflit d'intérêts, et les initiatives de marketing** pourraient avoir la priorité sur les actions.

Dpocircle.eu

Chief operating officer (COO)

Avantages

Les problèmes et les solutions en matière de protection de la vie privée sont **abordés sous l'angle de l'impact sur les activités de l'entreprise.**

Désavantages

La protection de la vie privée peut ne pas être prise en compte en raison d'initiatives et de délais **opérationnels qui priment sur les activités de protection de la vie** privée. En outre, les exigences légales en matière de protection de la vie privée pourraient ne pas être respectées si le directeur de l'exploitation n'a pas une **connaissance approfondie de toutes les obligations légales.**

Dpocircle.eu

Role du CISO

Le CISO

- A la responsabilité **d'évaluer les risques en matière de sécurité de l'information** aux côtés de l'exécutif, et la **formulation d'un plan de gestion des risques** aux côtés de l'exécutif et d'autres départements de l'entreprise.

- A un rôle dans la réponse aux incidents, briefing de l'entreprise sur les changements dans la sécurité de l'information et le paysage des menaces.

- joue un rôle de premier plan dans la définition de la politique, la conduite de campagnes de formation et de sensibilisation et la garantie du maintien des normes / conformité permanente aux normes Infosec

- Couvre la sécurité des réseaux, des télécommunications, des applications, la sécurité physique,

- la stratégie de sauvegarde des données,

<> **Responsable de la sécurité informatique** : il gère la sécurité de l'infrastructure technique et des applications.

Dpocircle.eu

Sécurité VS Privacy .. Clarification

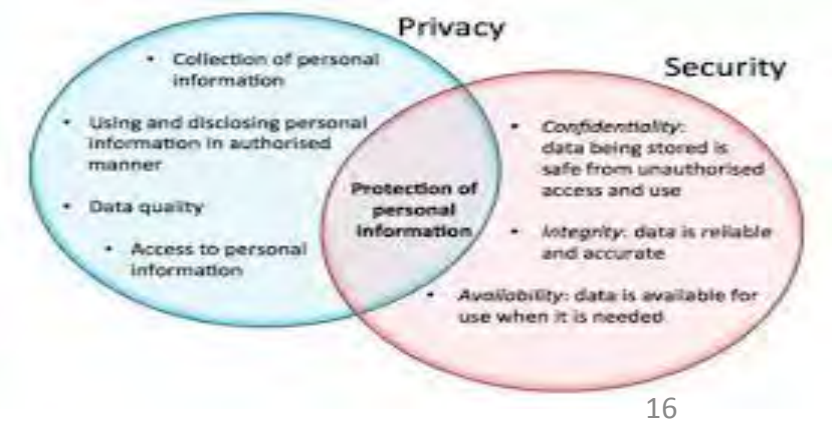
La sécurité ➔ CISO

➔ assure la protection de tous les types d'information, sous quelque forme que ce soit, de sorte que la *confidentialité, l'intégrité et la disponibilité* des informations soient maintenues.

(Privacy) La protection de la vie privée ➔ DPO

➔ garantit que les informations à caractère personnel sont recueillies, traitées (utilisées), protégées et détruites *légalement et équitablement*.

PS : Privacy a besoin de sécurité



Dpocircle.eu

Chief information security officer (CISO)

Avantages

La sécurité de l'information nécessaire à une gestion efficace de la vie privée est **mise en œuvre de la manière la plus efficace** pour protéger les informations personnelles et les systèmes, applications et réseaux associés.

Il pourrait également y avoir une utilisation plus efficace et plus efficiente des mesures de sécurité pour favoriser le respect de la vie privée.

Désavantages

Les exigences légales en matière de protection de la vie privée pourraient ne pas être respectées si le domaine de la sécurité de l'information ne dispose pas d'une connaissance approfondie de toutes les obligations légales. Le travail pourrait également **être davantage axé sur les activités de sécurité de l'information, en omettant éventuellement des considérations importantes relatives à la vie privée** telles que l'utilisation, le partage, la limitation de la collecte et autres.

Dpocircle.eu

Verdict

The DPOCircle (https://dpocircle.eu)

A Community

- DPO and GDPR professionals involved in implementing GDPR, Privacy and Data Protection compliance
- open to any alumni or participant in a Privacy, Data Protection or GDRP education delivered by any party, training organisation or university. Members are invited to promote their knowledge and to engage in continued education.

A Platform

Knowledge sharing platform is made available to members to assist them in communicating and sharing resources and tools

The Members

- organize round-table discussions, conferences, seminars and other educational events on specific topics of interest.
- are invited to share relevant information, documents and news that can benefit their fellow members.
- promote research and are interested to establish contacts with research centers, universities and solution providers with the aim of bringing value to privacy implementation

Dpocircle.eu

Merci !

Dpocircle.eu