
THE
PRIVACY
OFFICE
feel free to create
We are your privacy architect
www.tpo.solutions

DPO: une fonction d'avenir

05 octobre 2023

Sabine Mersch
Fondatrice et CEO

Agenda

- Introduction – Les défis du DPO
- Comment en faire une fonction d'avenir ?
- Expliquer l'intérêt du RGPD pour les organisations
- Ancrer la fonction dans la réalité opérationnelle
- Montrer l'avenir

Agenda

- Introduction – Les défis du DPO
- Comment en faire une fonction d'avenir ?
- Expliquer l'intérêt du RGPD pour les organisations
- Ancrer la fonction dans la réalité opérationnelle
- Montrer l'avenir

Introduction – Les défis du DPO

Chaque trimestre, nous organisons des Breakfasts DPO afin de permettre aux DPOs de la région de se rencontrer et d'échanger sur les sujets qui les intéressent.

Introduction – Les défis du DPO

Dans ce cadre et aussi dans ma propre pratique, les défis exprimés régulièrement par les DPO sont les suivants :

- Manque de moyens
- Manque d'assistance des collègues
- Manque de soutien du management

Introduction – Les défis du DPO

Le RGPD est perçu comme un problème et le DPO est associé à ce problème.

Agenda

- Introduction – Les défis du DPO
- **Comment en faire une fonction d'avenir ?**
- Expliquer l'intérêt du RGPD pour les organisations
- Ancrer la fonction dans la réalité opérationnelle
- Montrer l'avenir

Comment en faire une fonction d'avenir ?

1. Expliquer l'intérêt du RGPD pour les organisations
2. Ancrer la fonction dans la réalité opérationnelle
3. Montrer l'avenir

Agenda

- Introduction – Les défis du DPO
- Comment en faire une fonction d'avenir ?
- **Expliquer l'intérêt du RGPD pour les organisations**
- Ancrer la fonction dans la réalité opérationnelle
- Montrer l'avenir

Sans RGPD - Risque de sécurisation insuffisante des données

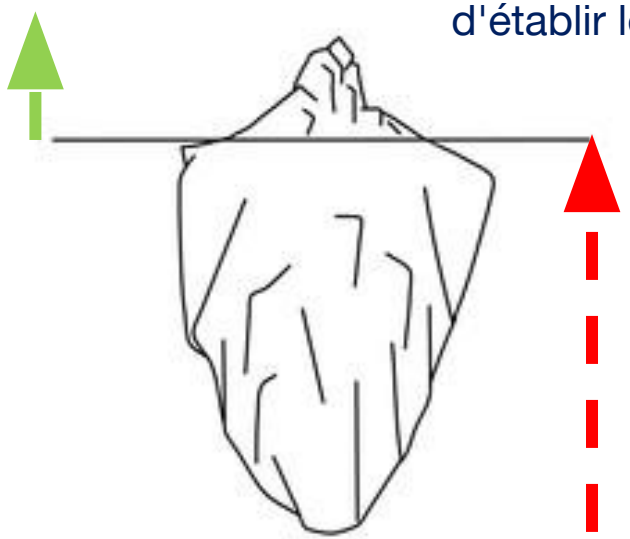
Ce que les organisations pensent

- Leurs données sont sécurisées **par leur service IT**

La réalité

- Les services informatiques ne protègent **que** les composants informatiques **sur site (on premise).**
- Toutes les données **hors site (cloud)** sont entre les mains de fournisseurs dont les obligations de sécurité doivent être définies **par contrat.**
- Les services informatiques **ne sont pas chargés d'établir les contrats.**

Sécurisation de données gérée par l'organisation



Sécurisation de données NON gérée par l'organisation

L’application effective du RGPD améliore la sécurisation des données

THE PRIVACY OFFICE

En obligeant les organisations à apporter des réponses concrètes aux questions suivantes :

- Comment est sécurisée notre infrastructure IT ?
- Quel est le périmètre de responsabilité de chaque prestataire IT ?
- Que fait le prestataire IT exactement ?
- Nos données sont-elles bien sécurisées chez nos hébergeurs?
- Combien de temps peut-on garder les données ?

