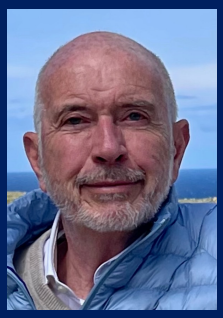
Role et complexité de la fonction de DPO ?



Prof. Dr. Jacques Folon

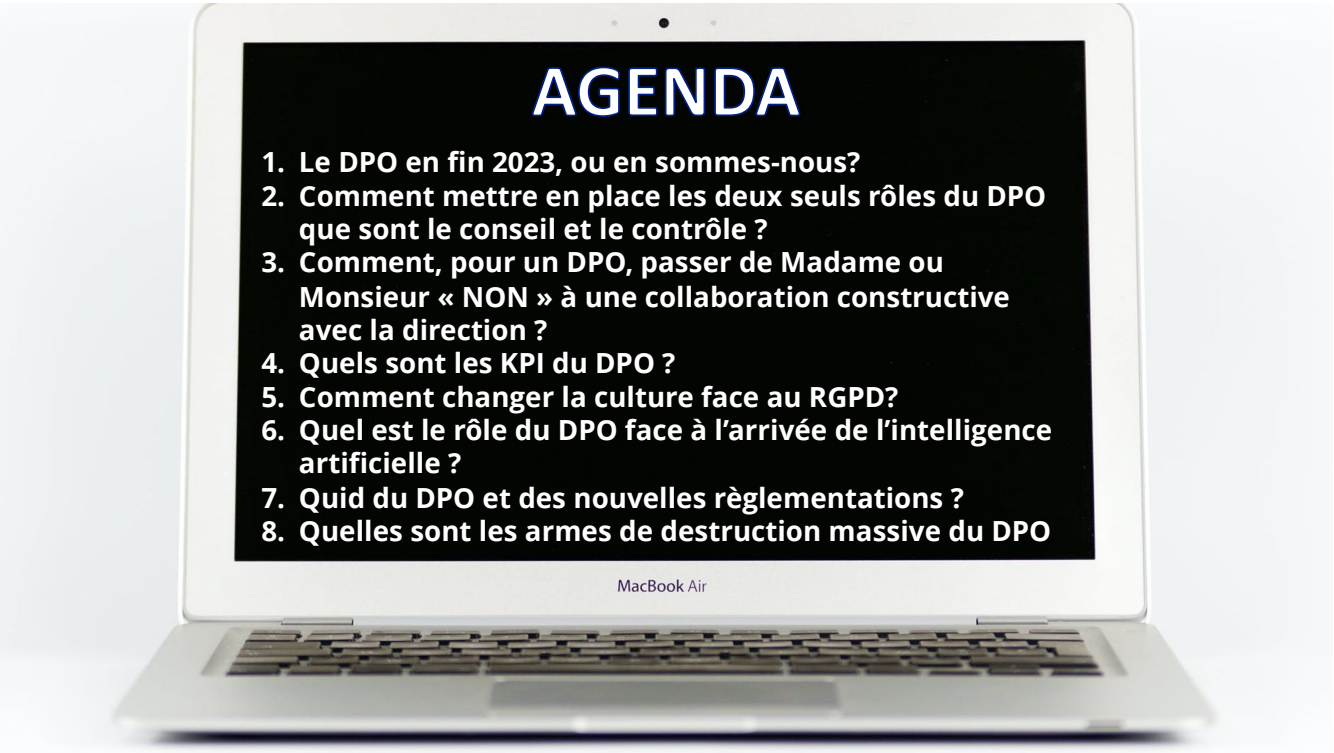
Jacques@gdprfolder.eu

www.linkedin.com/in/folon

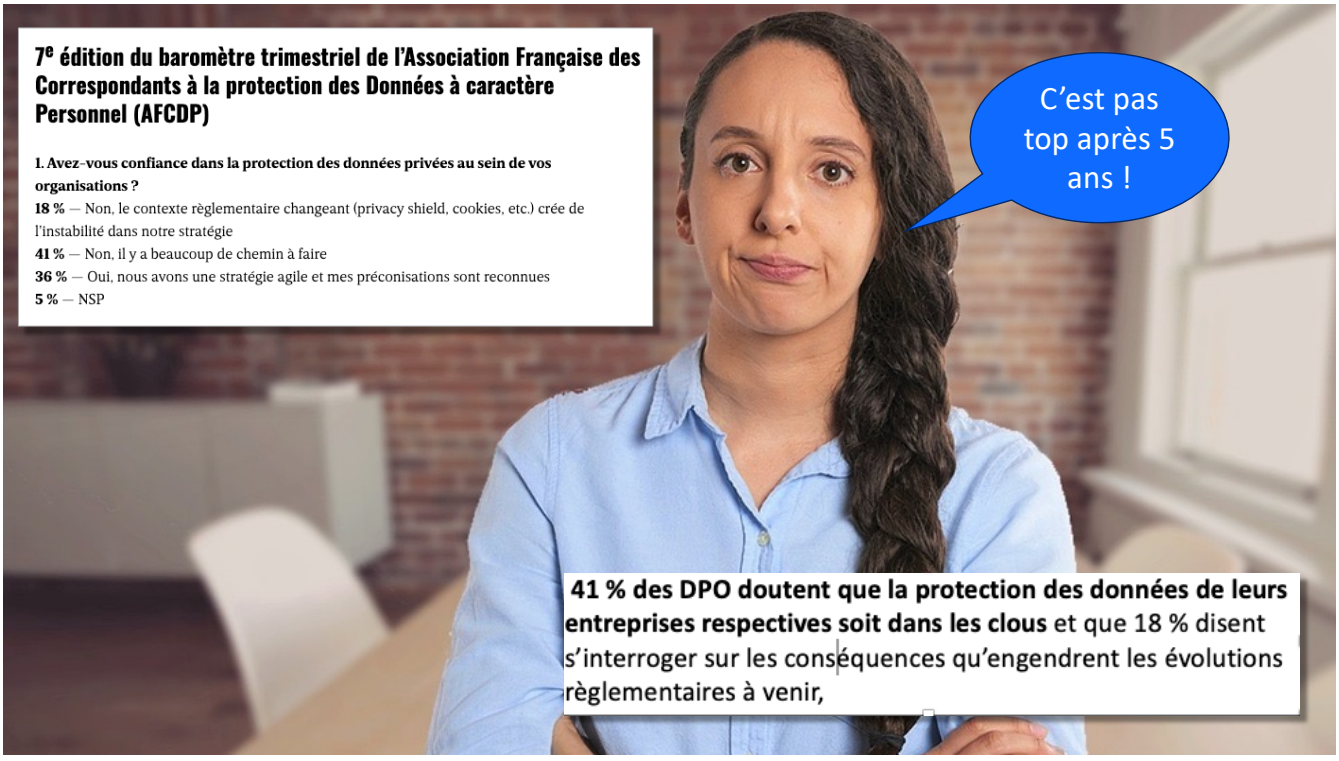
www.gdprfolder.com

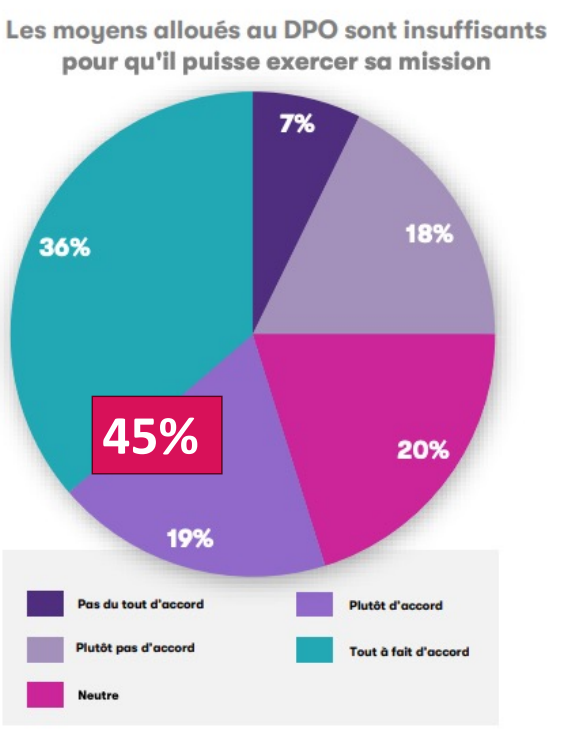
+32 475 98 21 15

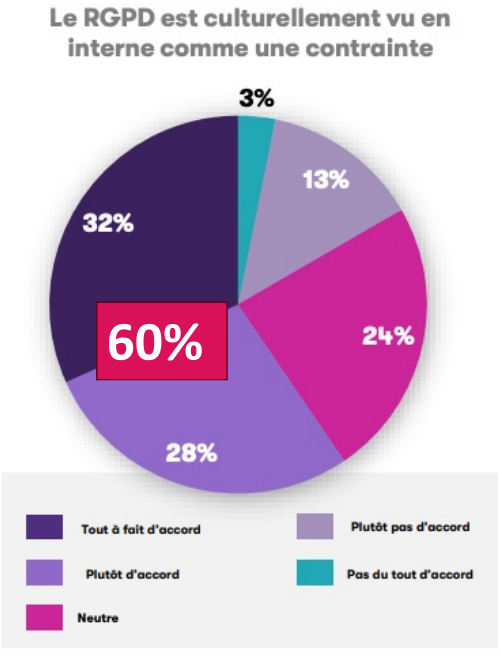
www.folon.com



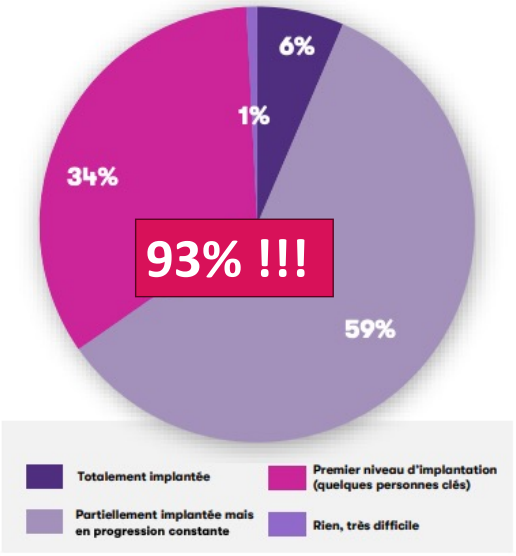

1/ DPO en fin 2023
Ou en sommes-nous?
MacBook Air


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
