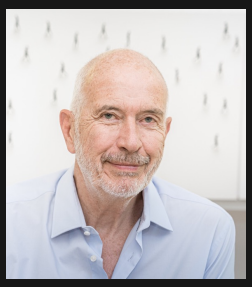
INTRODUCTION ET ACTUALITÉS

GESTION ET PROTECTION DES DONNÉES



Prof. Dr. Jacques Folon

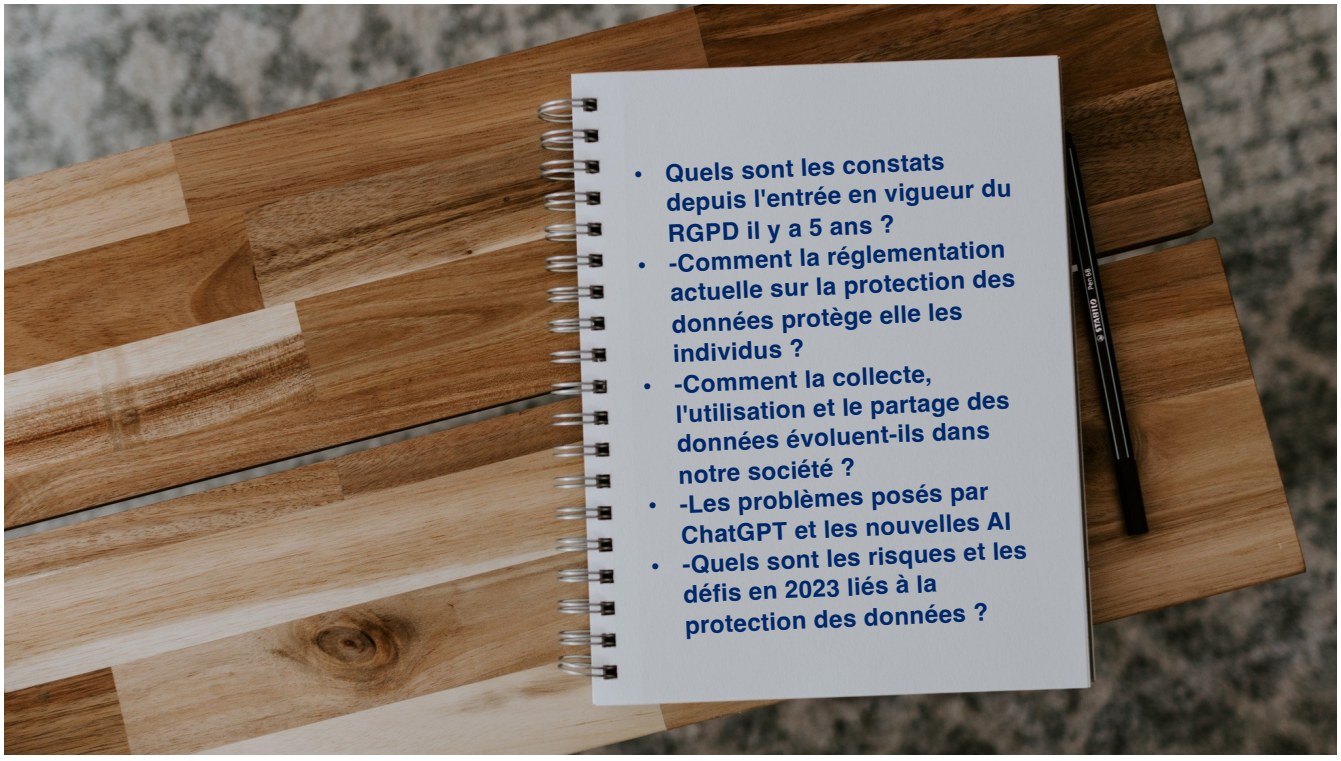
Jacques@gdprfolder.eu

www.linkedin.com/in/folon

www.gdprfolder.com

+32 475 98 21 15

www.folon.com

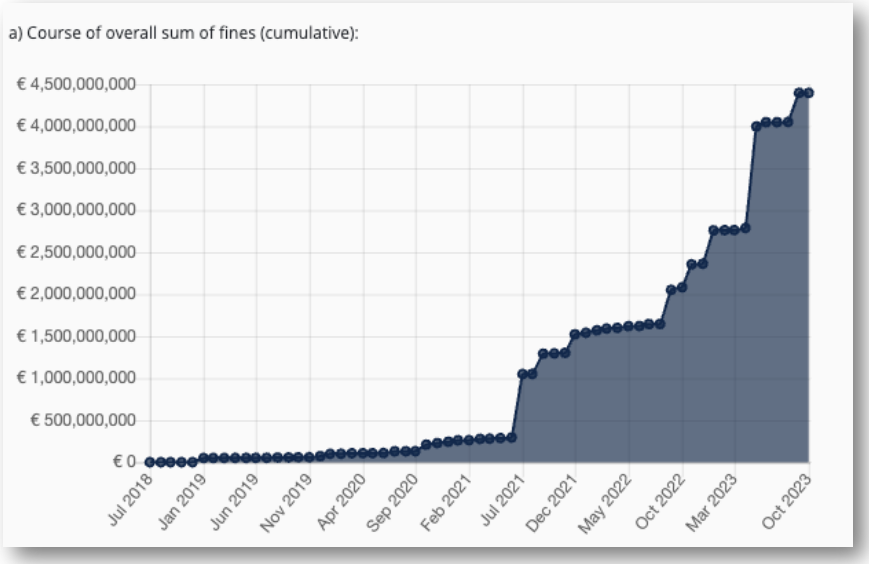



YOU ARE HERE
CONSTATS
APRES 5ANS


1998 - 2013
5 ANS DE RGPD
PETIT RAPPEL

ON LE SAVAIT DEPUIS 2016 ET … COMME LE BUG DE L'AN 2000
CE FUT COMME UNE SURPRISE

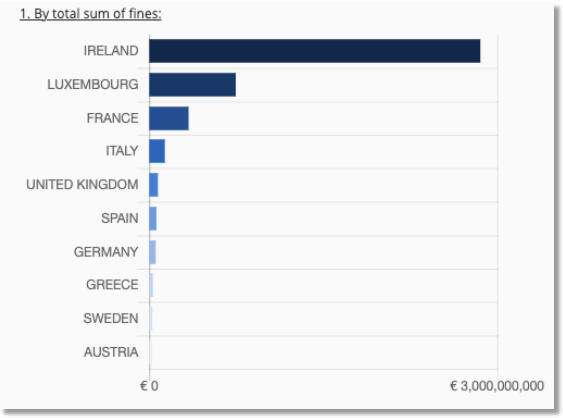
LES AMENDES QUI FONT PEUR !



GDPR Enforcement Tracker
https://www.enforcementtracker.com

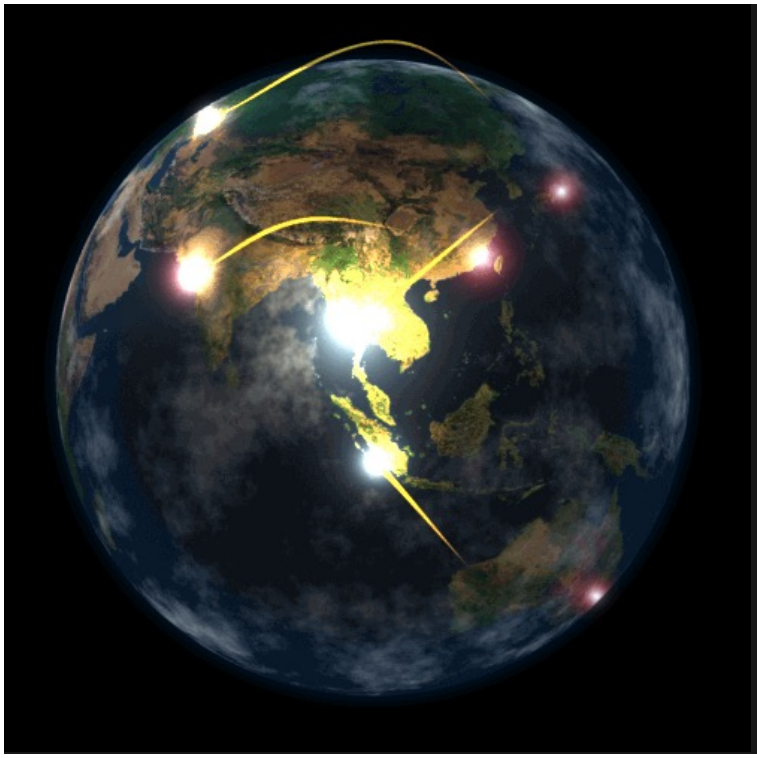
GDPR Enforcement Tracker - list of GDPR fines

Country	Number of Fines
SPAIN	748 (with total € 61,598,990)
ITALY	302 (with total € 134,279,327)
GERMANY	163 (with total € 55,385,033)
ROMANIA	155 (with total € 906,250)
HUNGARY	68 (with total € 2,518,861)
GREECE	59 (with total € 30,961,000)
POLAND	58 (with total € 3,480,869)
NORWAY	50 (with total € 10,417,950)
BELGIUM	40 (with total € 1,852,000)
CYPRUS	38 (with total € 1,366,500)



Violation	Number of Fines
Insufficient legal basis for data processing	590 (with total € 1,643,047,672)
Non-compliance with general data processing principles	493 (with total € 2,025,714,979)
Insufficient technical and organisational measures to ensure information security	339 (with total € 382,382,575)
Insufficient fulfilment of data subjects rights	181 (with total € 97,466,570)
Insufficient fulfilment of information obligations	179 (with total € 237,275,500)
Insufficient cooperation with supervisory authority	88 (with total € 6,146,029)
Insufficient fulfilment of data breach notification obligations	32 (with total € 1,781,082)
Insufficient involvement of data protection officer	15 (with total € 919,300)
Insufficient data processing agreement	11 (with total € 1,057,110)
Unknown	9 (with total € 9,250,000)

MANQUE DE CERTIFICATIONS



CONTEXTE DU RGPD
NOTRE MONDE EN 2023


CYBERSECURITY
YOU'VE BEEN HACKED!