Sans RGPD - Risque d'utilisation abusive des données

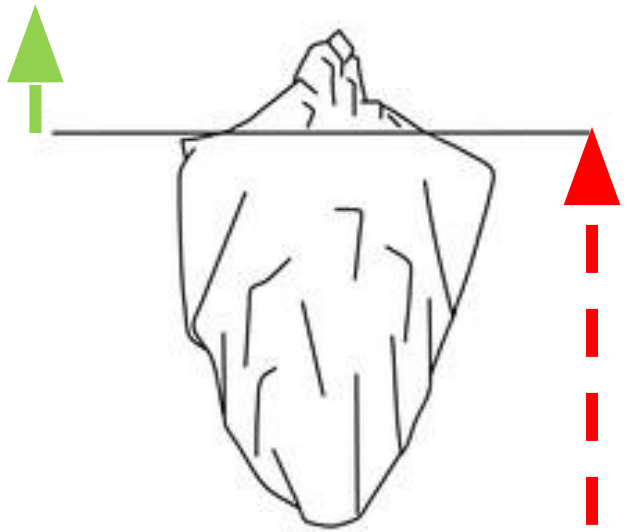
Ce que les organisations pensent

- Les prestataires de services veillent à ce que les organisations puissent légitimement utiliser les données traitées.
- Elles ne sont pas elles-mêmes responsables des données hébergées dans le cloud.

La réalité

- Beaucoup de services sont développés sans se soucier de l'utilisation légitime des données dans le chef du client
- Beaucoup de prestataires de services faisant appel à des sous-traitants ultérieurs ne se sentent pas non plus responsables des traitements effectués par ces derniers.

Utilisation de données gérée par l'organisation



Utilisation de données NON gérée par l'organisation

L’application effective du RGPD favorise l’utilisation légitime des données

En obligeant les organisations à apporter des réponses concrètes aux questions suivantes :

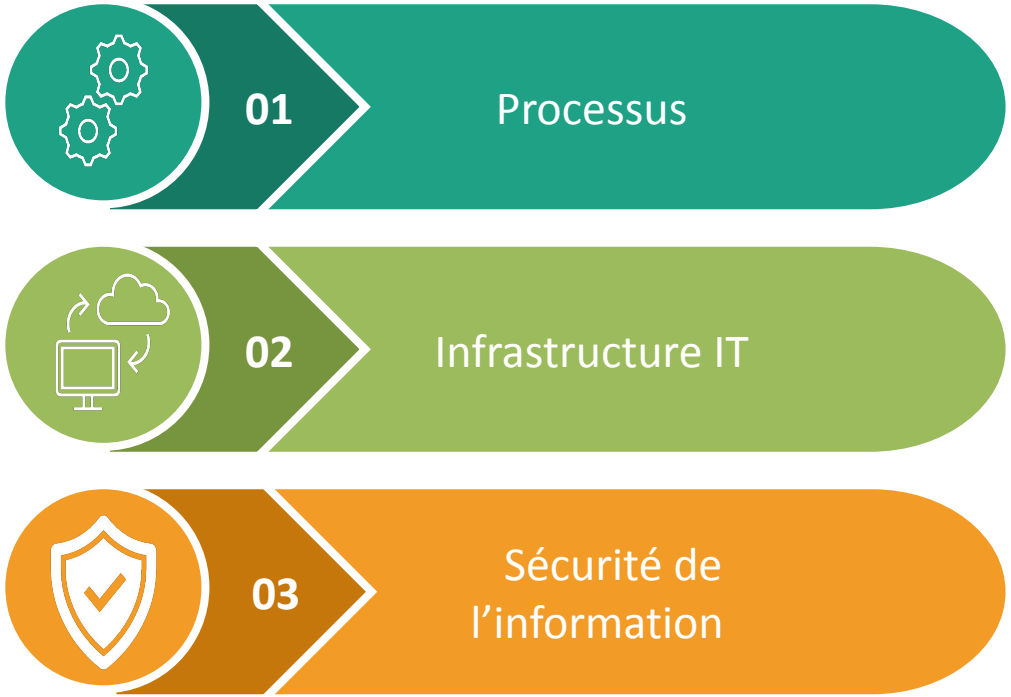
- Qui doit veiller à ce que l’utilisation des données soit légitime?
- Que pouvons-nous faire avec les données?
- Que peut faire le prestataire de services avec ces données ?

Agenda

- Introduction – défis du DPO
- Comment en faire une fonction d'avenir?
- Expliquer l'intérêt du RGPD pour les organisations
- **Ancrer la fonction dans la réalité opérationnelle**
- Montrer l'avenir

Ancrer la fonction dans la réalité opérationnelle

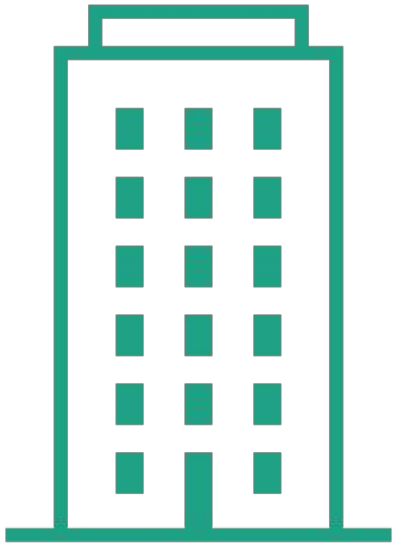
Pour générer une valeur ajoutée, il y a lieu d'ancrer la fonction de DPO dans la réalité de terrain.