C'est pas top après 5 ans !
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,

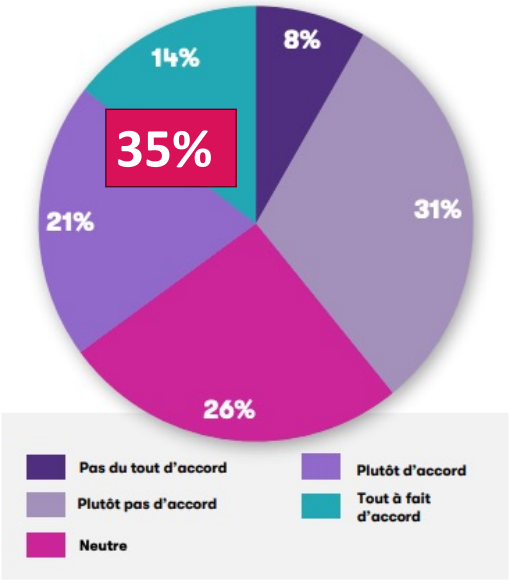

Les moyens alloués au DPO sont insuffisants pour qu'il puisse exercer sa mission
7%
18%
36%
45%
20%
19%
Pas du tout d'accord
Plutôt d'accord
Plutôt pas d'accord
Tout à fait d'accord
Neutre


Le RGPD est culturellement vu en interne comme une contrainte
3%
13%
32%
60%
24%
28%
Tout à fait d'accord
Plutôt pas d'accord
Plutôt d'accord
Pas du tout d'accord
Neutre