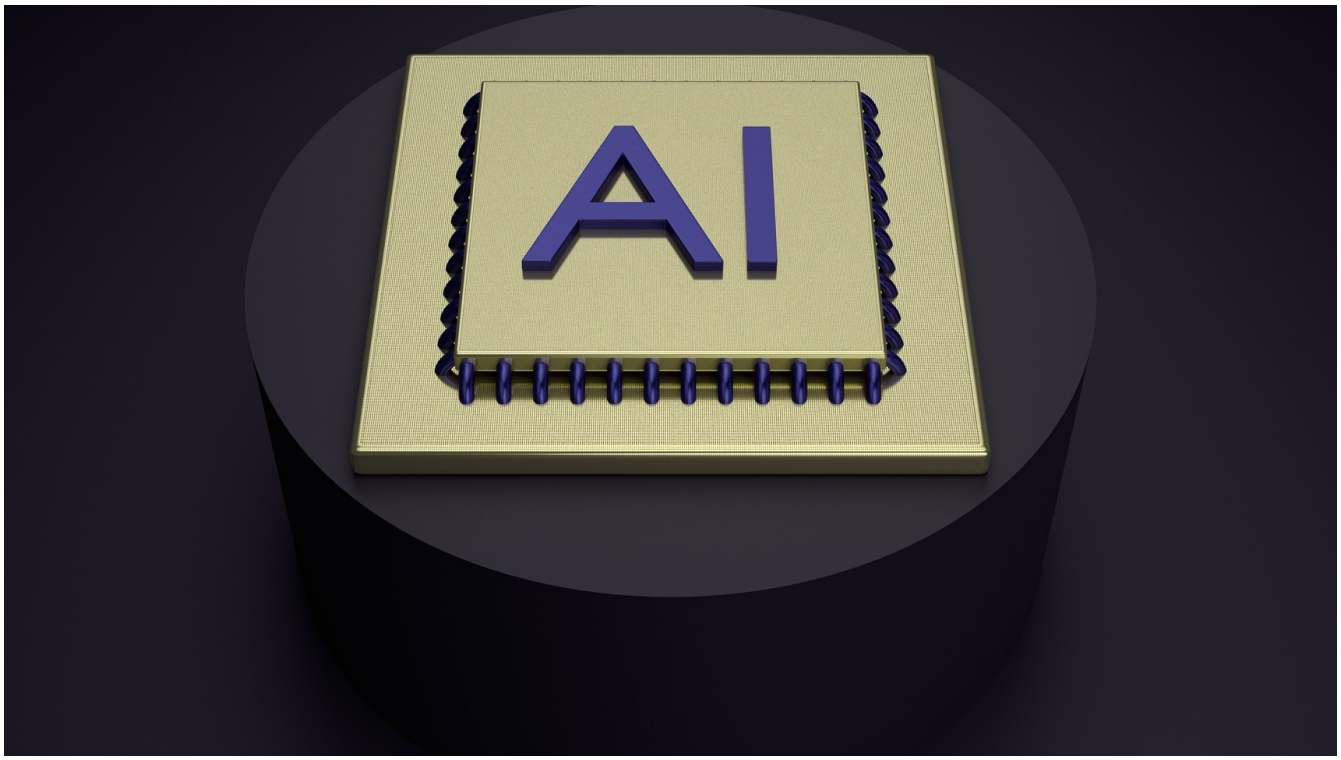
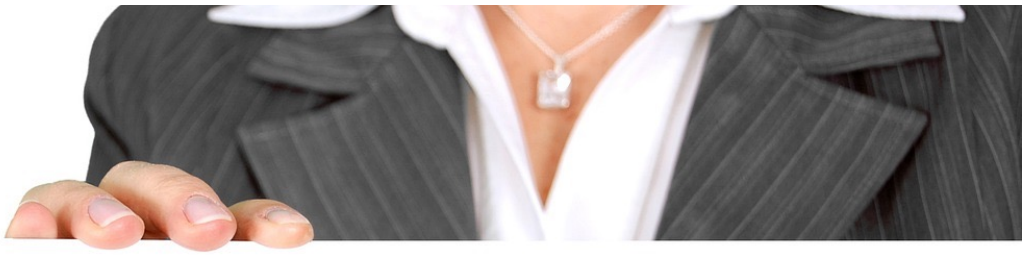
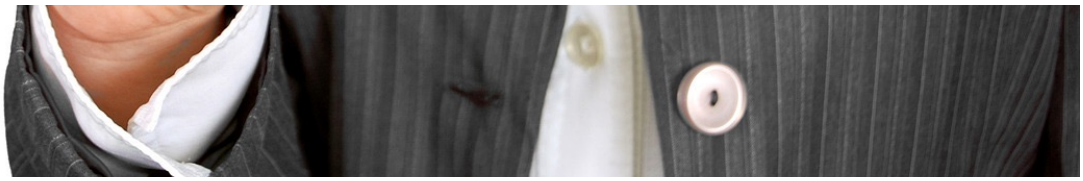

