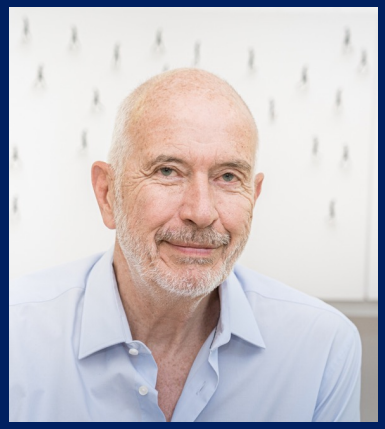
Role et complexité de la fonction de DPO ?



Prof. Dr. Jacques Folon

Jacques@gdprfolder.eu

www.linkedin.com/in/folon

www.gdprfolder.com

+32 475 98 21 15

www.folon.com

7e édition du baromètre trimestriel de l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP)

1. Avez-vous confiance dans la protection des données privées au sein de vos organisations ?

18 % — Non, le contexte règlementaire changeant (privacy shield, cookies, etc.) crée de l'instabilité dans notre stratégie

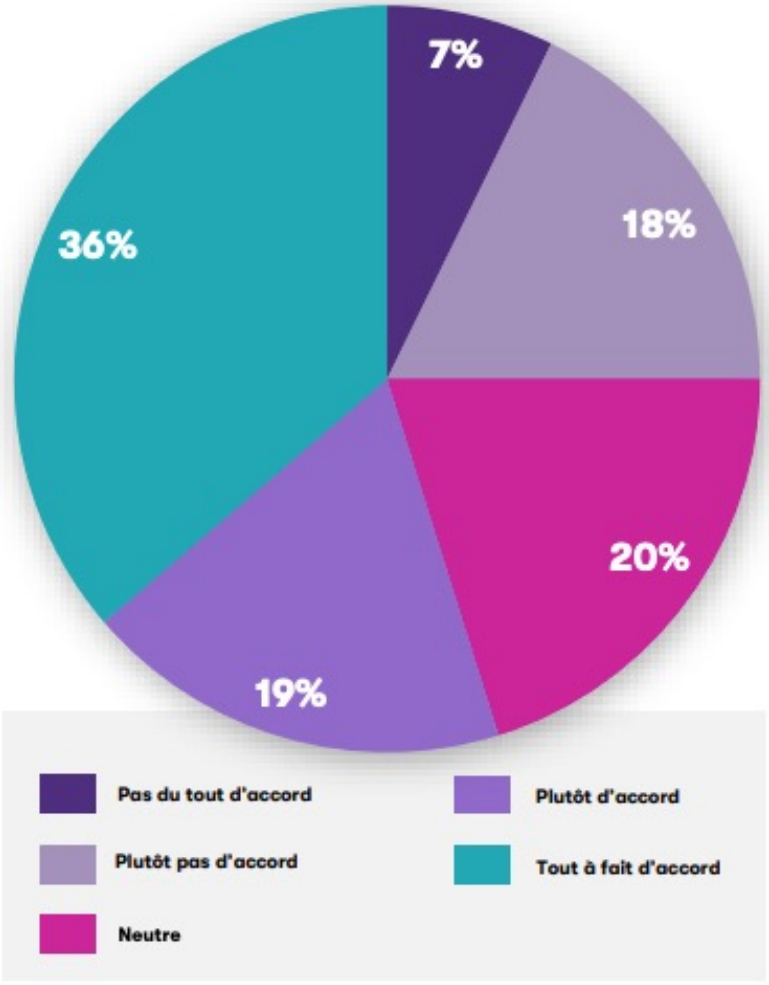
41 % — Non, il y a beaucoup de chemin à faire

36 % — Oui, nous avons une stratégie agile et mes préconisations sont reconnues

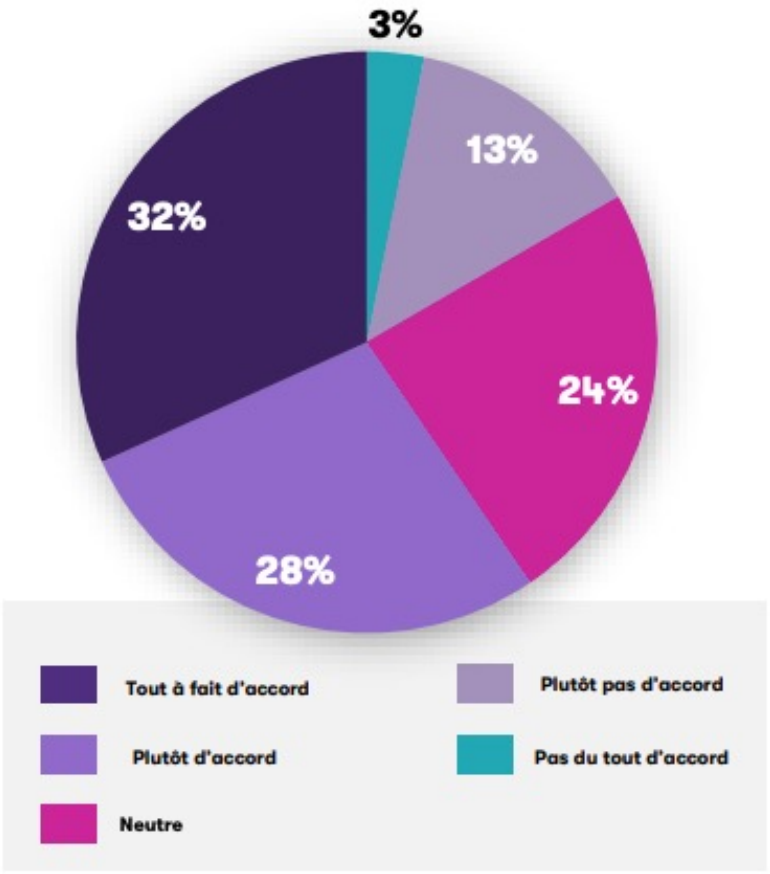
5 % — NSP

41 % des DPO doutent que la protection des données de leurs entreprises respectives soit dans les clous et que 18 % disent s'interroger sur les conséquences qu'engendrent les évolutions règlementaires à venir,

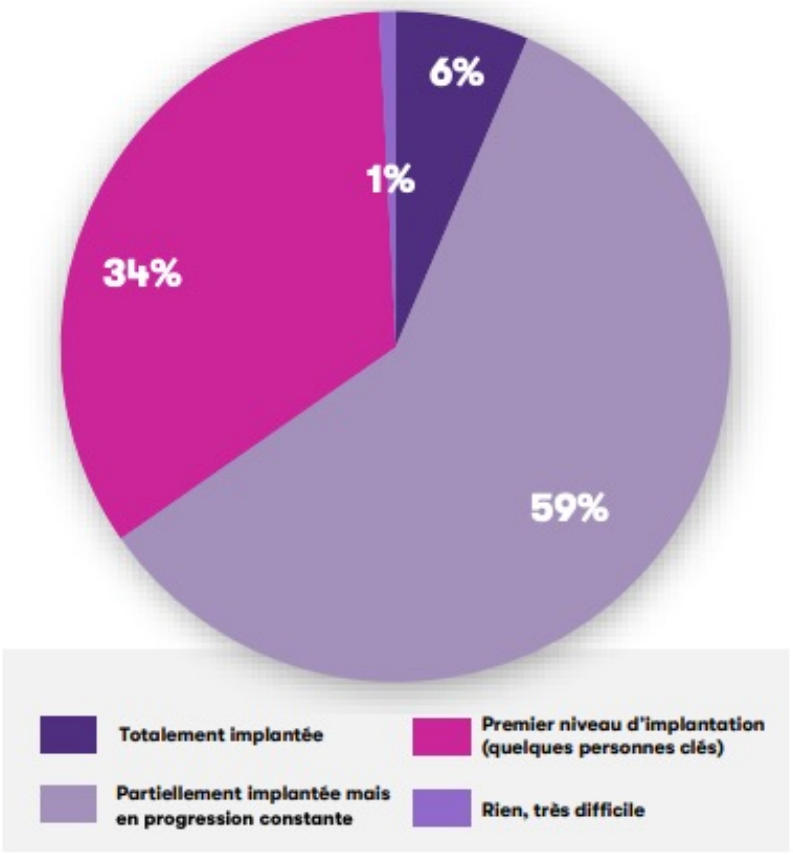
Les moyens alloués au DPO sont insuffisants pour qu'il puisse exercer sa mission