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



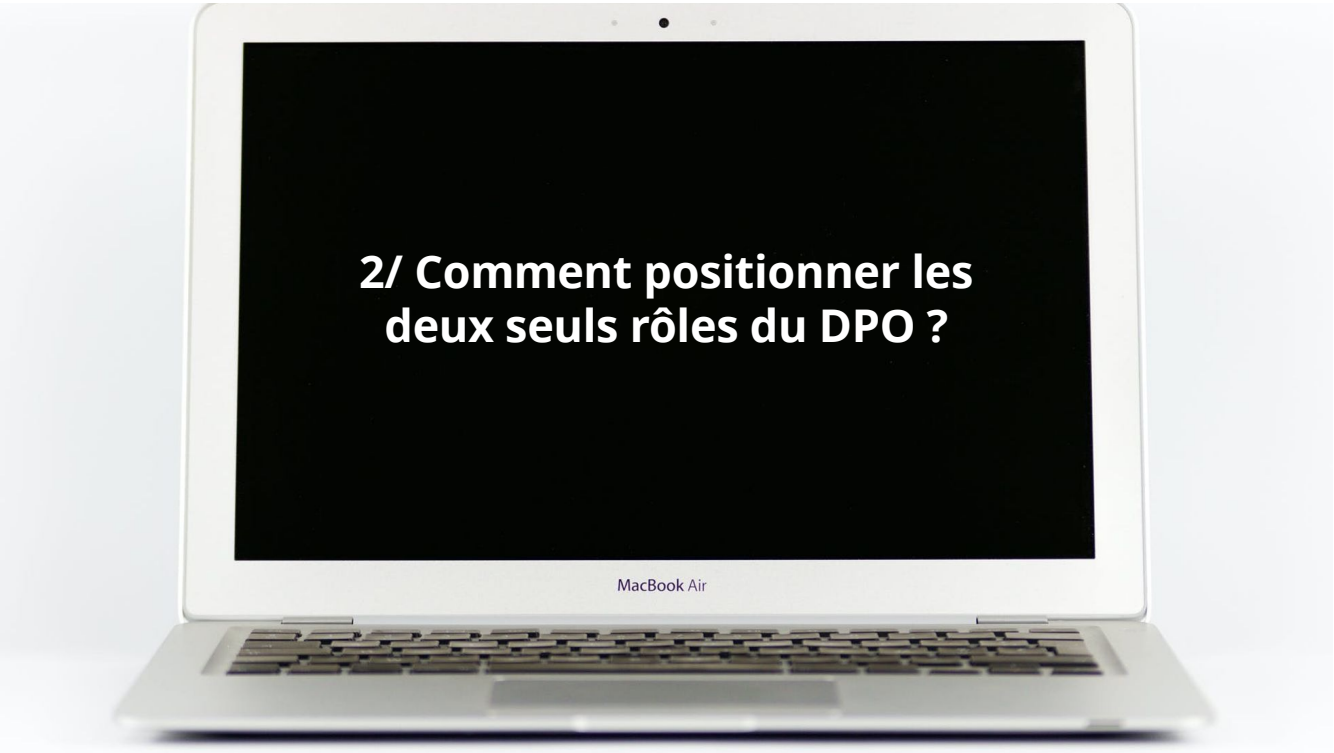
Nos clés pour une gouvernance adaptée

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

C'est beau la théorie !