AI

TABLE DES MATIÈRES

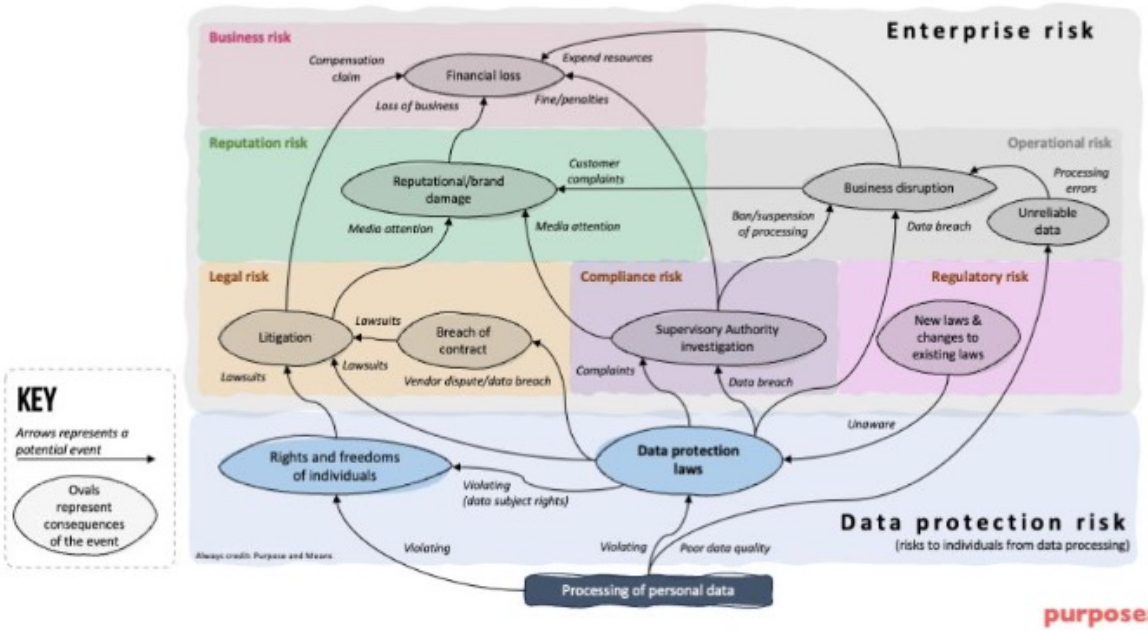


QUALITY CONTROL

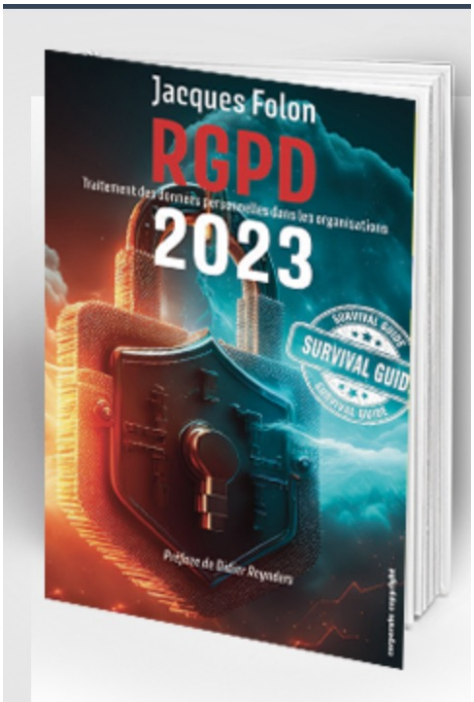
DPO AUTO-CERTIFIES

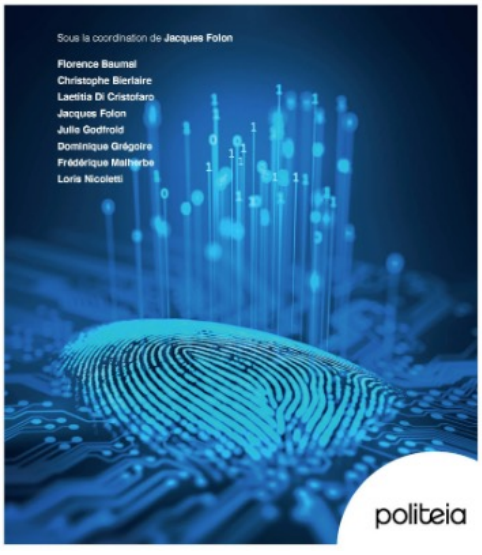


LINKING DATA PROTECTION RISK TO ENTERPRISE RISK



purposeandmeans.io



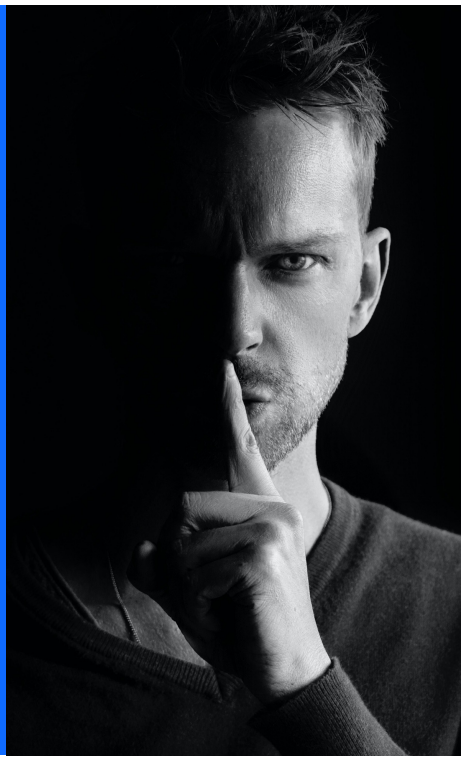


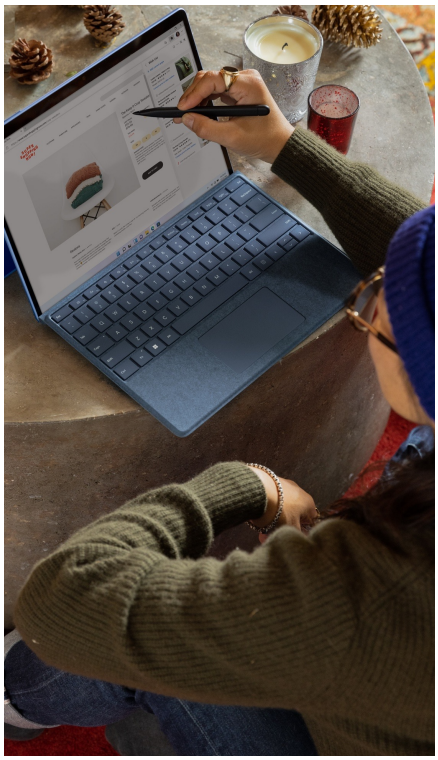
Exercice introductif

Imaginez que l'APD vous annonce sa visite suite à une plainte.

Comment et que préparez-vous?

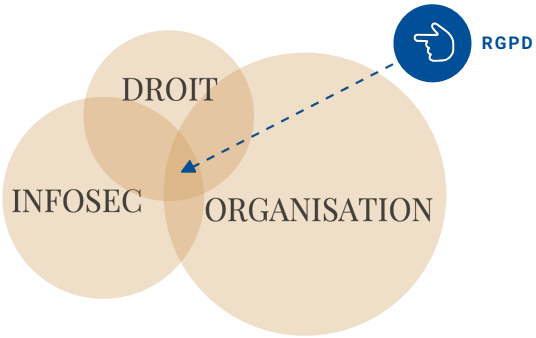
1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre





RGPD = gestion des data !!

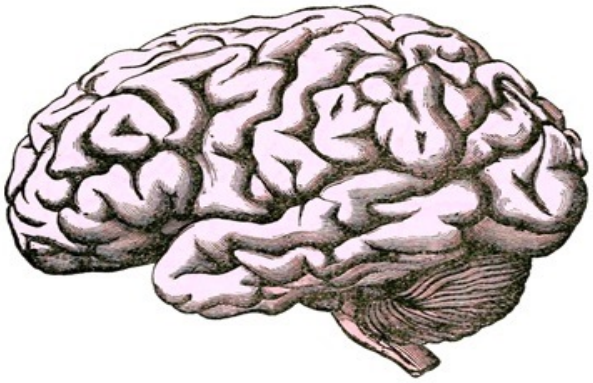
Combinaison de 3 éléments



LE GDPR CA PEUT ETRE POSITIF

MEILLEURE CONNAISSANCE DES PROCESSUS INTERNES

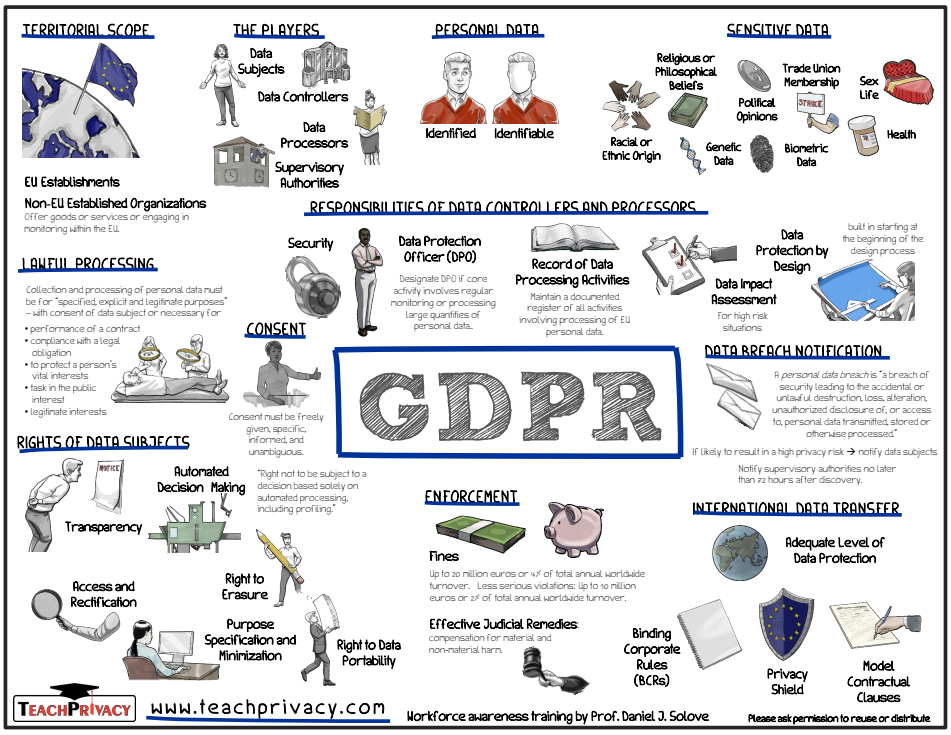
For an organization
to know itself,
it must know about
the data it keeps.



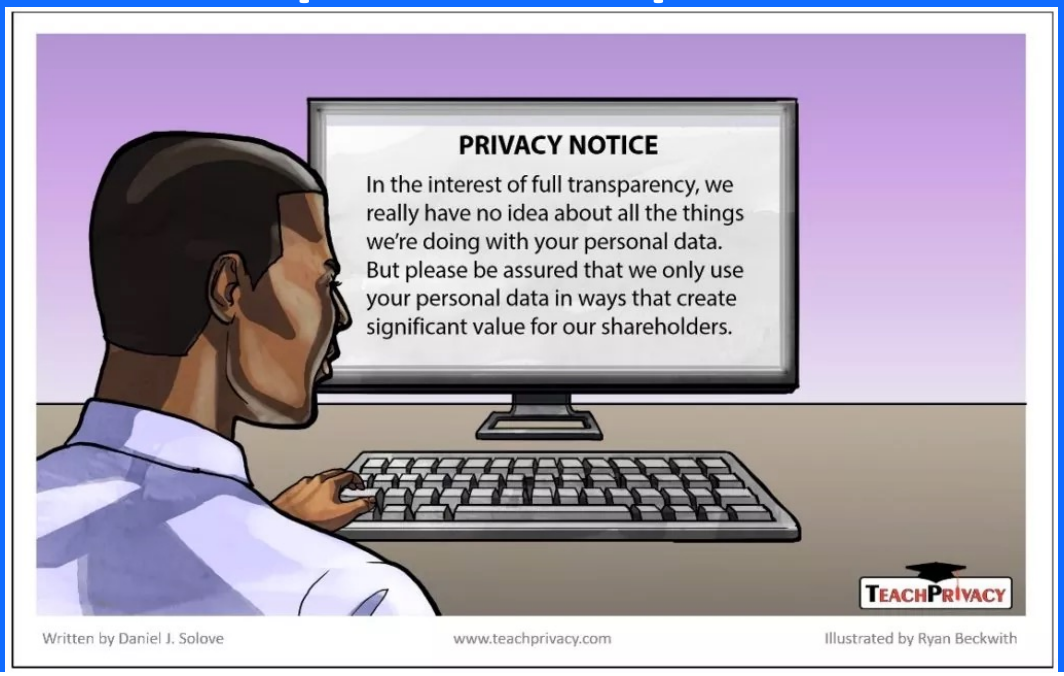
TEACHPRIVACY www.teachprivacy.com

2 DIFFERENT WORLDS ? NOT REALLY THEY ARE NEARLY THE SAME !

Un petit résumé ?



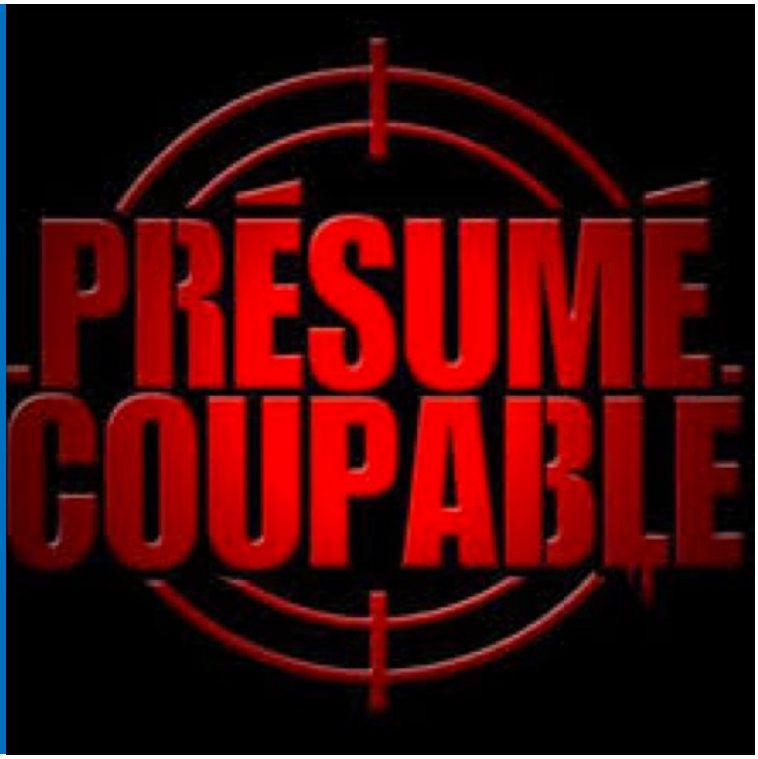
Principe de transparence !