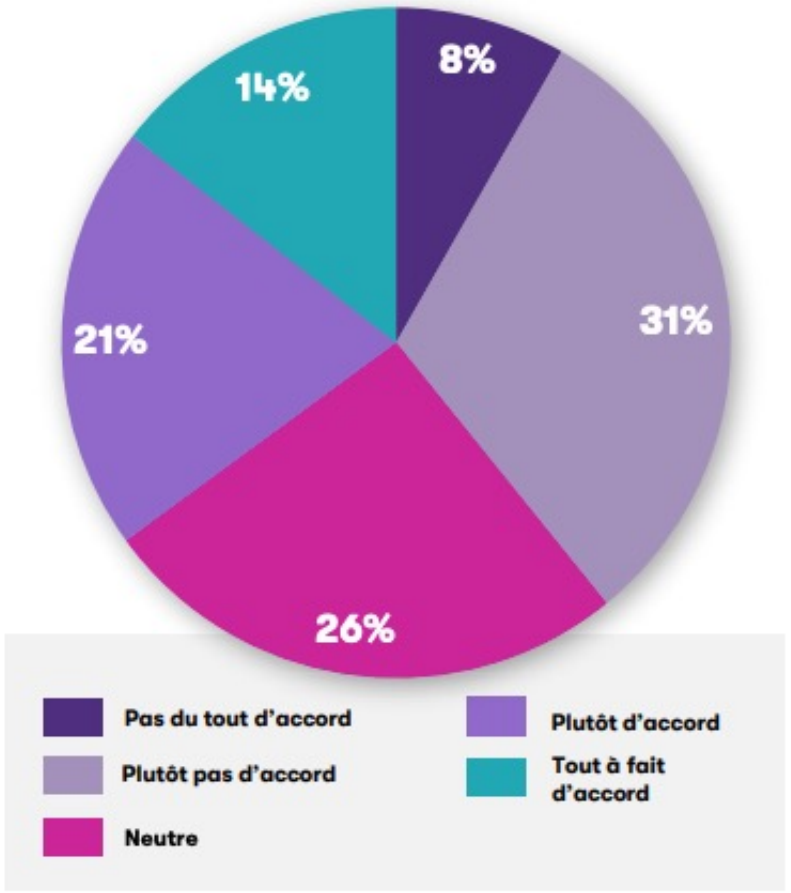
Le RGPD est culturellement vu en interne comme une contrainte



Comment évaluez-vous le niveau d'acculturation à la protection des données ?



Les collaborateurs pensent que la sécurité, bien que nécessaire, est un frein à leur activité