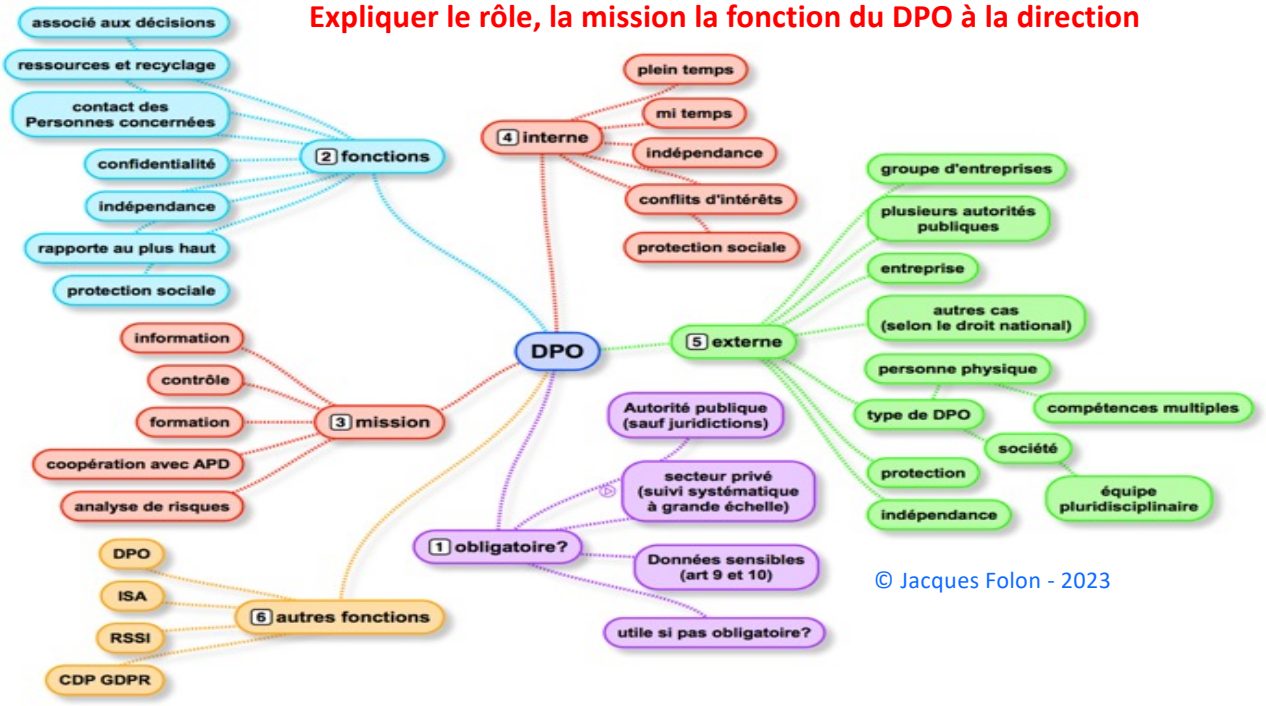
Grant Thornton




Les deux seuls rôles du DPO
conseil
contrôle


Importance d'être présenté
à la direction

Expliquer le rôle, la mission la fonction du DPO à la direction



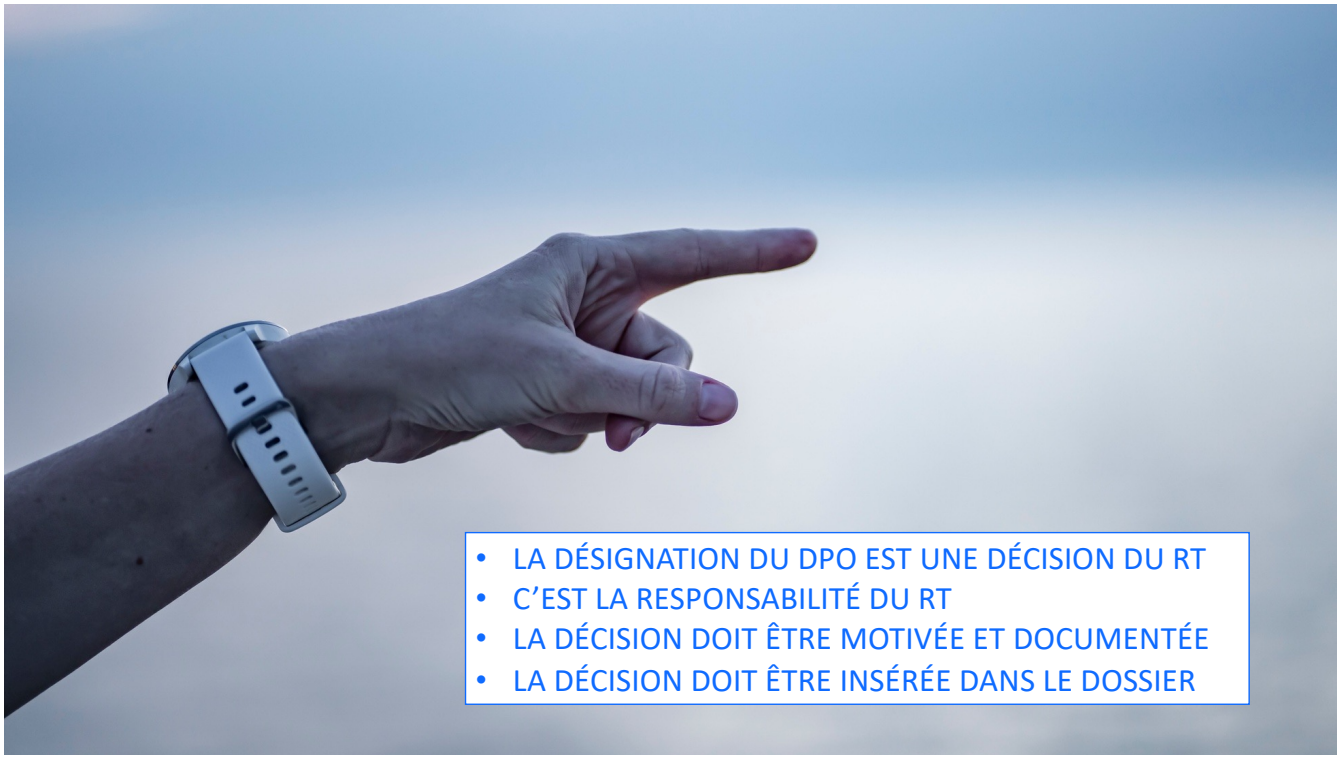
Rappeler que le DPO ne décide pas: c'est le RT qui décide !

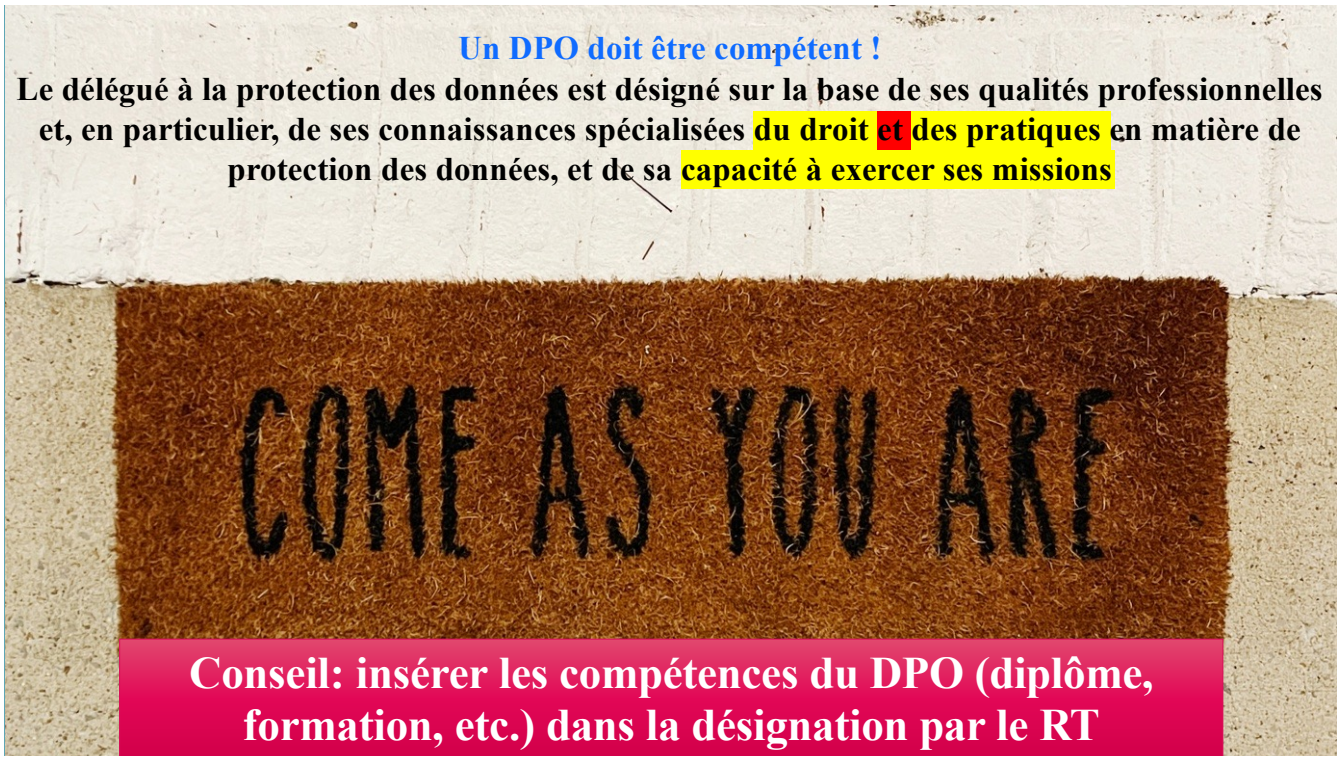
Rôles et fonctions

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


• 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


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
COME AS YOU ARE
Conseil: insérer les compétences du DPO (diplôme, formation, etc.) dans la désignation par le RT


QUI PEUT ÊTRE DPO ?
Attention aux conflits d'intérêts

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

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

FORMATION MINIMALE
- 12 JOURS
- DROIT
- SÉCURITÉ INFORMATION (iso 2700X)
- 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
- PAS DE CONFLIT D'INTERET INTERNE


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


ET SI ON CREAIT UN
INSTITUT DES DPO
POUR METTRE UN PEU D'ORDRE
DANS LA PROFESSION ?
LE 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.
TROP DE DPO SONT NOMMES SANS REFLEXION SUR LE ROLE DE LA FONCTION ET LES COMPETENCES NECESSAIRES

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

L'article 38, paragraphe 2, du RGPD exige que l'organisme aide son DPO *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 DPO 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 DPO 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 DPO puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services;
- formation continue.

L'article 38, paragraphe 3, dispose que le DPO 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*».