Accountability principle

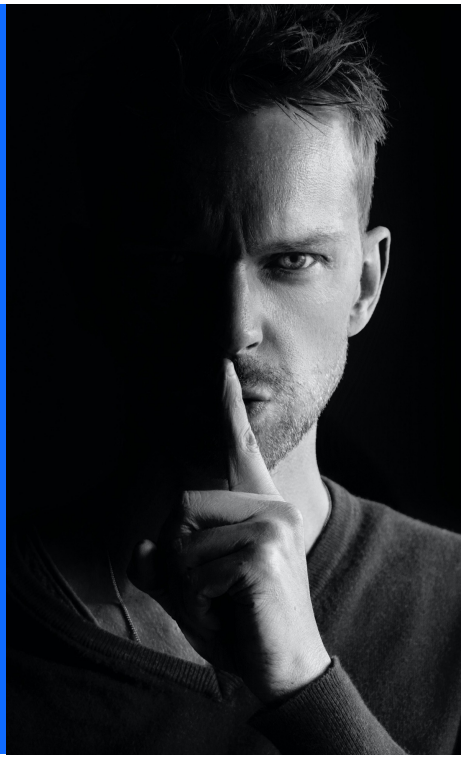
- You must be compliant!
- You must show it !

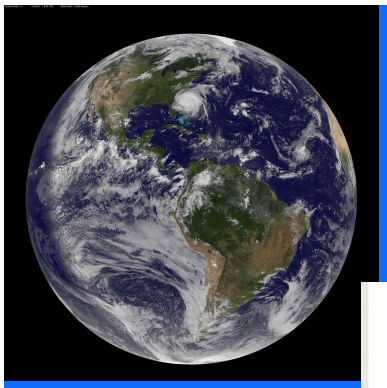
Vous devez être capable de démontrer que vous êtes en règle par rapport au RGPD



Obtenir une certification RGPD ?

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre





Article 3 - Champ d'application territorial

1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

> a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
>
> b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

3. Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.

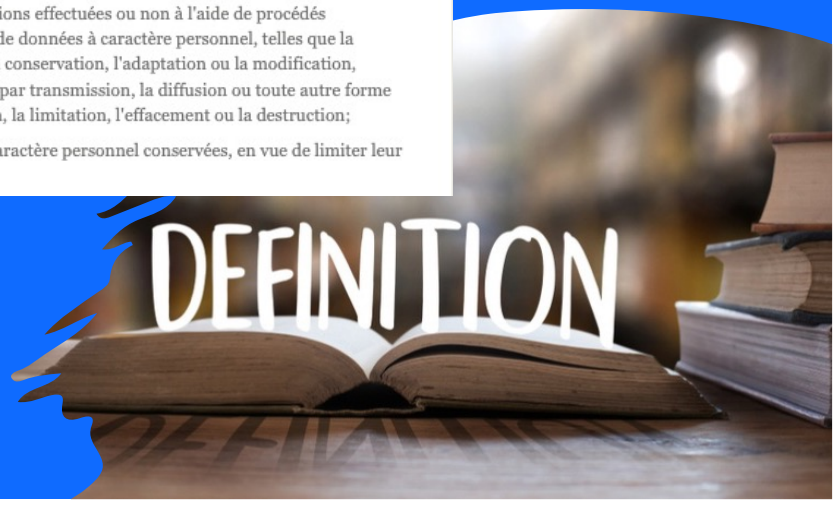
Article 4 - Définitions

Aux fins du présent règlement, on entend par :

1. «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2. «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

3. «limitation du traitement», le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur;



4. «profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

5. «pseudonymisation», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

6. «fichier», tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

7. «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

8. «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

9. «destinataire», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

10. «tiers», une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;

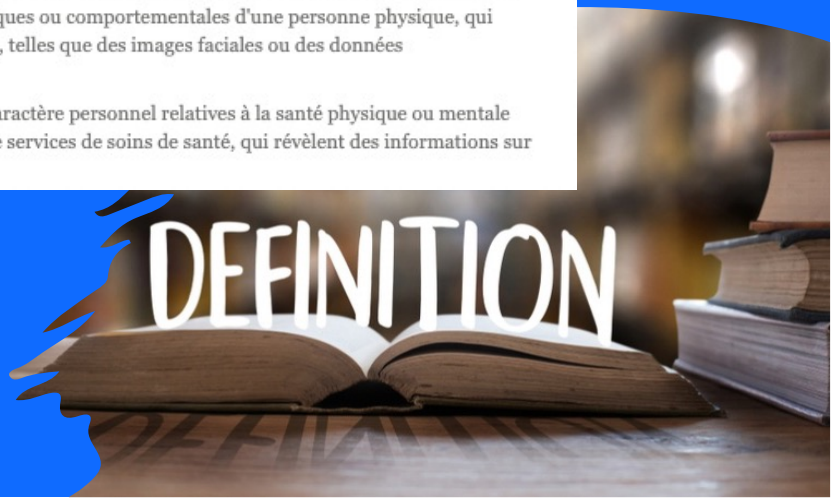
11. «consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

12. «violation de données à caractère personnel», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

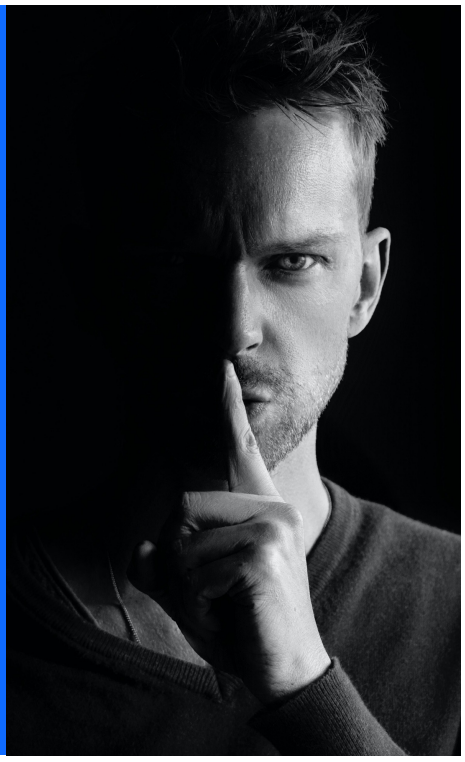
13. «données génétiques», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

14. «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

15. «données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;



1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



le dossier rgpd pour l'accountability

But à atteindre

- Avoir un dossier complet
- Obligation de moyen
- La sécurité de l'information en fait partie
- Et la compliance est comprise dans ISO27002

LE DOSSIER RGPD NE SERA JAMAIS FINI !

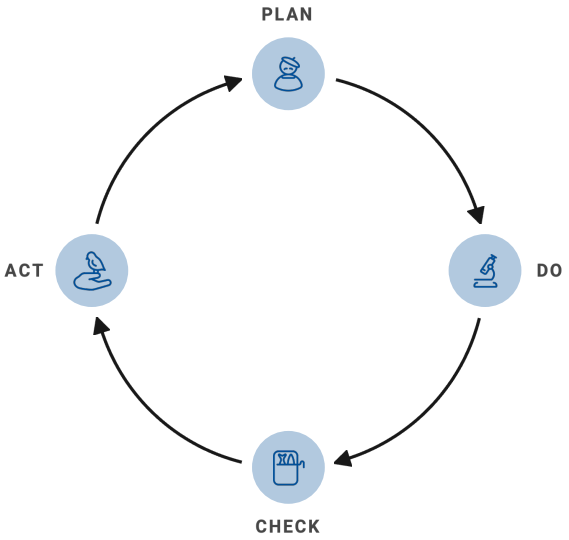
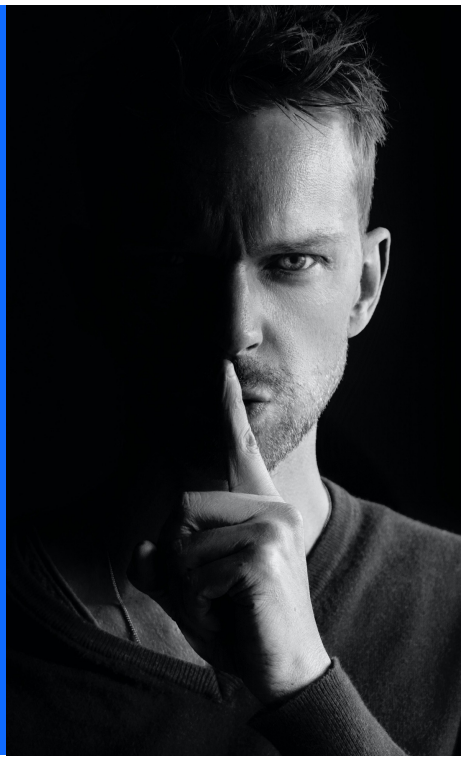