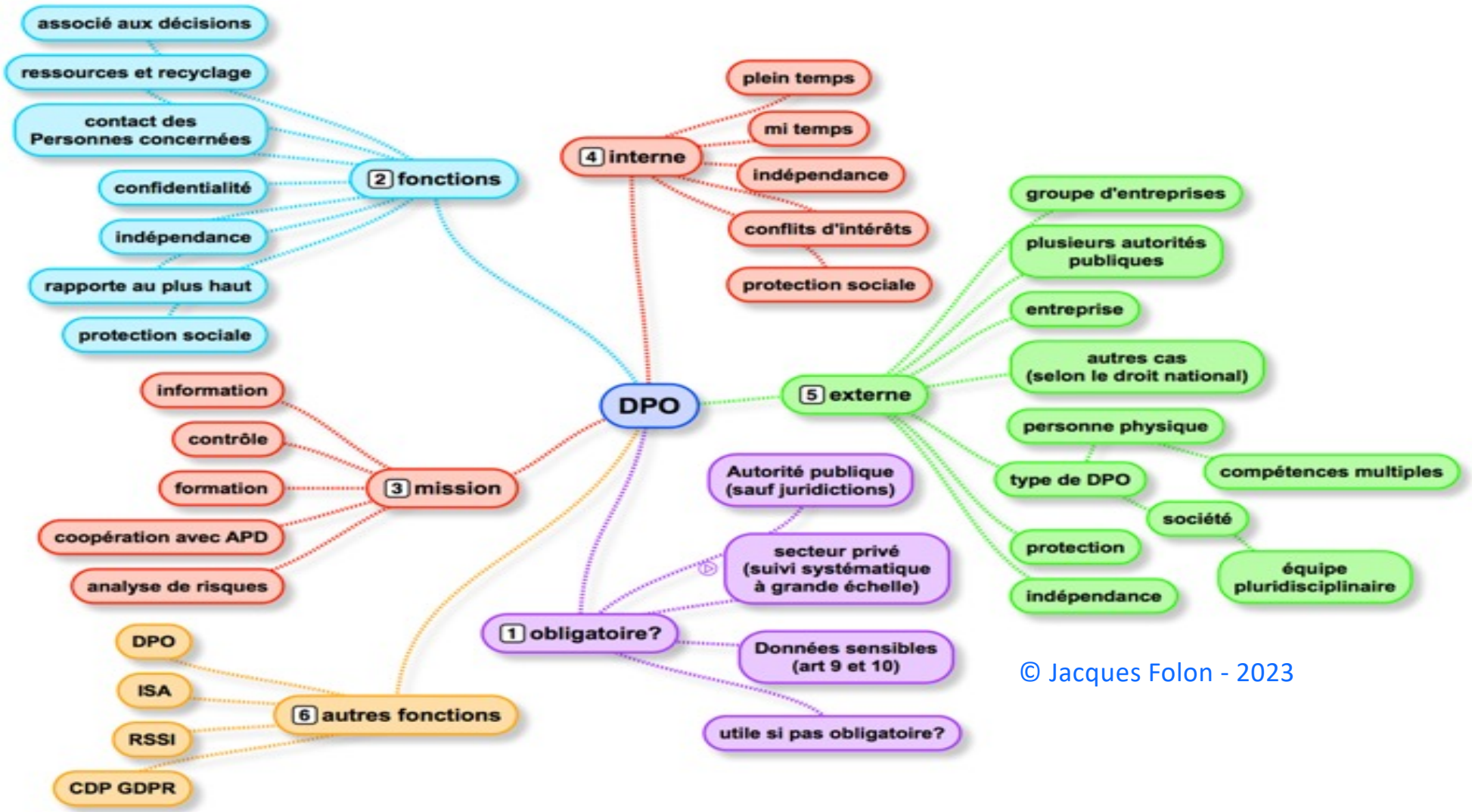


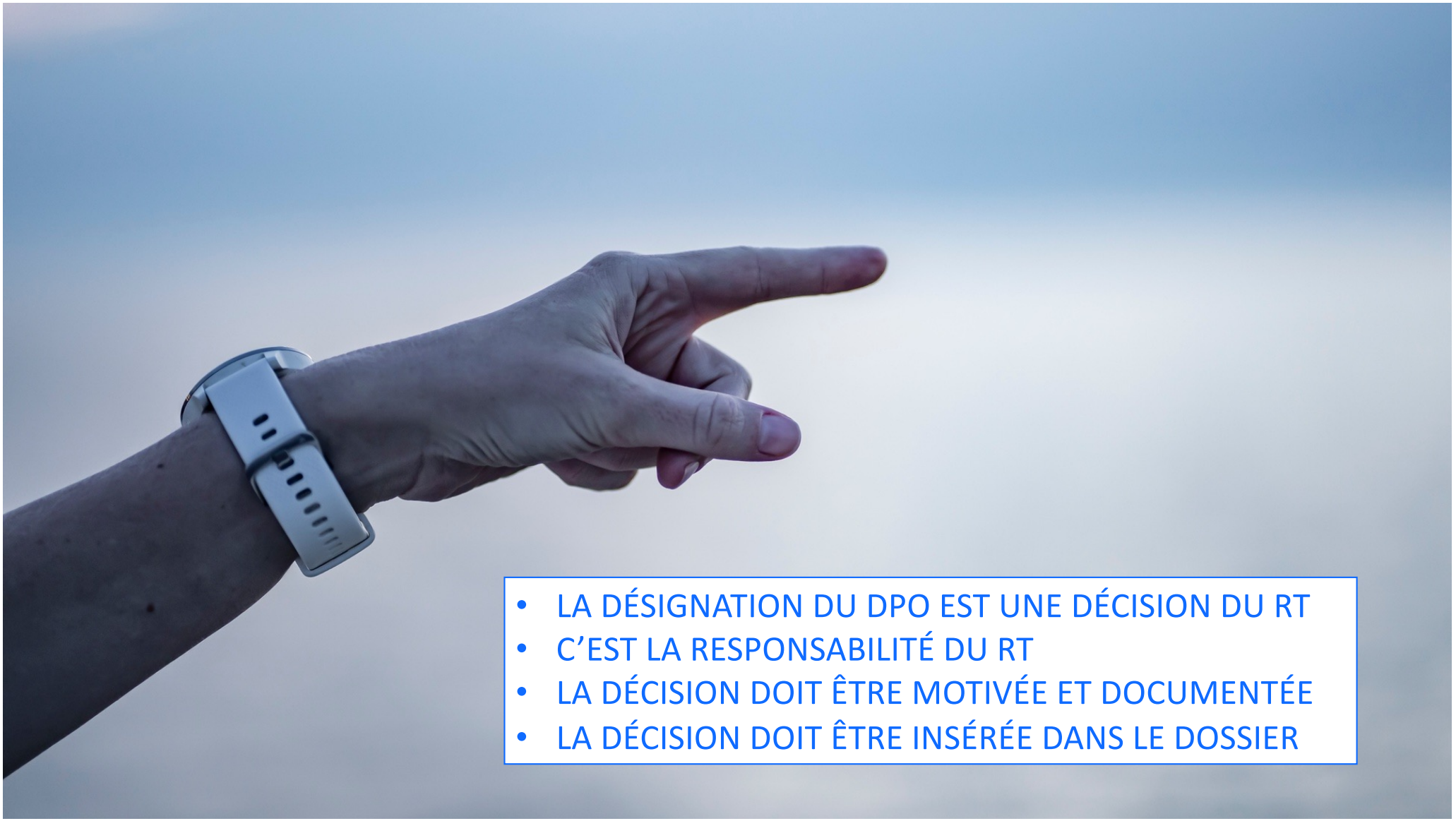
Nos clés pour une gouvernance adaptée

Une gouvernance efficace en matière de RGPD doit reposer sur :

- Une direction générale accessible et pleinement impliquée dans le projet de déploiement de la conformité au RGPD
- Un positionnement stratégique du *DPO* lui assurant une bonne visibilité au sein de l'organisation, ainsi qu'un rattachement hiérarchique pertinent afin qu'il exerce ses missions en collaboration avec les différents départements internes
- Une sensibilisation de l'ensemble des collaborateurs au RGPD, de la direction, jusqu'au maillage le plus fin de l'organisation
- La mise en œuvre d'audits réguliers afin de déterminer le niveau de maturité en matière de RGPD et les axes de progression envisageables
- L'allocation au *DPO* de moyens humains et matériels nécessaires à la bonne conduite de sa mission

Grant Thornton




• LA DÉSIGNATION DU DPO EST UNE DÉCISION DU RT
• C’EST LA RESPONSABILITÉ DU RT
• LA DÉCISION DOIT ÊTRE MOTIVÉE ET DOCUMENTÉE
• LA DÉCISION DOIT ÊTRE INSÉRÉE DANS LE DOSSIER

QUI PEUT ÊTRE DPO ?