1. Au niveau des processus

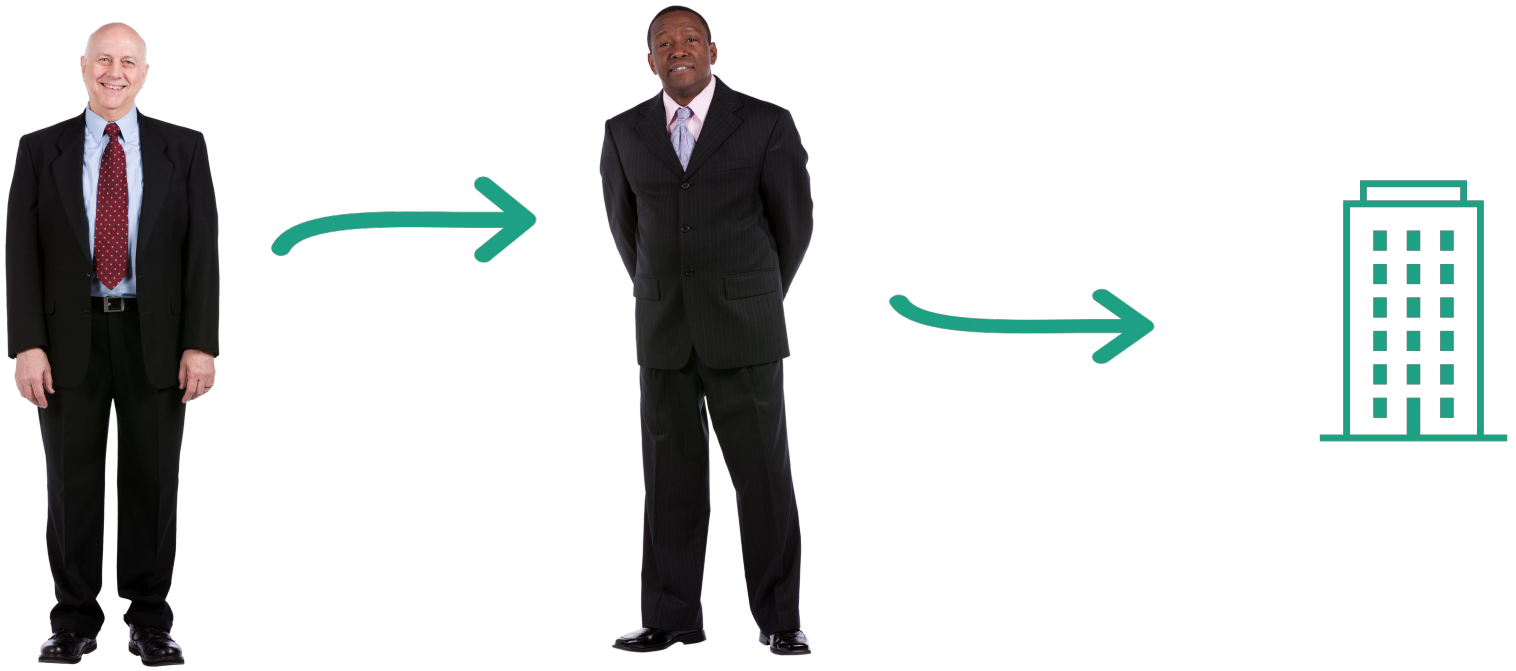
01 Processus

Faire le lien entre le registre des traitements (art. 30) et les processus opérationnels.



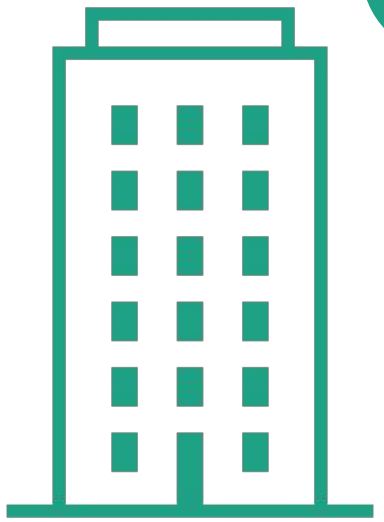
Comment?