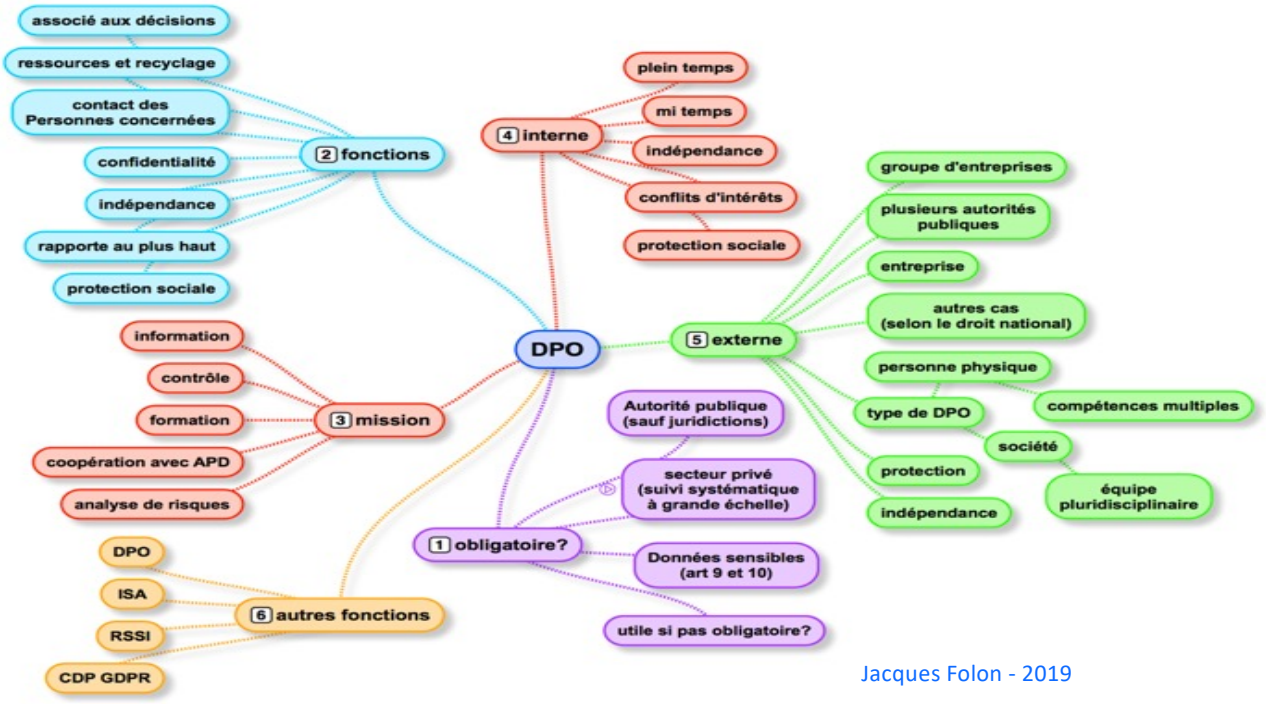
Table des matières

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



A quoi ça sert un DPO ?

DATA PROTECTION OFFICER



Jacques Folon - 2019

Rôles et fonctions

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

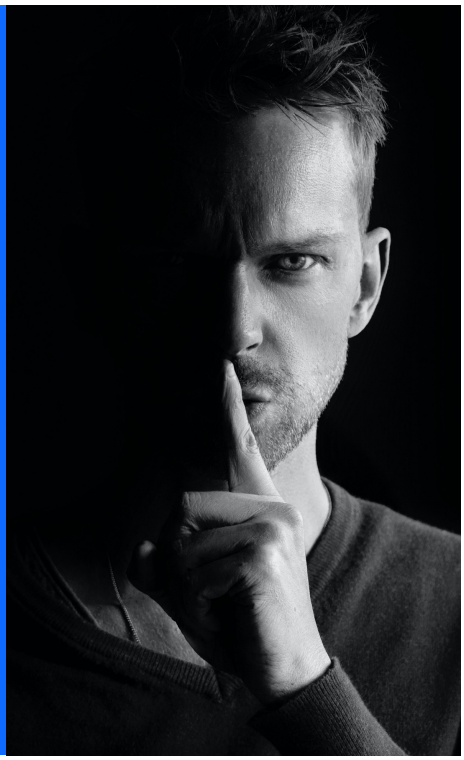
Le DPO a un rôle de conseil et de contrôle du respect du RGPD. Le RGPD comprend les mesures de sécurité techniques et organisationnelles nécessaires pour protéger les données personnelles. Il ne peut participer à des décisions opérationnelles sous peine de conflit d'intérêt avec sa fonction de contrôle	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

- Le DPO ne décide pas !
- QUID DU RSSI?
- Décisions à prendre
- Acter les décisions
- Quid en cas de désaccord?
- Exemples de décisions

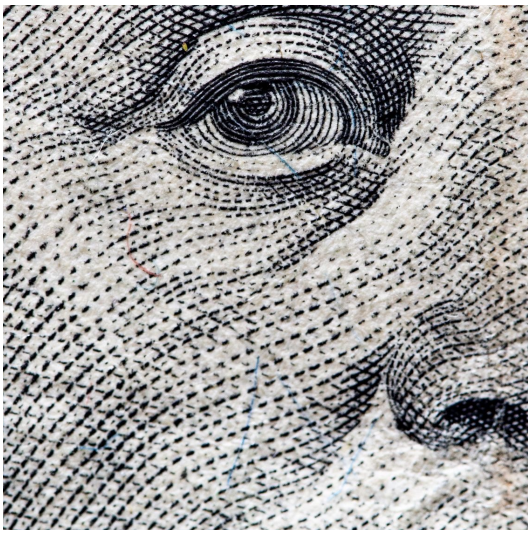
Que met-on dans le dossier ?

- Décision de nomination motivée de la direction
- Ou
- Décision motivée de ne pas avoir de DPO
- Information de l'APD
- Les « avis du DPO »

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



Qui est "responsable de traitements" ?



CE N'EST PAS UNE QUESTION SIMPLE

- Il faut analyser les faits
- Parfois certains se trompent
- ce n'est pas parce c'est dans la loi que c'est vrai

“le responsable de traitement définit les moyens et les finalités du traitement.”

RGPD ART 4,7

“seul ou conjointement avec d'autres”

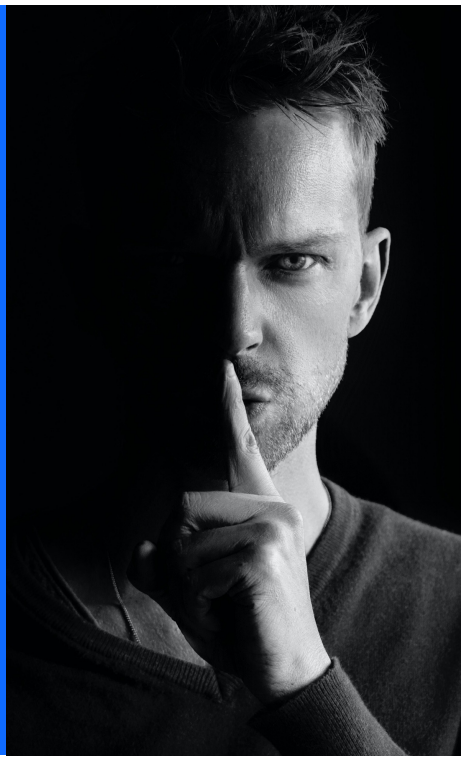
RGDP ART 4,7

“Le responsable des traitements est une personne morale, pas son dirigeant”

“"le service ou le département"”

Que met-on dans le dossier ?

- Décision motivée de la direction



Le sous-traitant

Art 4 "sous-traitant", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

Art. 28,1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Le sous-traitant

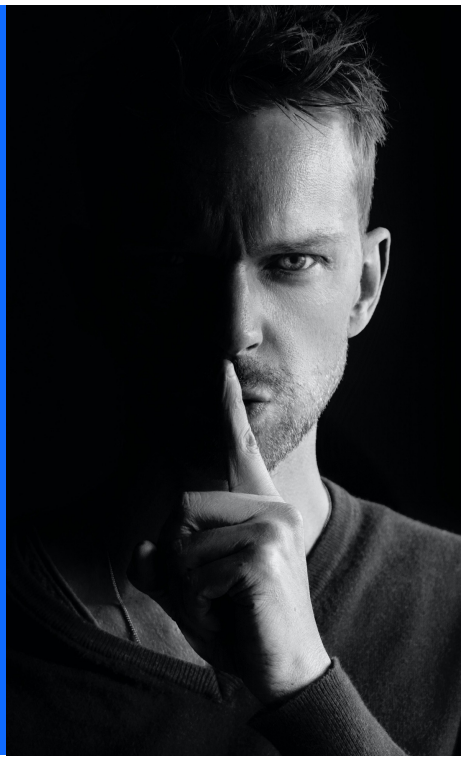
Art 28, 3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

On y reviendra

Que met-on dans le dossier ?

- Tous les contrats de ST
- Les Data Processing Agreements des grandes entreprises
- Les analyses si les St sont américains

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



Site internet

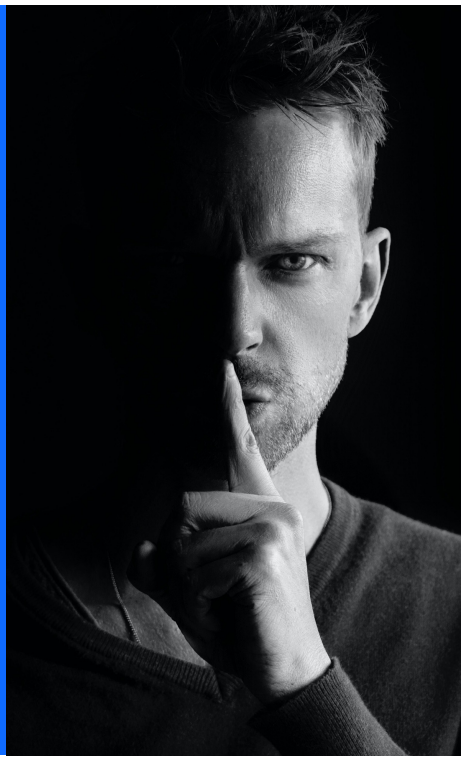
le site internet est très visible…

- Double opt-in
- Conservation des accords (contrat, consentement)
- Cookies
- Marketing digital
- Google analytics
- Durée de conservation
- Privacy policies (plusieurs finalités)
- Collaboration DPO – ICT – RSSI-marketing

Que met-on dans le dossier ?

- Les privacy policies
- Les procédures de collecte
- les preuves de conservation
- Les cookies policies

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



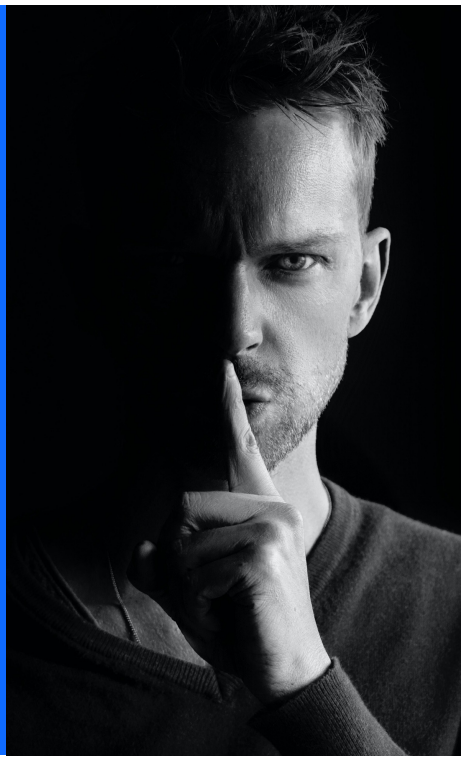
toutes les bases de données...