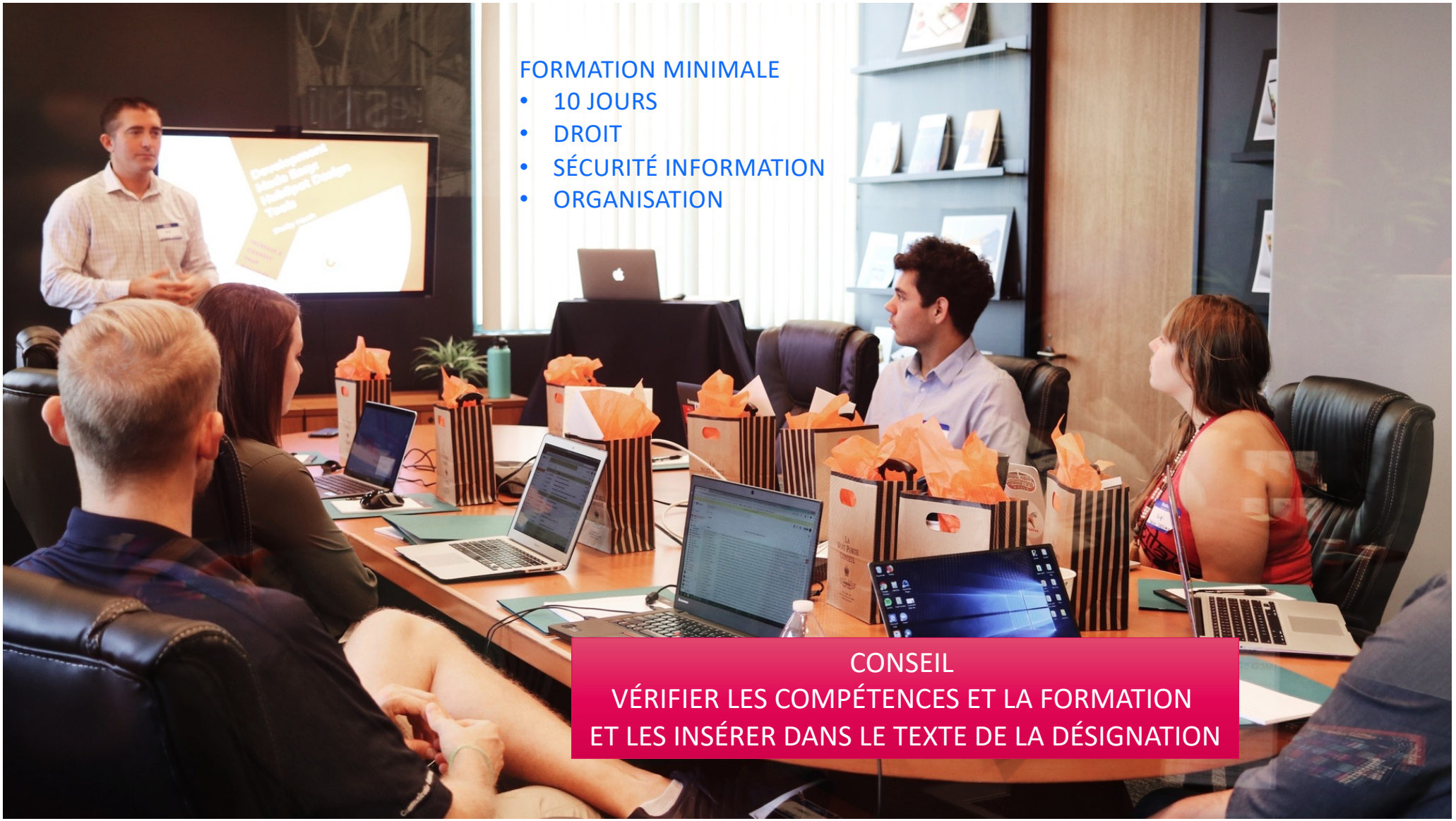
PAS DE DIPLÔME SPÉCIFIQUE

- 1/3 JURISTES
- 1/3 ICT
- 1/3 AUTRES
- LE RGPD CE N'EST PAS QUE DU DROIT !

Un DPO doit être compétent !

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 exercer ses missions

Conseil: insérer les compétences dans la désignation par le RT



FORMATION MINIMALE

- 10 JOURS
- DROIT
- SÉCURITÉ INFORMATION
- ORGANISATION

CONSEIL
VÉRIFIER LES COMPÉTENCES ET LA FORMATION
ET LES INSÉRER DANS LE TEXTE DE LA DÉSIGNATION

DPO INTERNE OU EXTERNE ?

DPO INTERNE

- CONNAIT BIEN L'ENTREPRISE
- EXPERIENCE MOINS VASTE
- MOINDRE INDEPENDANCE
- CONFITS D'INTERÊTS POSSIBLES
- DOIT ÊTRE VOLONTAIRE

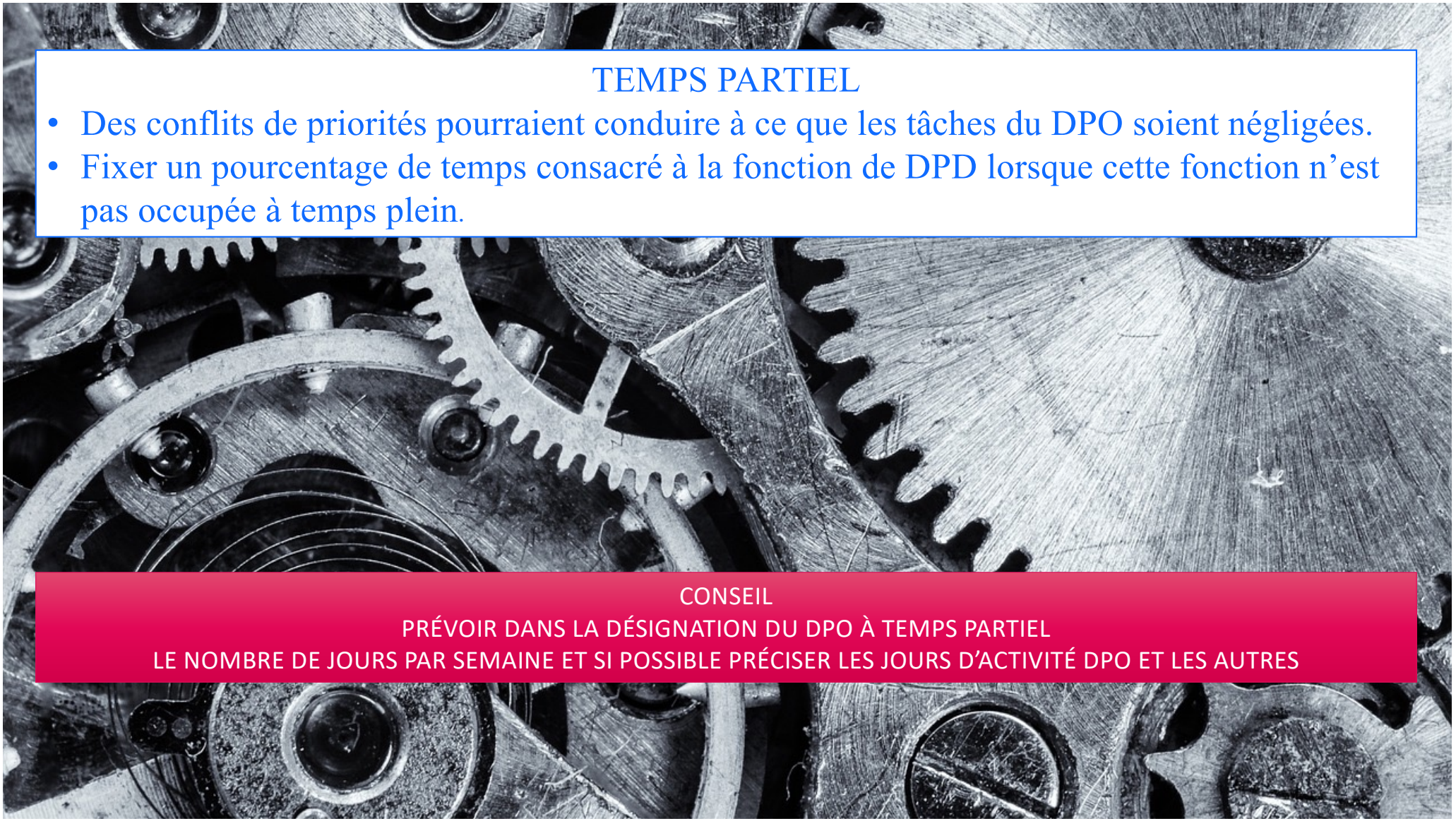
DPO EXTERNE

- CONNAIT MOINS L'ENTREPRISE
- EXPERIENCE PLUS VASTE
- MEILLEURE INDEPENDANCE

QUELLE EST LA DURÉE D'UN MANDAT DE DPO ?
DURÉE FIXE?
DURÉE INDÉTERMINÉE ?

CONSEIL
UNE DURÉE FIXE RENOUVELABLE DE TROIS ANS
PAR EXEMPLE RENFORCE L'INDEPENDANCE


LR NOMBRE DE MANDATS DE DPO N'EST MALHEUREUSEMENT PAS LIMITE PAR LA LOI NI LE RGPD ET DONC PARFOIS PLUS DE 100 MANDATS POUR UN DPO !!
La disponibilité d'un DPO est essentielle pour que les personnes concernées puissent prendre contact avec lui.
CONSEIL
C'EST LA RESPONSABILITÉ DU RT DE VÉRIFIER ET DE LE PRÉCISER DANS LA NOMINATION