- En proposant que le responsable du processus porte également la responsabilité opérationnelle de la conformité RGPD des traitements de données liés à ce processus



Avantages en termes d'utilisation des données

Avantages



- Bénéficier du droit d'utilisation des données pour les besoins réels grâce à une base légale appropriée (art. 6 et 9)
- Bénéficier de l'opportunité de réutilisation des données à des fins statistiques (art. 5 (1) b) RGPD)
- Garder la maitrise des données grâce à une bonne qualification juridique de l'organisation
- Maintenir le droit d'utilisation des données sur la durée grâce à l'identification exhaustive des finalités de traitement

2. Au niveau de l'infrastructure IT

02 Infrastructure IT

- Faire le lien entre le registre des traitements (art. 30 RGPD) et les produits informatiques

Comment?

- En faisant nommer un responsable technique responsable de rapporter l'ensemble des produits informatiques utilisés

Avantages en termes de gestion des fournisseurs et autres destinataires

- Bénéficier d'une vue claire sur le périmètre de la responsabilité de l'organisation grâce à l'identification de tous les destinataires de données qualifiant de sous-traitants
- Utiliser les contrats de sous-traitance pour cadrer l'utilisation des données par ces sous-traitants
- Utiliser les contrats de sous-traitance et les contrats entre responsables conjoints comme moyen obligatoire d'obtenir des garanties de sécurisation concrète de la part de ce type de partenaires externes

3. Au niveau de la sécurisation de l'information

03 Sécurité de l'information

- Faire le lien entre le registre des traitements (art. 30 RGPD) et les activités de sécurisation de l'infrastructure sous-jacente

Comment?

- Utiliser le même référentiel sécurité pour la protection des données personnelles que pour les autres informations
- Faire le lien entre l'infrastructure à sécuriser et les risques pour les personnes concernées

Avantages en termes de sécurisation de l'infrastructure

Avantages

- Bénéficier d'un curseur en matière de sécurisation en identifiant le niveau de sécurisation obligatoire de manière rationnelle selon les critères de l'article 32 RGPD (risques, règles de l'art, coûts)
- Utiliser l'obligation de documenter les mesures de sécurité en place pour évaluer le niveau de sécurisation de l'infrastructure

Agenda

- Introduction – défis du DPO
- Comment en faire une fonction d'avenir?
- Expliquer l'intérêt du RGPD pour les organisations
- Ancrer la fonction dans la réalité opérationnelle
- **Montrer l'avenir**

Montrer l’avenir

Le DPO est bien placé pour préparer le terrain aux législations à venir.

- **NIS2**
  - Art. 21 – Mesures de gestion des risques en matière de cybersécurité
  - Art. 23 – Obligations d’information
- **AI Act**
  - Art. 5 – Pratiques interdites en matière d’intelligence artificielle
  - Art. 6 – Règles relatives à la classification de systèmes d’IA comme systèmes à haut risque
  - Art. 10 – Données et gouvernance des données
  - Art. 13 – Transparence et fourniture d’informations aux utilisateurs
  - Art. 52 – Obligations de transparence pour certains systèmes d’IA
- **AI liability directive**
- **Product liability directive**

Questions ?

Merci !

Contactez-nous

The Privacy Office

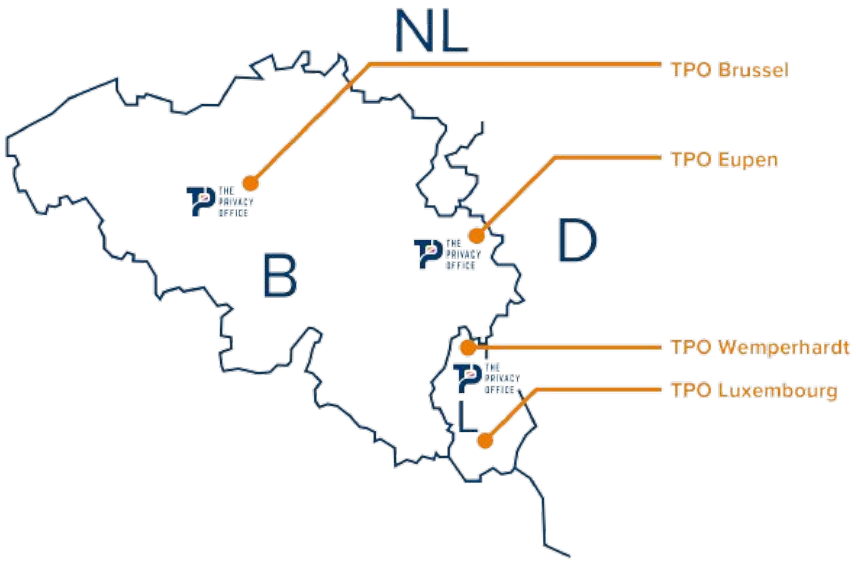
Consultance

www.tpo.solutions

Basée en Belgique

Contact : info@tpo.solutions

DPO externe



Software

www.tpomap.com

Basée au Luxembourg

Contact : marketing@tpomap.com