- Données sensibles
- RH
- Secrets d'affaires
- Identifier les départements à risques
- On commence par sécuriser les worst case
- Procédure en cas de vol/perte
- Shadow IT !
- Journalisation
- Back-ups
- Préparer réponse au droit d'accès

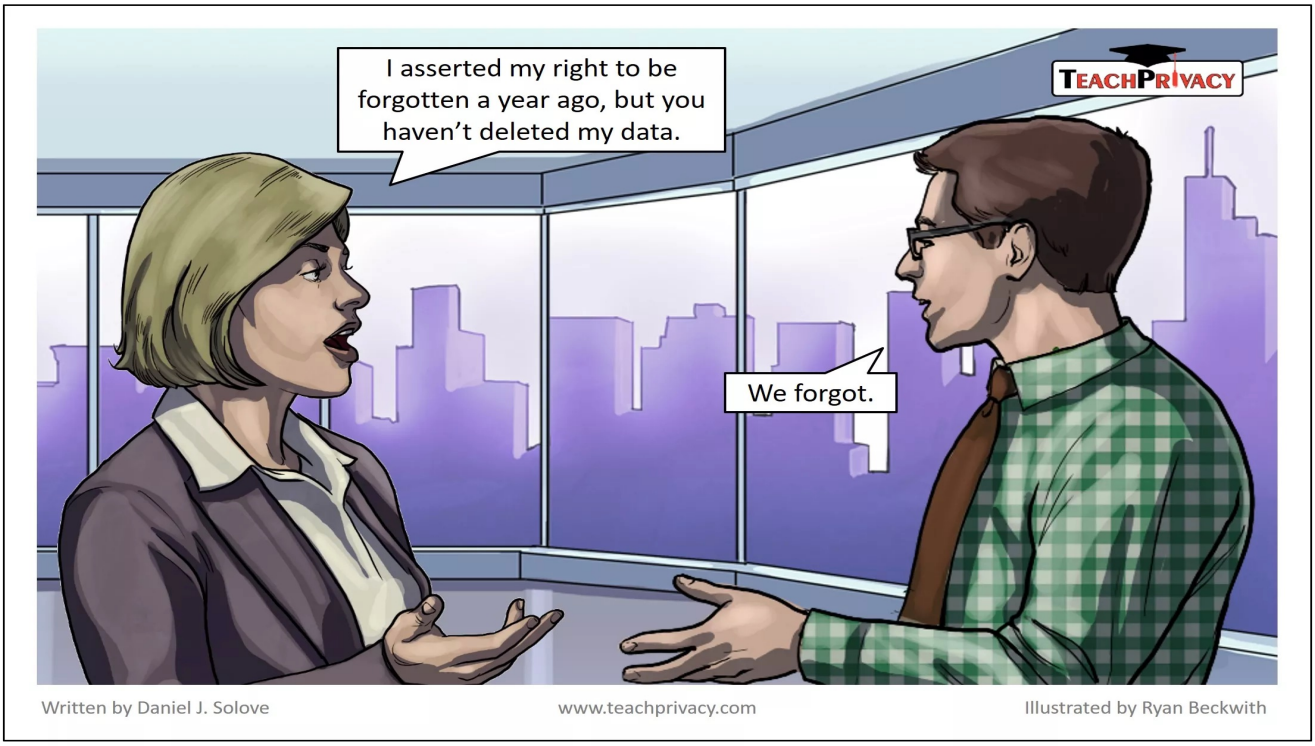
Que met-on dans le dossier ?

- L'inventaire des DB
- Les data contenues
- L'identité des responsables opérationnels

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



☑TRANSPARENCE
☑INFORMATIONS LORS DE LA COLLECTE
☑DROIT D'ACCES
☑DROIT DE RECTIFICATION
☑DROIT A L'EFFACEMENT
☑DROIT A LA LIMITATION DU TRAITEMENT
☑PORTABILITE
☑DROIT D'OPPOSITION AU PROFILAGE

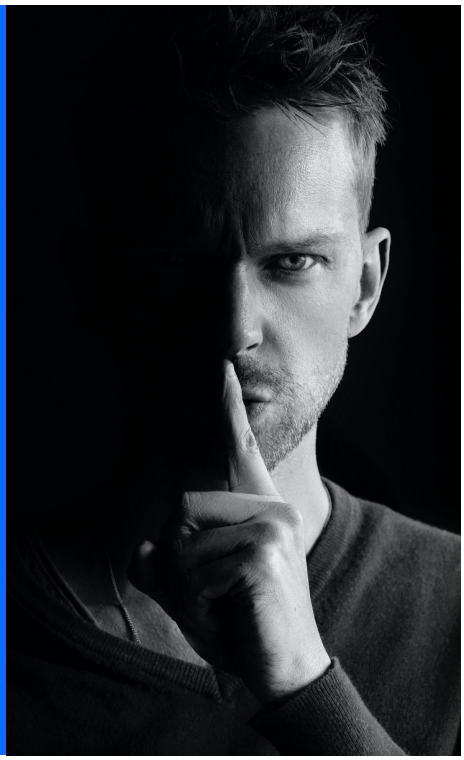

I asserted my right to be forgotten a year ago, but you haven't deleted my data.
We forgot.
TEACHPRIVACY
Written by Daniel J. Solove
www.teachprivacy.com
Illustrated by Ryan Beckwith


• EXERCICE
• Imaginez une demande
• Que fait-on ?
• Qui contacter?
• Comment répondre?
• Qui répond?
• Est-on certain de répondre en un mois?

Que met-on dans le dossier ?

- La procédure
- Les demandes et réponses

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



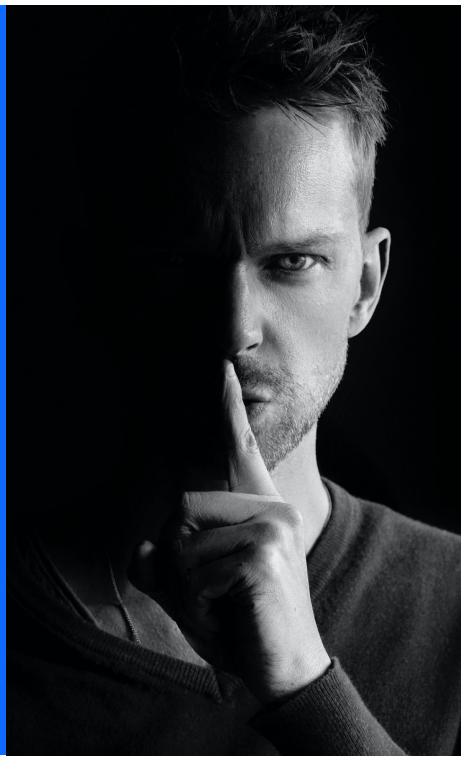
Les mesures de sécurité techniques et organisationnelles

- **Certification?**
- **Plan de sécurité?**
- **Analyse de risques**
- **Il faut une référence**
- **Voir DPIA CNIL**
- **Déclaration vs. Réalité**
- **IAM ?**

Que met-on dans le dossier ?

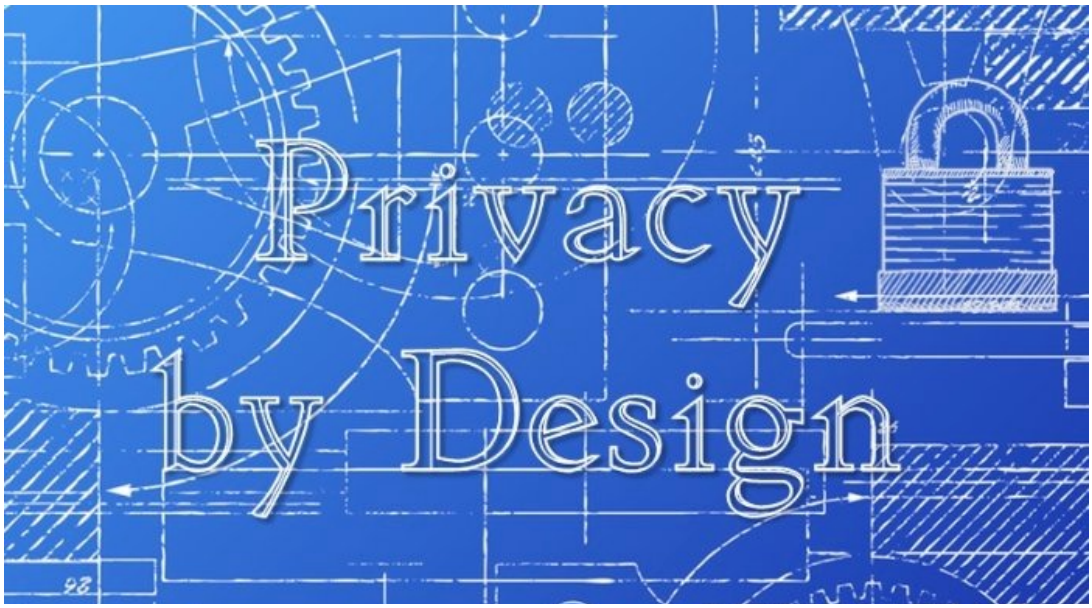
- Le plan de sécurité
- Les mesures de sécurité
- Les éventuelles certifications ISO ou autres

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



General Data Protection Regulation

PRIVACY BY DESIGN MEANS
THINK PRIVACY FIRST !