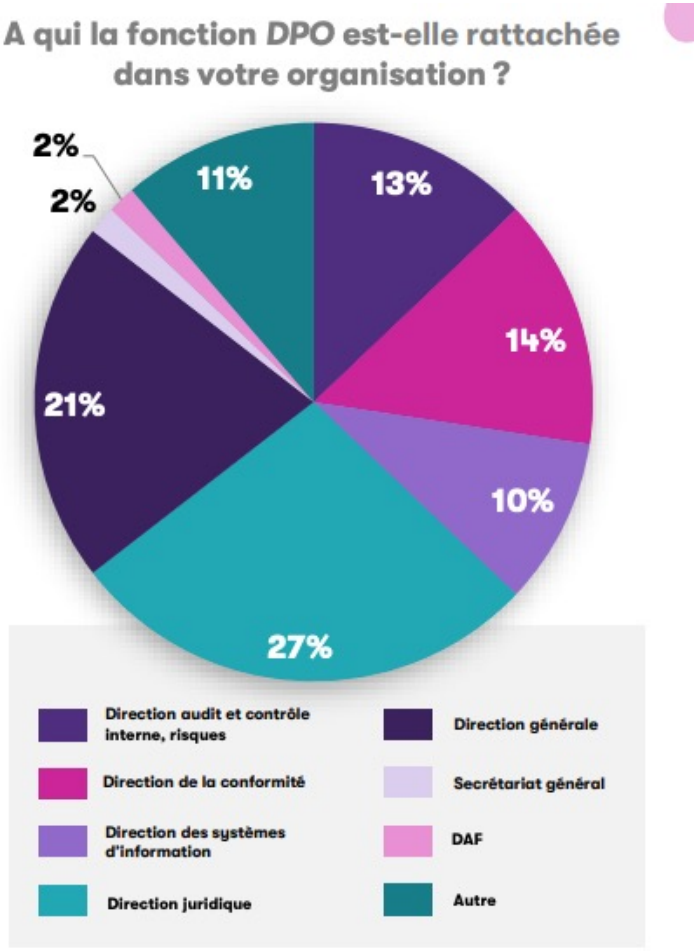
TEMPS PARTIEL

- Des conflits de priorités pourraient conduire à ce que les tâches du DPO soient négligées.
- Fixer un pourcentage de temps consacré à la fonction de DPD lorsque cette fonction n'est pas occupée à temps plein.

CONSEIL

PRÉVOIR DANS LA DÉSIGNATION DU DPO À TEMPS PARTIEL

LE NOMBRE DE JOURS PAR SEMAINE ET SI POSSIBLE PRÉCISER LES JOURS D'ACTIVITÉ DPO ET LES AUTRES



LE DPO « RAPPORTE » AU PLUS HAUT NIVEAU DE LA HIÉRARCHIE

CONSEIL

RATTACHER HIERARCHIQUEMENT LE DPO AU PLUS HAUT NIVEAU

L’article 38 du RGPD dispose que le responsable du traitement et le sous-traitant doivent veiller à ce que le DPD «*soit associé, d’une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel*».

EN THÉORIE …

LE RT devrait veiller, par exemple, à ce que:

- le DPD soit invité à participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire;
- sa présence soit recommandée lorsque des décisions ayant des implications en matière de protection des données sont prises. Toutes les informations pertinentes doivent être transmises au DPD en temps utile afin de lui permettre de fournir un avis adéquat;
- l'avis du DPD soit toujours dûment pris en considération. En cas de désaccord, le G29 recommande, à titre de bonne pratique, de consigner les raisons pour lesquelles l'avis du DPD n'a pas été suivi;
- le DPD soit immédiatement consulté lorsqu'une violation de données ou un autre incident se produit.

CONSEIL: RAPPELER RÉGULIÈREMENT L'ARTICLE 38 LORSQUE L'INFO ARRIVE TROP TARD

L'article 38, paragraphe 2, du RGPD exige que l'organisme aide son DPD *en fournissant les ressources nécessaires pour exercer [ses] missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées*.

- soutien actif de la fonction du DPO par l'encadrement supérieur (par exemple, au niveau du conseil d'administration);
- temps suffisant pour que les DPD puissent accomplir leurs tâches. (temps partiel ET DPO externe)
- soutien adéquat du point de vue des ressources financières, des infrastructures (locaux, installations, équipements) et du personnel, le cas échéant;
- communication officielle de la désignation du DPD à l'ensemble du personnel afin de veiller à ce que l'existence et la fonction de celui-ci soient connues au sein de l'organisme;
- accès nécessaire à d'autres services, tels que les ressources humaines, le service juridique, l'informatique, la sécurité, etc., de manière à ce que les DPD puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services;
- formation continue.

« Une grande échelle » ?

- le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée;
- le volume de données et/ou le spectre des données traitées;
- la durée, ou la permanence, des activités de traitement des données;
- l'étendue géographique de l'activité de traitement.

EXEMPLES

Constituent des traitements à grande échelle :

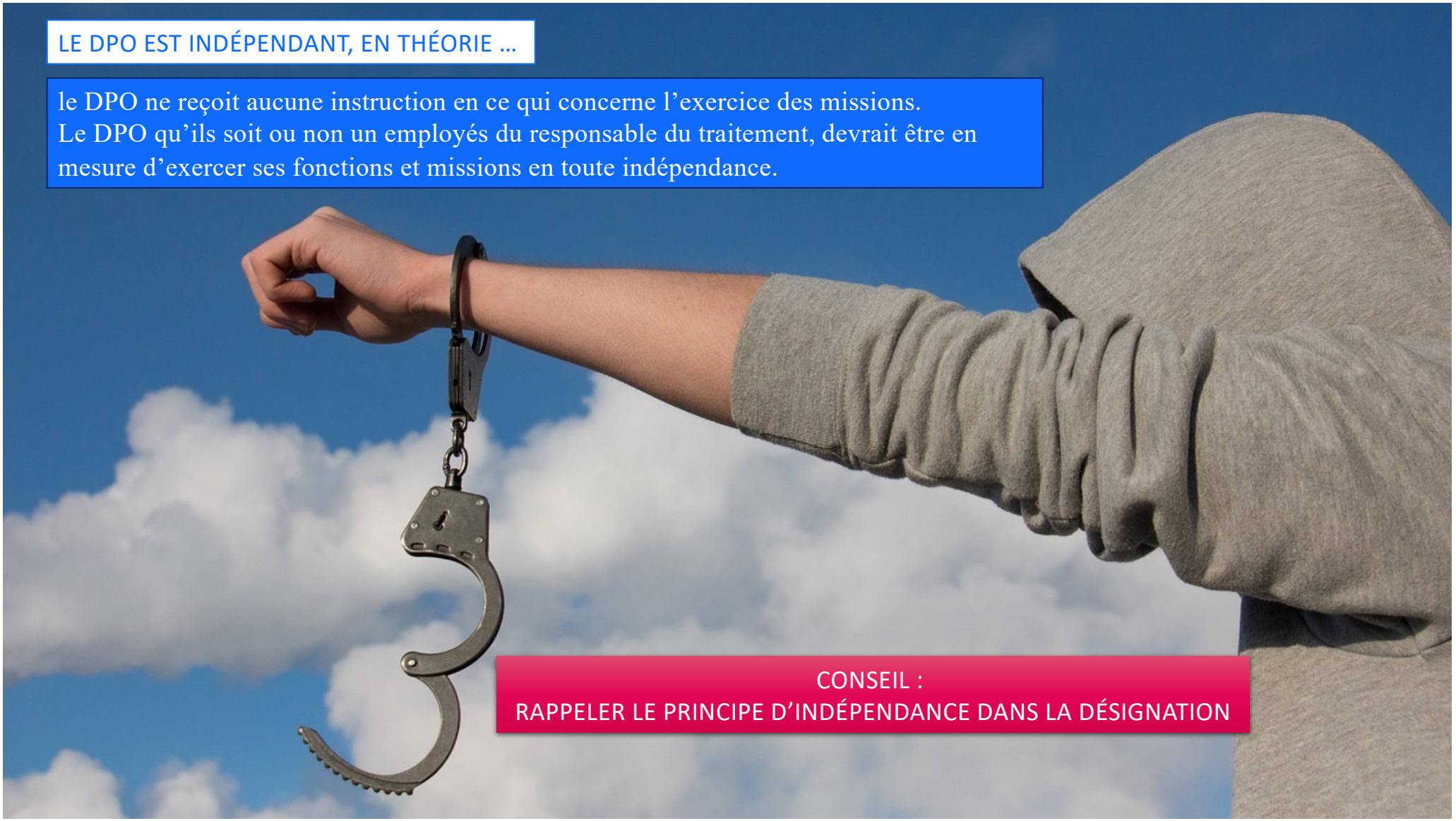
- le traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités ;
- le traitement des données de voyage des passagers utilisant un moyen de transport public urbain (suivi par les titres de transport, par exemple) ;
- le traitement des données de géolocalisation en temps réel des clients d'une chaîne internationale de restauration rapide à des fins statistiques par un sous-traitant spécialisé dans la fourniture de ces services ;
- le traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités ;
- le traitement des données personnelles par un moteur de recherche à des fins de publicité ciblée ;
- le traitement des données (contenu, trafic, localisation) par des fournisseurs de services de téléphonie ou internet[1].