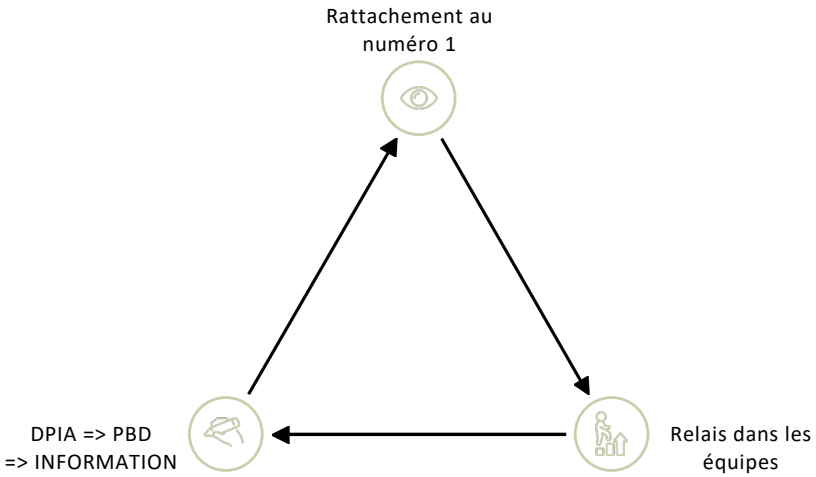
UN DPO EXTERNE EST-IL UN SOUS-TRAITANT AU SENS DU RGPD ?

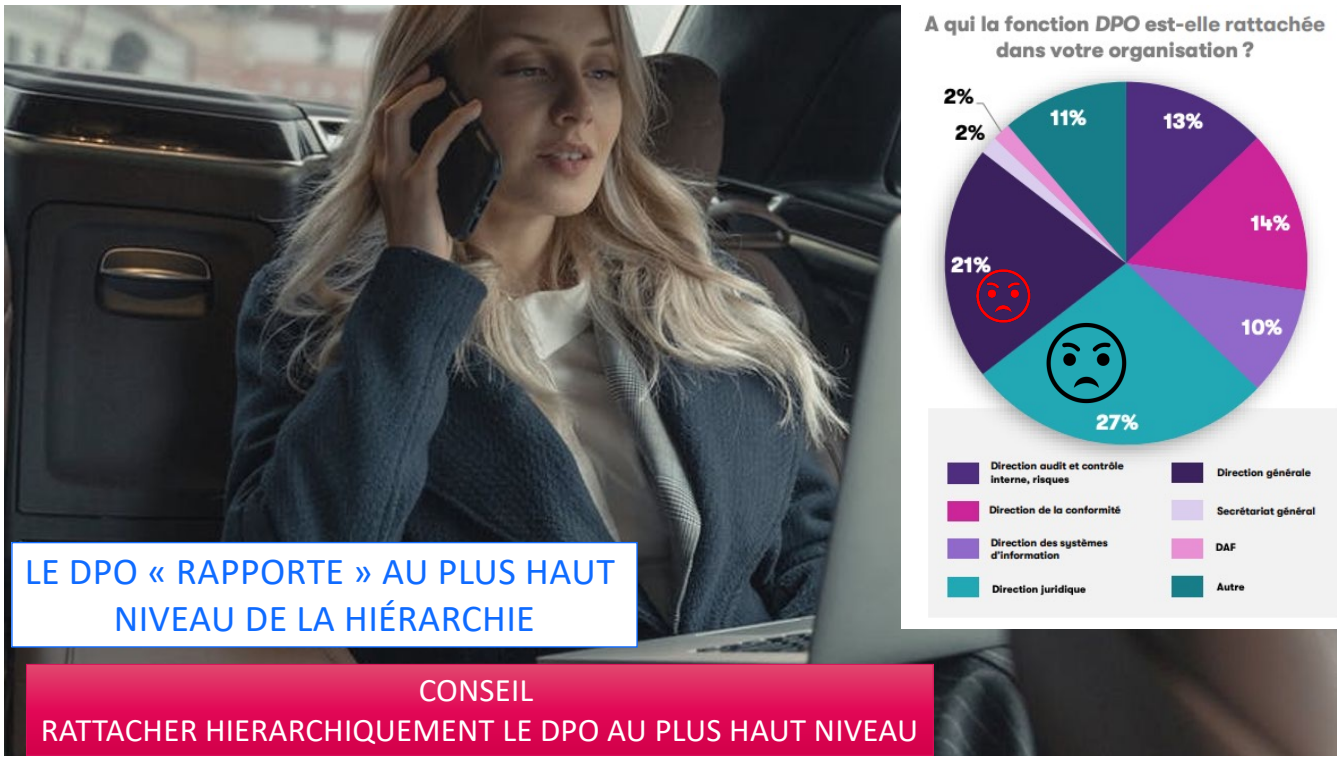
Administration publique ?

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°.

3/COMMENT NE PAS ÊTRE MONSIEUR OU MADAME NON ET CRÉER UNE COLLABORATION CONSTRUCTIVE ?

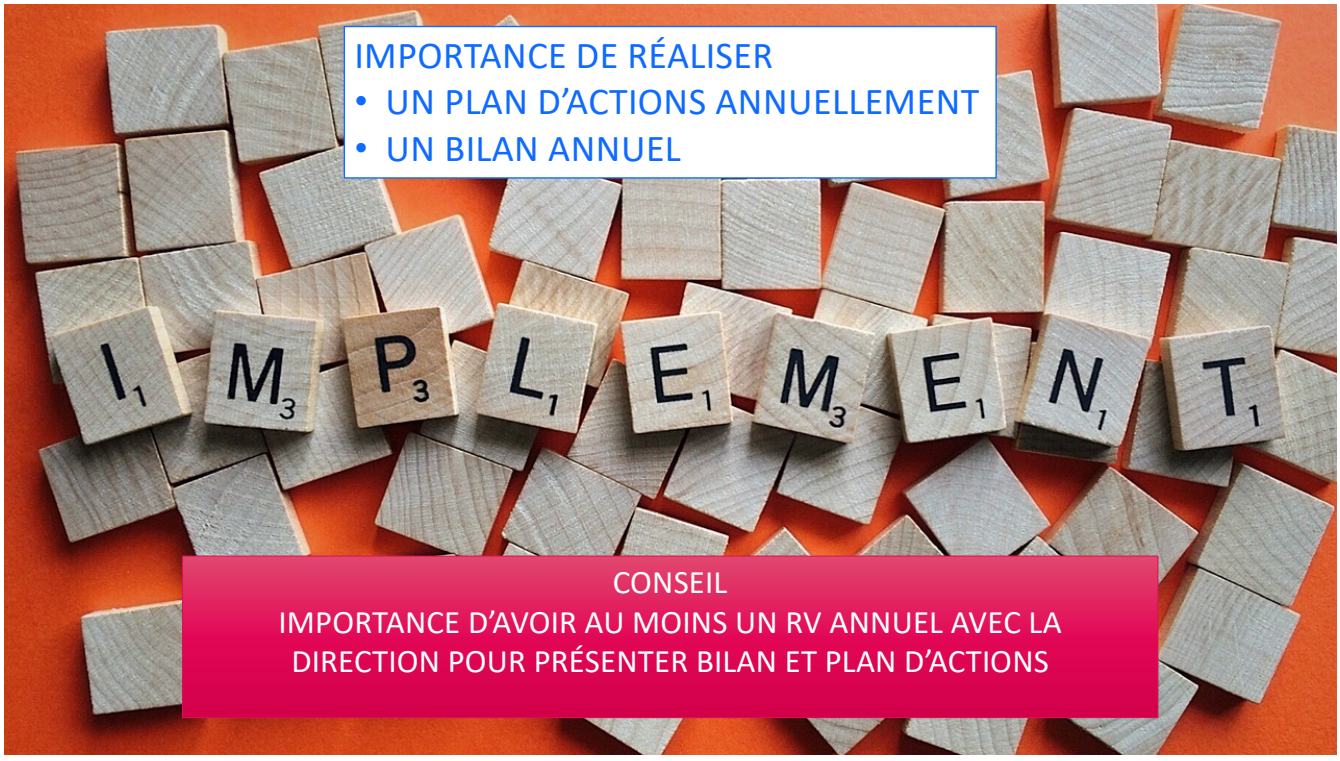
TROIS MOYENS DE NE PAS DEVOIR DIRE NON ET D'ÊTRE INFORMÉ "EN TEMPS UTILE"