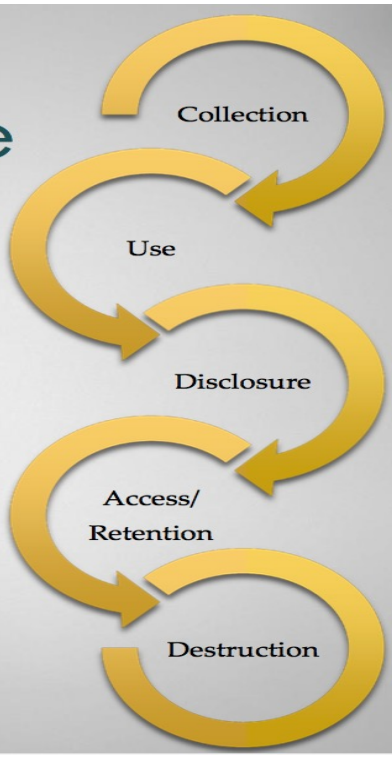


- **Privacy by design?**
- **Il faut documenter !**
- **Comment faire?**
- **Comment le démontrer?**
- **Comment convaincre les développeurs?**

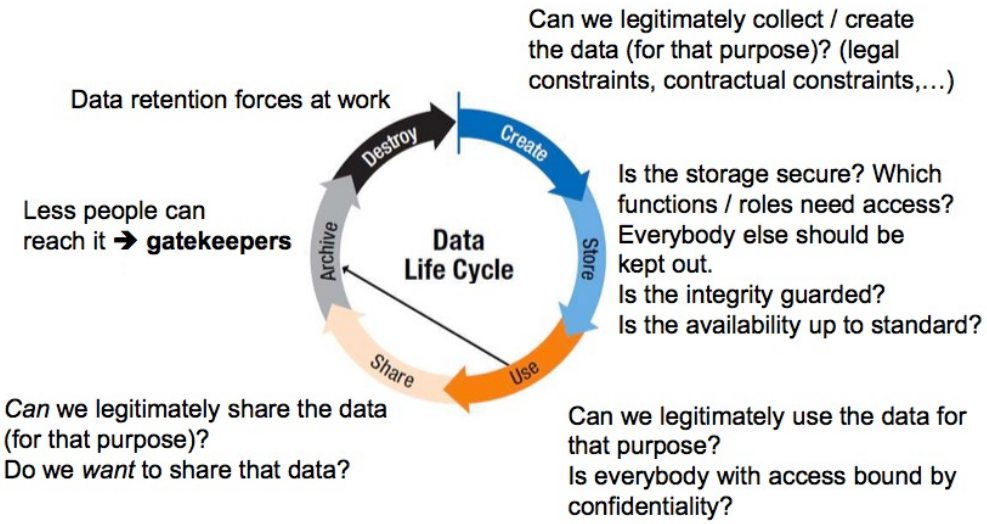
DATA QUALITY IS ESSENTIAL

Core Principles: Information Lifecycle

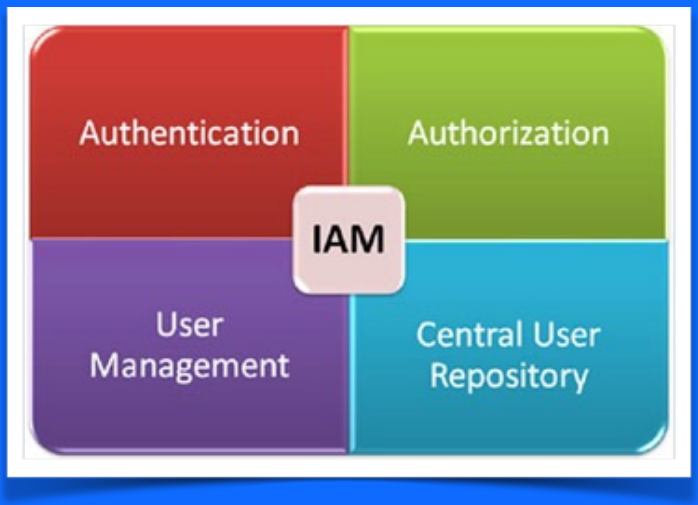
Privacy by Design requires contemplating each phase of the information lifecycle



Look at the entire data lifecycle



Identity Access Management (GESTION DES ACCÈS)



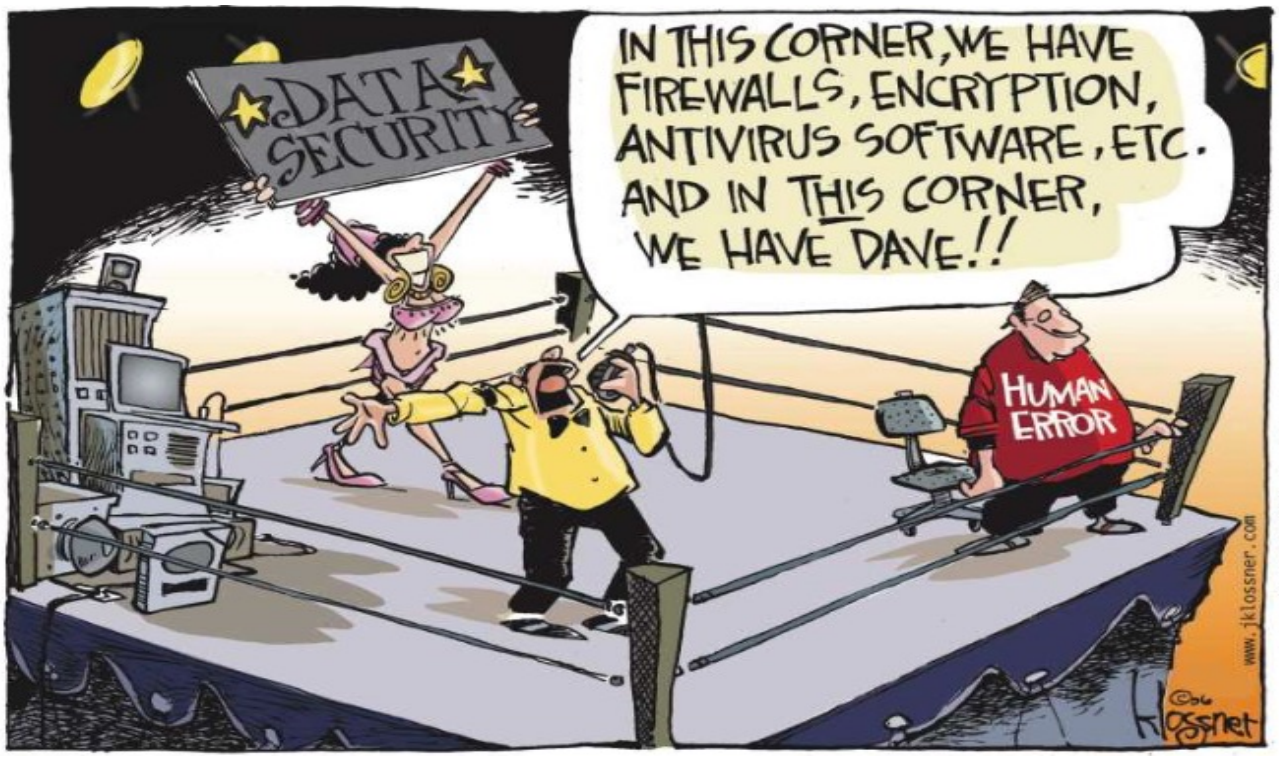
GDPRfolder

Quelles sont les questions à se poser??

- Les personnes sont-elles ce qu'elles disent être??
- Sont-elles des membres réels de notre communauté ?
- Ont-elles reçu les autorisations nécessaires ?
- Le respect de leurs données personnelles est-il mis en place?

Exemples de questions

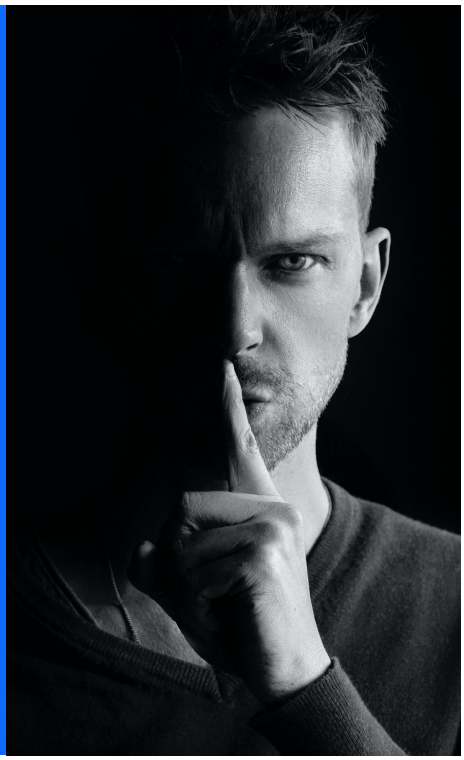
- Quel mot type de mot de passe donner?
- Quelles sont les activités autorisées?
- Quelles sont les activités interdites?
- A quelle catégorie de personne cette nouvelle identité doit-elle être attachée?
- A quel moment du processus d'entrée les autorisations doivent-elles être données?
- Quelles modalités de contrôle sont mises en place?
- Peut-on prouver tout cela à un auditeur ?
- Quid de l'e-discovery?