Ne constituent pas des traitements à grande échelle :

- le traitement des données de patients par un médecin de quartier exerçant à titre individuel si la patientèle est inférieure à 10 000 personnes par an (cf. le référentiel pour les cabinets médicaux et paramédicaux) ;
- le traitement des données personnelles relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

LE DPO EST INDÉPENDANT, EN THÉORIE …

le DPO ne reçoit aucune instruction en ce qui concerne l'exercice des missions.
Le DPO qu'ils soit ou non un employés du responsable du traitement, devrait être en mesure d'exercer ses fonctions et missions en toute indépendance.



CONSEIL :
RAPPELER LE PRINCIPE D'INDÉPENDANCE DANS LA DÉSIGNATION

L’article 38, paragraphe 3, dispose que le DPD ne devrait pas être «*relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l’exercice de ses missions*».


UN DPO EXTERNE EST-IL UN SOUS-TRAITANT
AU SENS DU RGPD ?

L'article 38, paragraphe 6, autorise les DPO à «*exécuter d'autres missions et tâches*».
Il exige toutefois que l'organisme veille à ce que «*ces missions et tâches n'entraînent pas de conflit d'intérêts*».

Le DPO peut exercer d'autres fonctions au sein de l'organisme (DPO à temps partiel). Toutefois, il ne doit pas avoir de pouvoir décisionnel sur la détermination des finalités et moyens de traitements : le DPO ne doit donc pas être « juge et partie ». L'existence d'un conflit d'intérêts s'apprécie au cas par cas.

Conseil
indiquer dans la désignation que cette question a été étudiée et qu'il n'y a pas de conflit d'intérêt

Art. 5. Pour l'application de la présente loi, on entend par "autorité publique" :

1° l'état fédéral, les entités fédérées et les autorités locales;

2° les personnes morales de droit public qui dépendent de l'Etat fédéral, des entités fédérées ou des autorités locales;

3° les personnes, quelles que soient leur forme et leur nature qui :

- ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial; et

- sont dotées de la personnalité juridique; et

- dont soit l'activité est financée majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2°, soit la gestion est soumise à un contrôle de ces autorités ou organismes, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes;

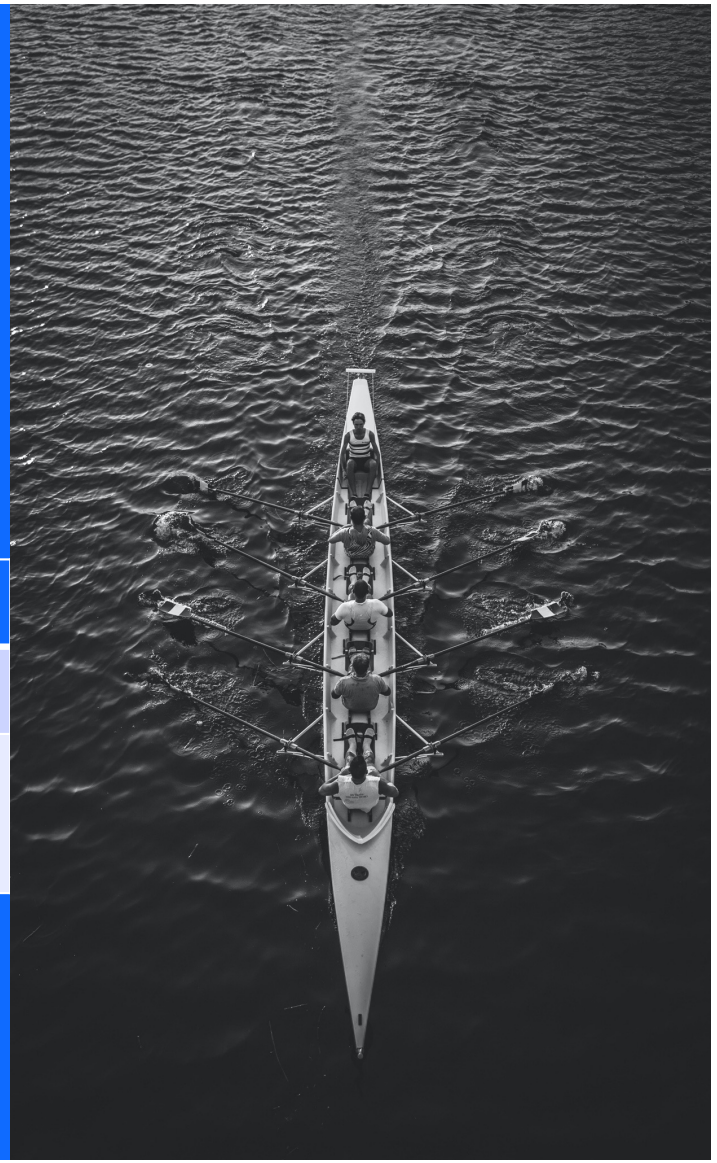
4° les associations formées par une ou plusieurs autorités publiques visées au 1°, 2° ou 3°.