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

CONSEIL
RATTACHER HIERARCHIQUEMENT LE DPO AU PLUS HAUT NIVEAU



IMPORTANCE DE RÉALISER
- UN PLAN D'ACTIONS ANNUELLEMENT
- UN BILAN ANNUEL

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

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 DPO 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, l'EDPB recommande, à titre de bonne pratique, de consigner les raisons pour lesquelles l'avis du DPO n'a pas été suivi;**
- **le DPO 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

CRÉER UN RÉSEAU DE CORRESPONDANTS DANS LES DIFFÉRENTS DÉPARTEMENTS PERMET D'ÊTRE INFORMÉ

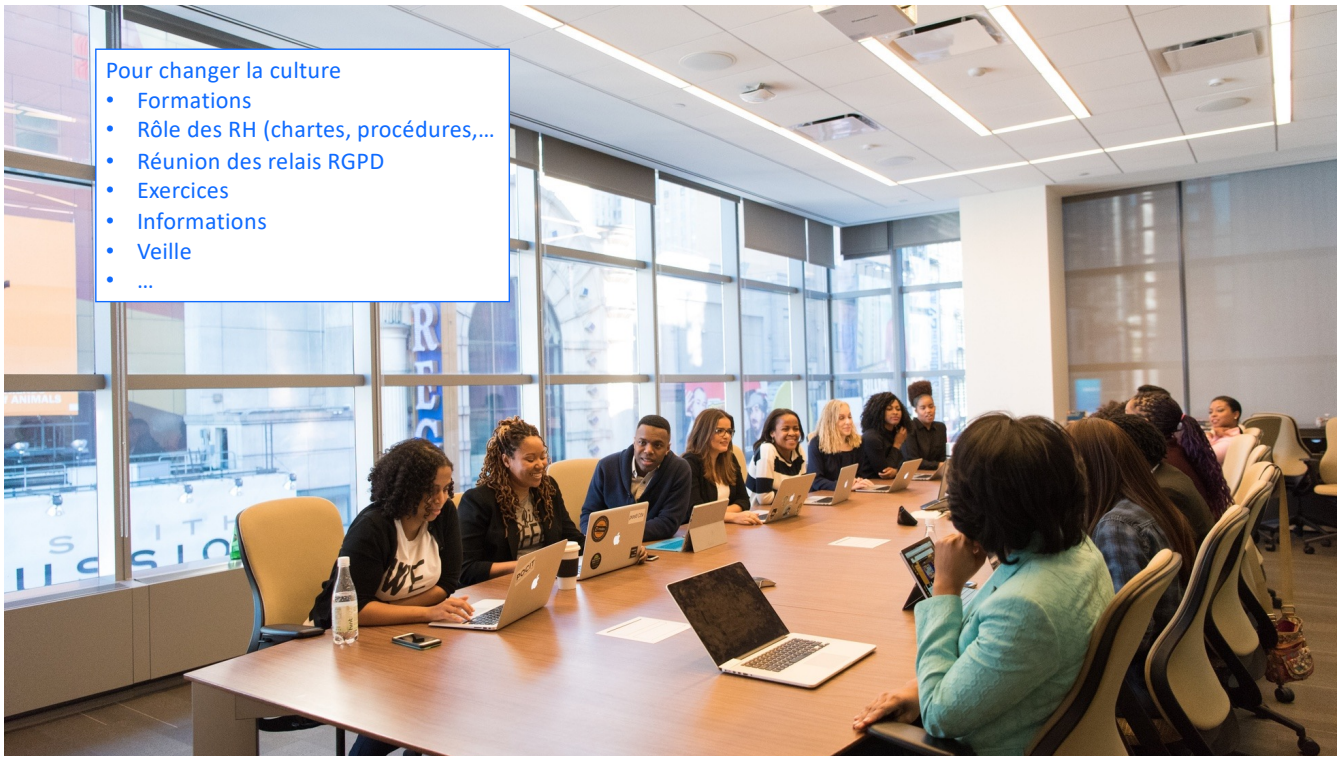
4/ QUELS SONT LES KPI DU DPO ?

LE SEUL KPI PERMANENT EST LE « DOSSIER RGPD »

- C'EST LA BASE DU PLAN D'ACTIONS
- C'EST LA BASE DU BILAN ANNUEL
- C'EST LA COLONNE VERTÉBRALE DU RGPD
- C'EST LA PREUVE DE L'ACCOUNTABILITY


5/ culture d’entreprise


CHANGER UNE CULTURE D’ENTREPRISE
• CA PREND DU TEMPS !
• LES VALEURS
• LES RITES
• LES HISTOIRES
• IL FAUT ÊTRE PATIENT


Pour changer la culture
• Formations
• Rôle des RH (chartes, procédures,…
• Réunion des relais RGPD
• Exercices
• Informations
• Veille
• …


6/ RGPD ET IA : DEUX FRÈRES ENNEMIS ?
CAUTION
Inicio
Re Pág
Av Pág

Leonardo Cervera Navas
Director of the European Data Protection Supervisor.