Le DPO ne décide pas
C’est le RT qui décide !
WRONG
WAY

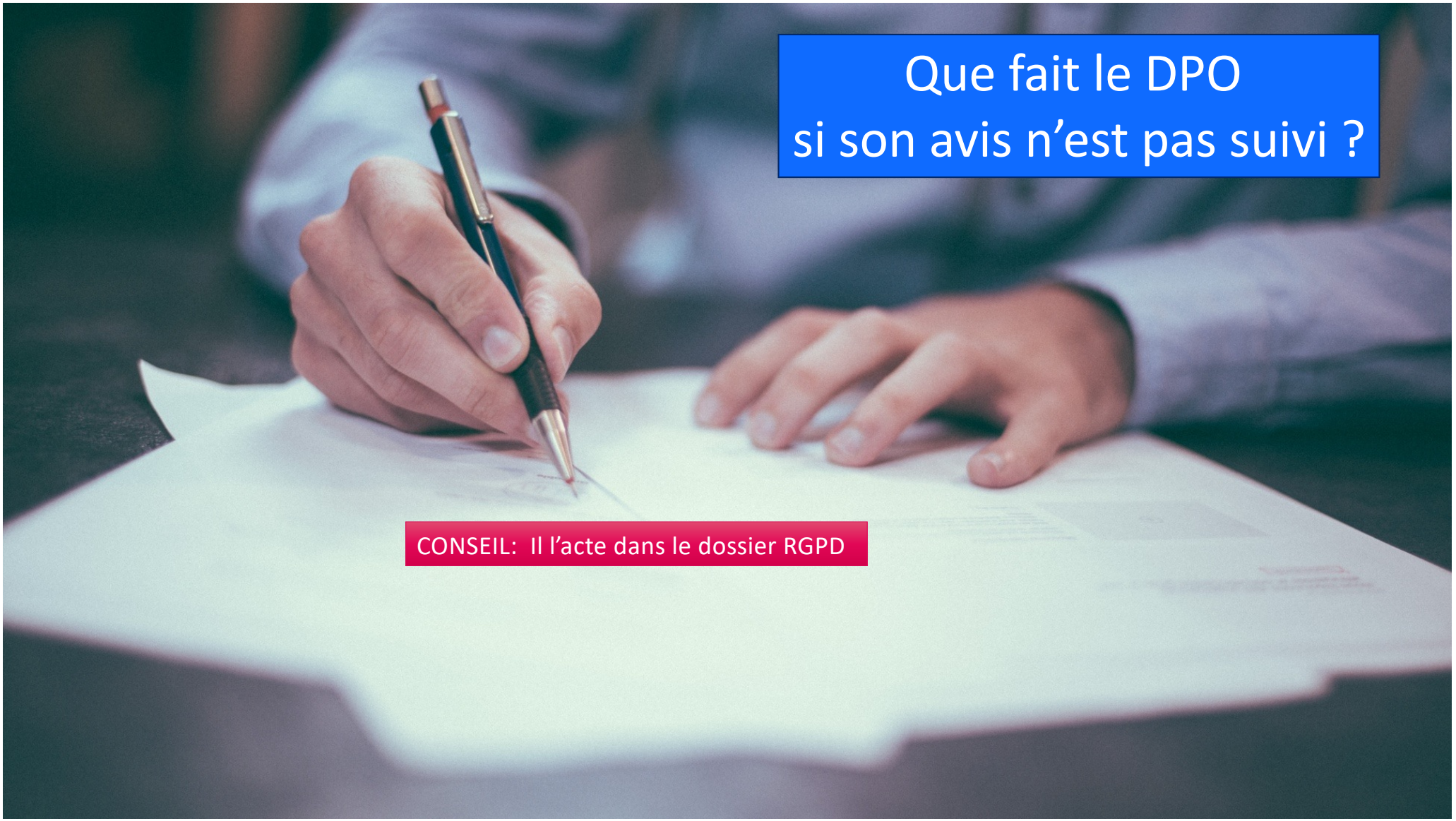

Rôle du DPO
conseil
contrôle

Rôles et fonctions

RÔLE	RGPD	INFOSEC
CONSEIL	DPO	DPO - CISO
OPÉRATIONNEL	CHEF DE PROJET	RSSI



Le DPO a un rôle de conseil et de contrôle du respect du RGPD. Le RGPD comprend les mesures de sécurité techniques et organisationnelles nécessaires pour protéger les données personnelles. Il ne peut participer à des décisions opérationnelles sous peine de conflit d'intérêt avec sa fonction de contrôle	**Le CISO conseille l'organisation quant à la stratégie de sécurité, la mise en place du plan de sécurité, les mesures de sécurité de l'information. Contrairement au DPO son rôle peut aller jusqu'à la recommandation au niveau opérationnel. Plus le CISO a un rôle opérationnel plus la nécessité d'un contrôle externe existe**
Le chef de projet RGPD est en charge, avec les correspondants RGPD dans les différents départements de la mise en place du dossier RGPD, qui, en vertu du principe d'accountability permet au responsable de traitement de démontrer sa mise en conformité.	Le RSSI est en charge de la sécurité de l'information au jour le jour, et cela peut aller jusqu'à la sécurité physique des locaux. Il met en place les mesures préconisées par le CISO et collabore avec le DPO et le chef de projet RGPD
La base de référence est le RGPD et les normes ISO 2700x	La base de référence est les normes ISO 2700x


Que fait le DPO
si son avis n’est pas suivi ?
CONSEIL: Il l’acte dans le dossier RGPD


IMPORTANCE DE RÉALISER
• UN PLAN D'ACTIONS ANNUELLEMENT
• UN BILAN ANNUEL
IMPLEMENT
CONSEIL
IMPORTANCE D'AVOIR AU MOINS UN RV ANNUEL AVEC LA DIRECTION POUR PRÉSENTER BILAN ET PLAN D'ACTIONS

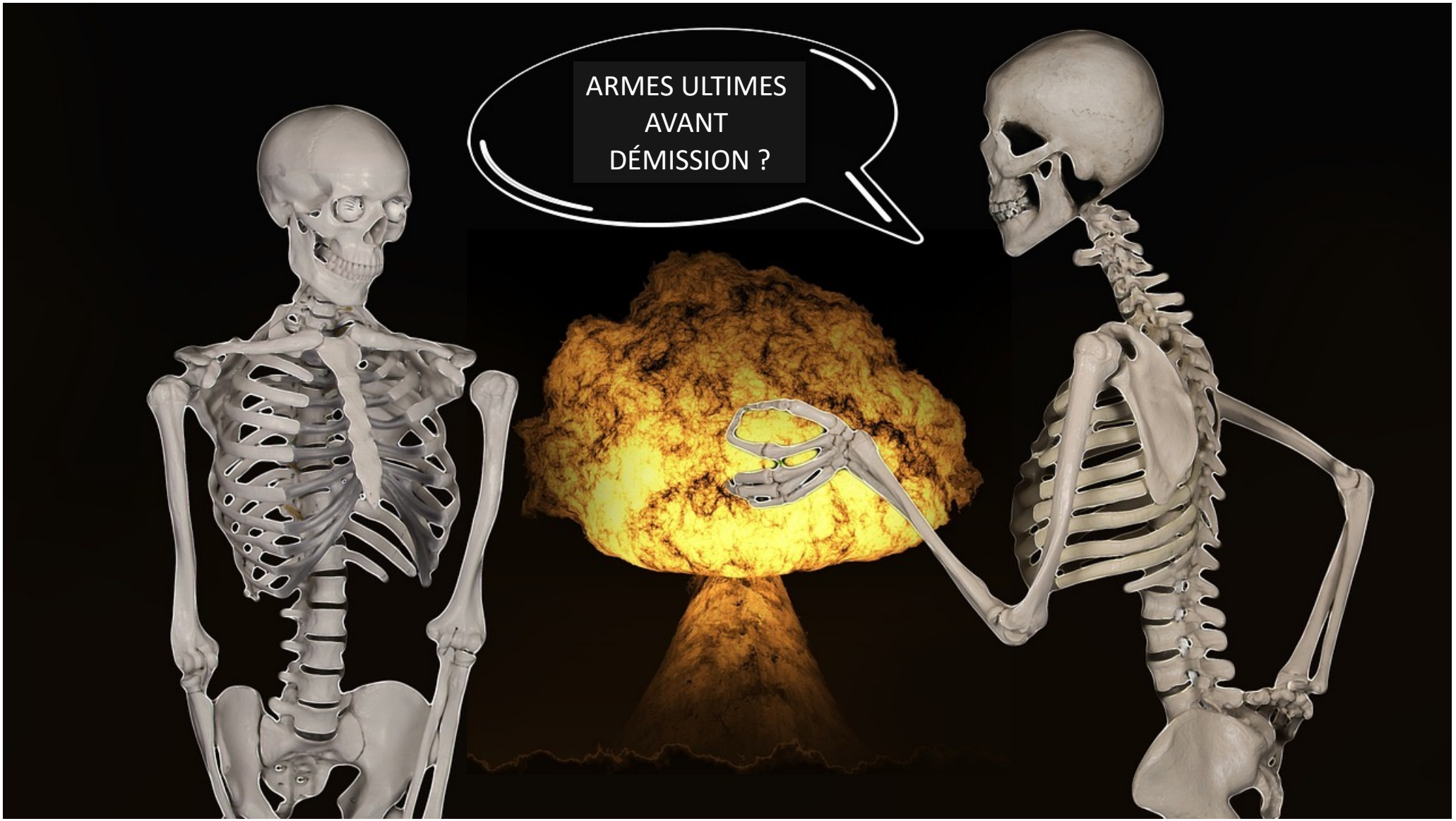
RISK BASED APPROACH

L'article 39, paragraphe 2, requiert que le DPD tienne «*dûment compte [...] du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement*».

CONSEIL

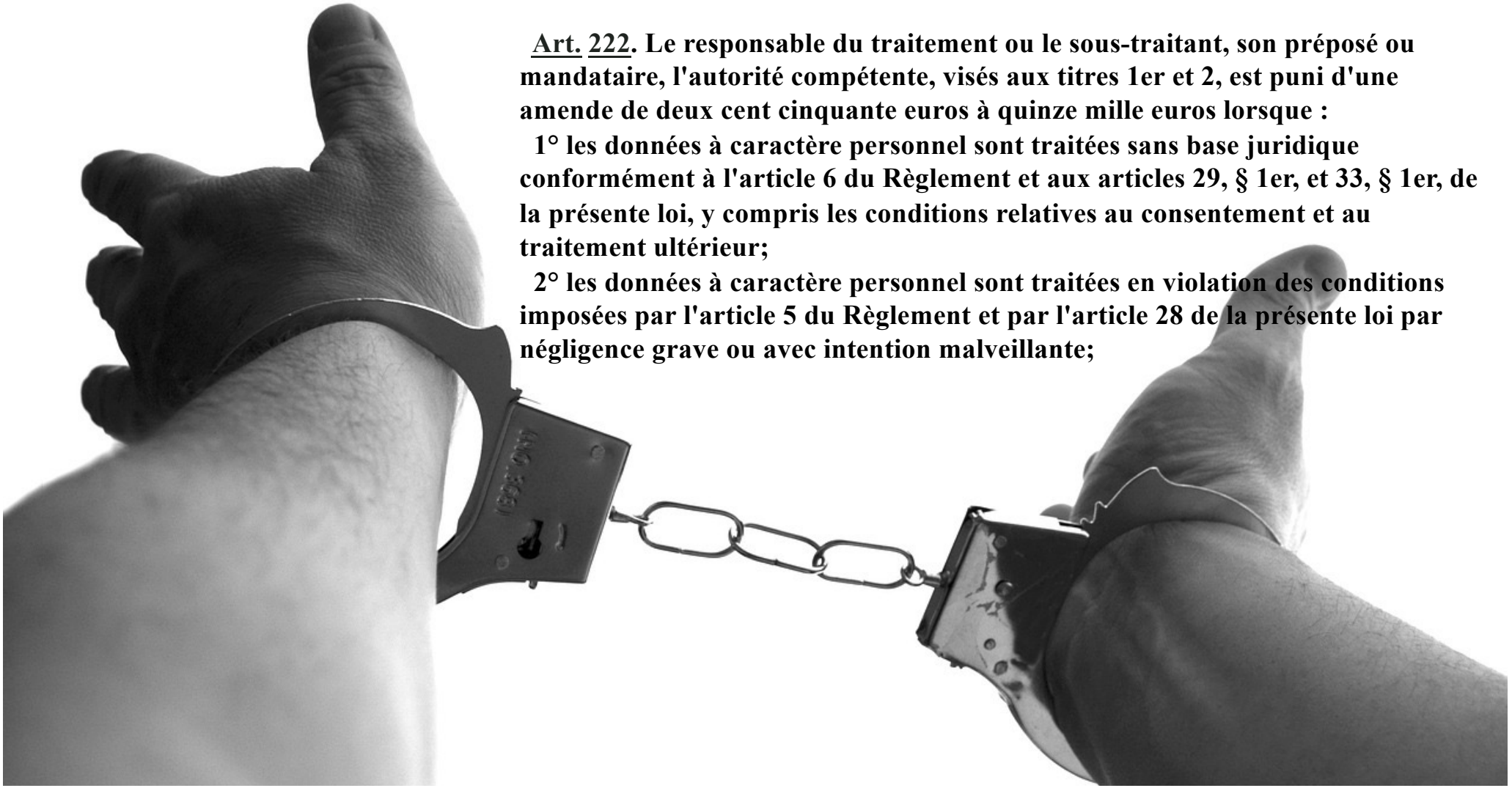
CELA PERMET DE PRIORISER LES ACTIONS DANS LE PLAN D'ACTIONS

LE PLUS RISQUÉ & LE PLUS VISIBLE D'ABORD


ARMES ULTIMES
AVANT
DÉMISSION ?


LE DPO PEUT-IL ETRE LANCEUR D’ALERTE
SI LE RT NE RESPECTE PAS LE RGPD ?

CHAPITRE II. - Sanctions pénales



Art. 222. Le responsable du traitement ou le sous-traitant, son préposé ou mandataire, l'autorité compétente, visés aux titres 1er et 2, est puni d'une amende de deux cent cinquante euros à quinze mille euros lorsque :

1° les données à caractère personnel sont traitées sans base juridique conformément à l'article 6 du Règlement et aux articles 29, § 1er, et 33, § 1er, de la présente loi, y compris les conditions relatives au consentement et au traitement ultérieur;

2° les données à caractère personnel sont traitées en violation des conditions imposées par l'article 5 du Règlement et par l'article 28 de la présente loi par négligence grave ou avec intention malveillante;

Quel avenir pour le *DPO* ?

La vision de la conformité passe par une vision intégrée des risques vers laquelle doit aller le DPO.

Olivier Guillo
Founding partner
Smart Global Governance

L'imbrication des données personnelles et des données non personnelles implique nécessairement l'évolution du métier de ***DPO vers une fonction plus globale de Data Regulation Officer ou de Data Ethic Officer.***

Aurélie Banck
DPO, Compliance Officer
Europcar Mobility Group

Plus qu'un chef d'orchestre de la conformité, le ***DPO devient un facilitateur entre les fonctions*** *métiers pour l'amélioration des processus internes* ***et un ambassadeur de la culture et des valeurs de*** *l'entreprise.*

Jennifer Godin
DPO du groupe ROQUETTE

Une réflexion sur le positionnement du DPO comme acteur de la conformité au sens large au sein de l'entreprise, doit se poser à l'avenir.

Michel Seigne
DPD Touraine Logement

L'intégration des données personnelles dans une gouvernance plus large de la donnée va amener sans doute les entreprises à créer un rôle de Data ***Officer qui va bien au****-delà de celui du DPO.*

Isabelle du Chatelier
Group Data Protection Officer
Dassault Systèmes

Grant Thornton

TEACHPRIVACY

www.teachprivacy.com

Written by Daniel J. Solove

Illustrated by Ryan Beckwith

SOURCE DES GRAPHIQUES

https://go.grant-thornton.fr/rs/238-RET-064/images/2022-12-Grant-Thornton-Enquete%20vis%20ma%20vie%20de%20DPO.pdf