EDPS
European Data Protection Supervisor

“Nous devrons avoir une interprétation souple du RGPD dans le cadre du développement de l’intelligence artificielle”

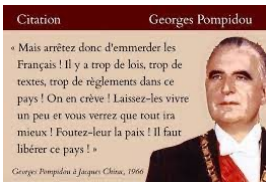
Journée d’étude DPOPRO du 25/8/2018 à la FEB

Rôle du DPO

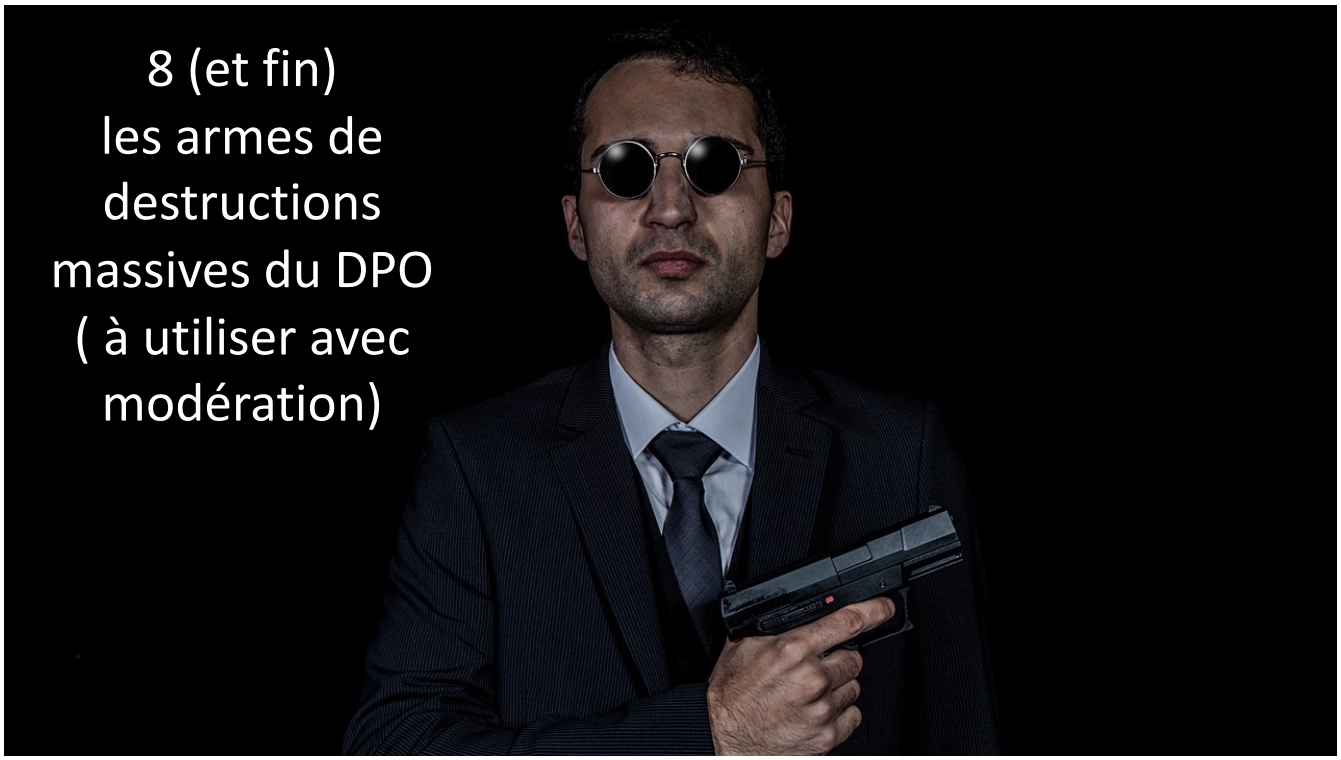
- Veille technologique
- Veille réglementaire
- Information du personnel
- Gestion des risques
- Charte IA => charte informatique

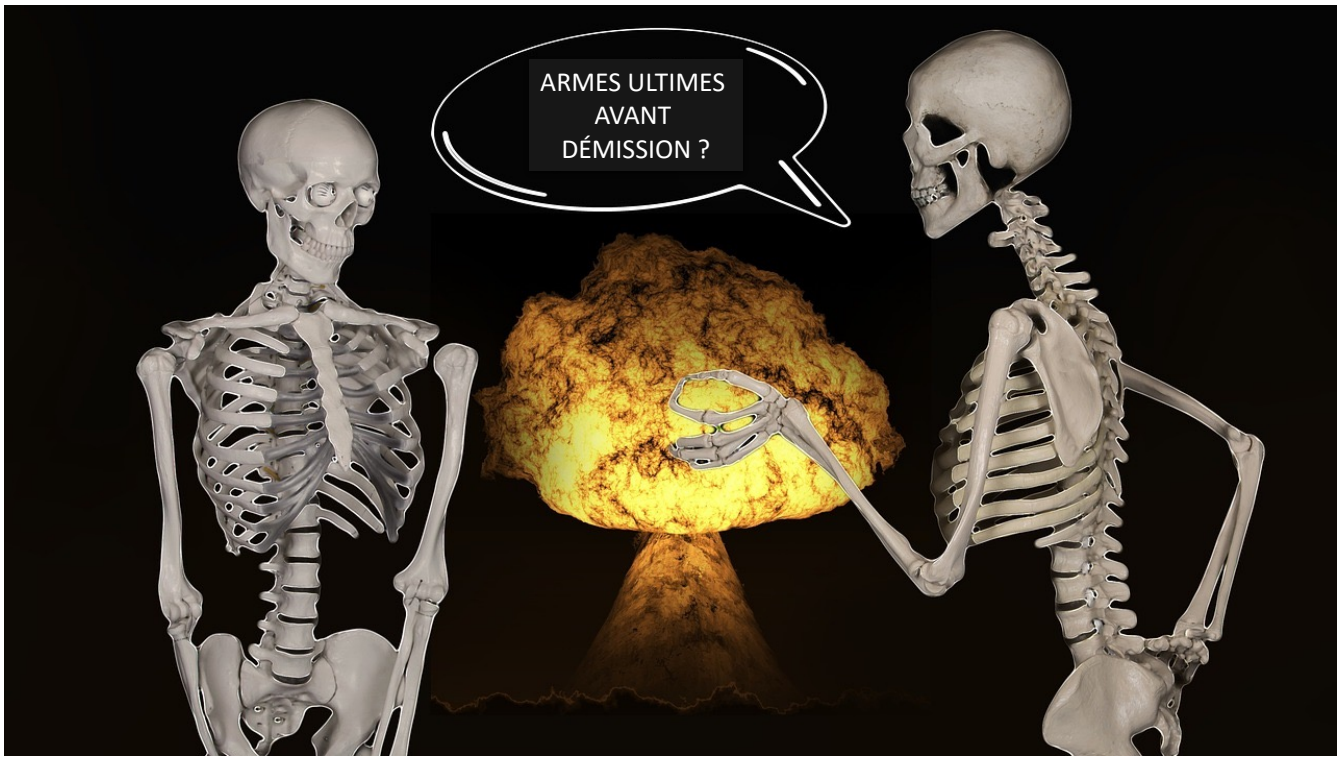
7. Nouvelles règlementations

Un excès de règlementations !
Et tout ça pour le DPO !

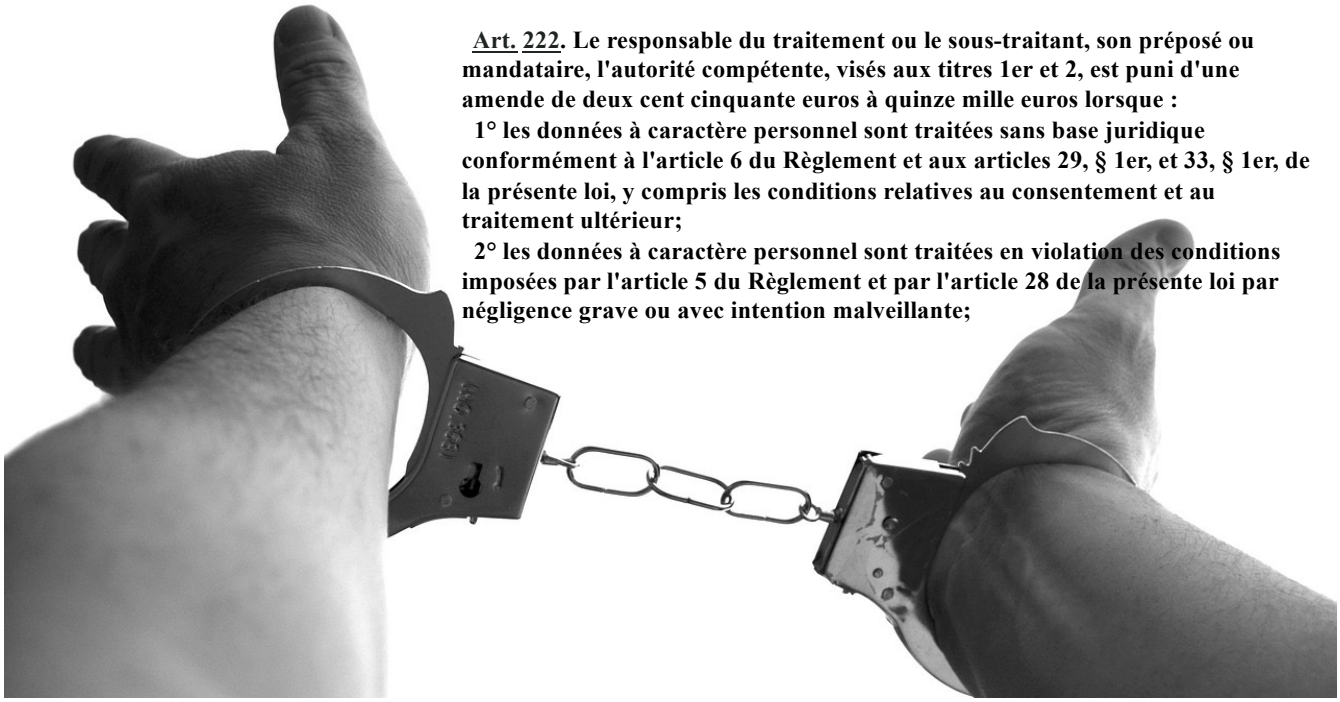



Et n’oublions pas
les lanceurs d’alerte


8 (et fin)
les armes de
destructions
massives du DPO
(à utiliser avec
modération)


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 :

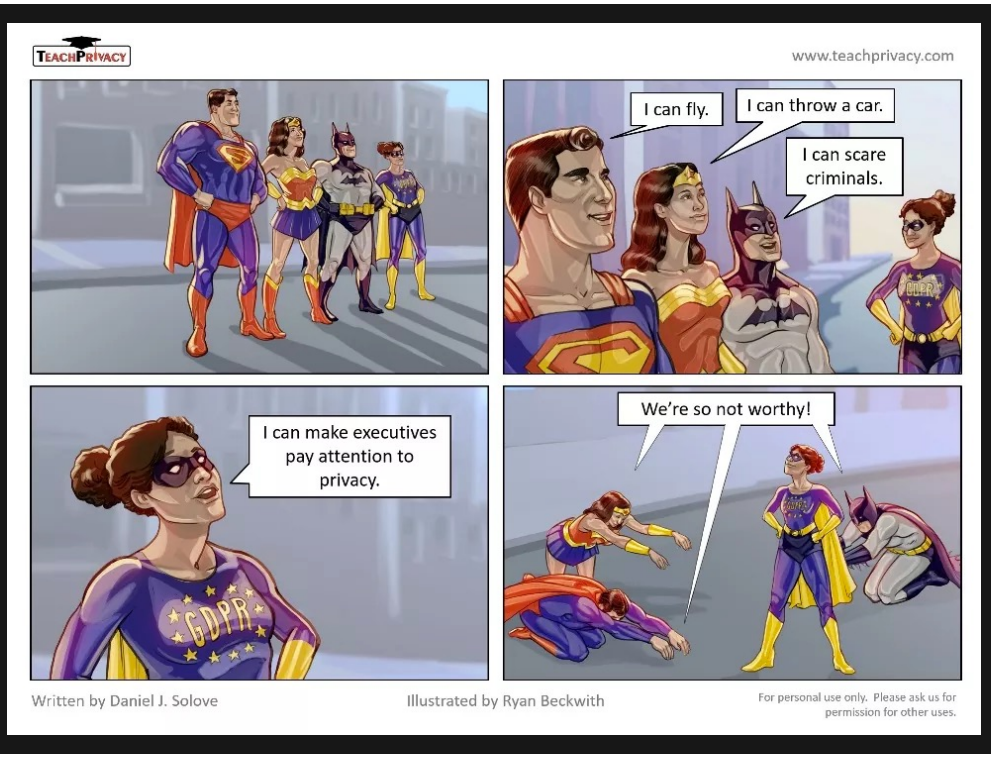
1° les données à caractère personnel sont traitées sans base juridique conformément à l'article 6 du Règlement et aux articles 29, § 1er, et 33, § 1er, de la présente loi, y compris les conditions relatives au consentement et au traitement ultérieur;

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;

CONCLUSION

LES DPO SONT DES PERSONNES EXCEPTIONNELLES, DES SUPER HÉROS.

MAIS EST-CE QUE LES AUTRES LE SAVENT ?




No one knows
what it's like
To be The
Batman


THANK YOU

SOURCE DES GRAPHIQUES

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