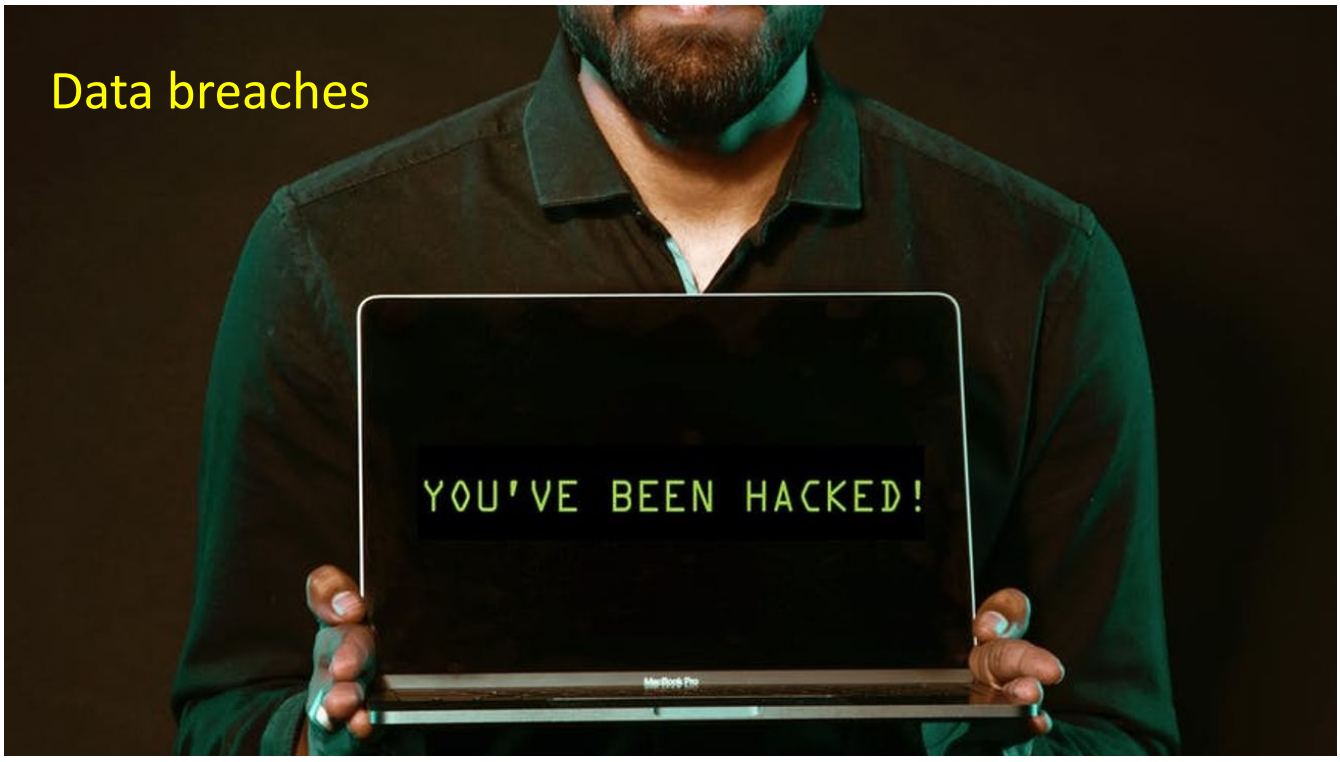


Que met-on dans le dossier ?

- La documentation
- L'avis du DPO

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre

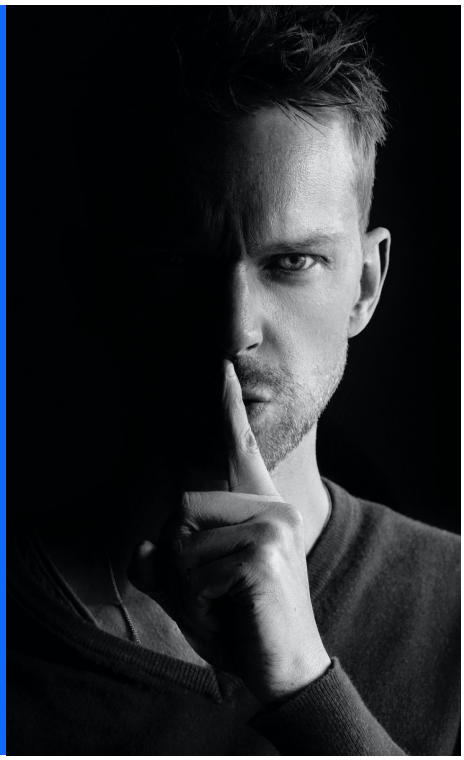


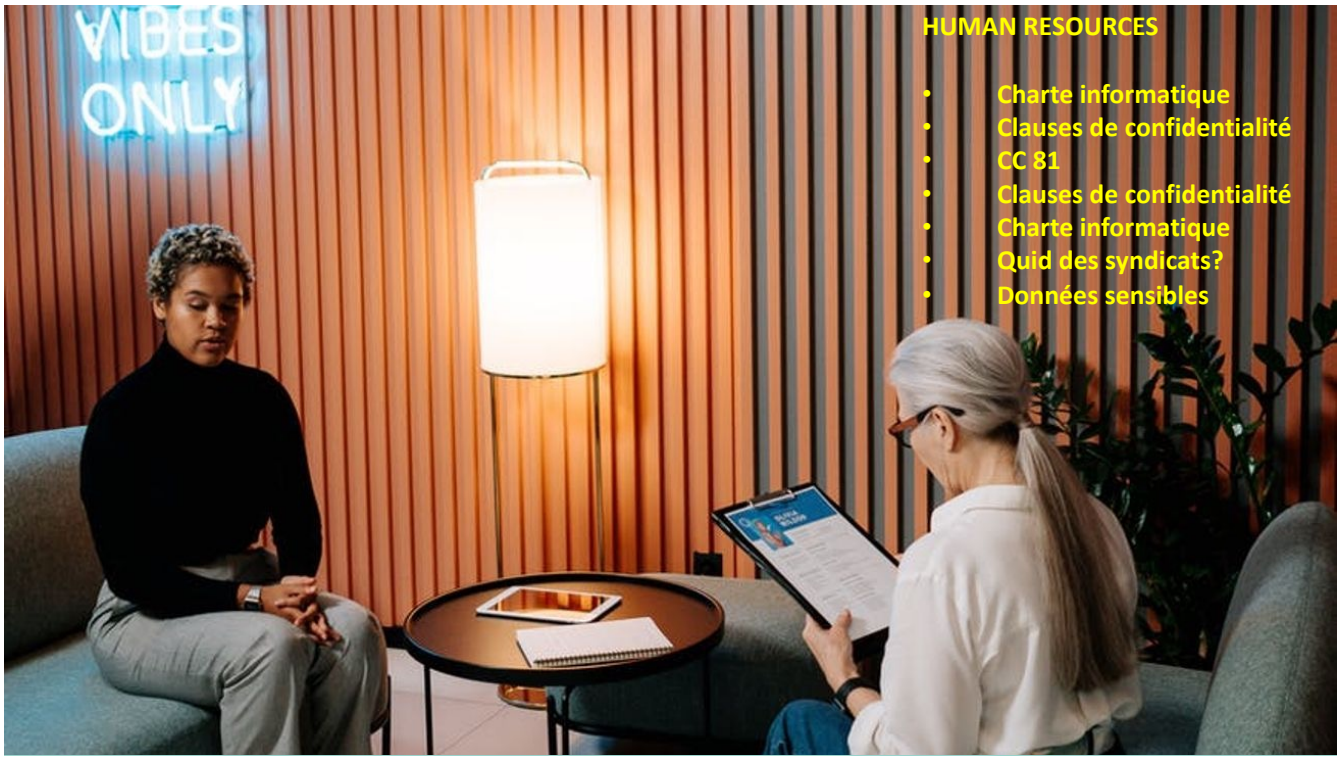


Que met-on dans le dossier ?

- La procédure
- le registre des incidents
- l'avis du DPO
- les décisions de la direction
  - Rien
  - APD
  - Personnes concernées
- Les mesures correctives

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre





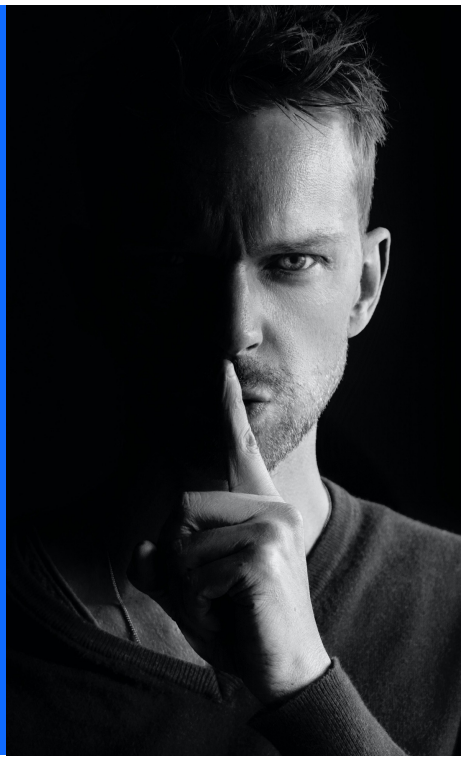
HUMAN RESOURCES

- Charte informatique
- Clauses de confidentialité
- CC 81
- Clauses de confidentialité
- Charte informatique
- Quid des syndicats?
- Données sensibles

Que met-on dans le dossier ?

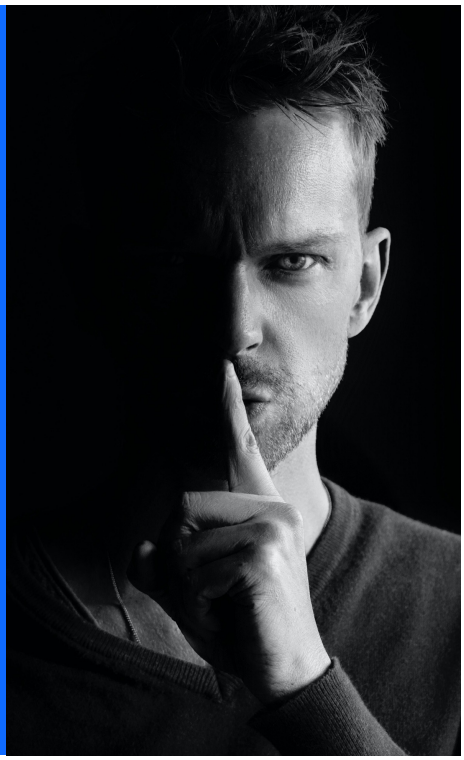
- Toutes les procédures
- La preuve des information
- La preuve de la distribution des procédures
- La preuve des formations

1. **Introduction**
2. **Quelques définitions**
3. **Le but: le dossier GDPR**
4. **DPO or not DPO?**
5. **Le responsable de traitement**
6. **Le sous-traitant**
7. **Le site Internet**
8. **Les DB existantes**
9. **Les droits des personnes**
10. **Les mesures de sécurité tech. et orga.**
11. **Privacy by design**
12. **Data breaches**
13. **Les RH**
14. **Les DPIA**
15. **Le registre**



- Outil de la CNIL
- Comment faire?
- Qui autour de la table?
- On commence par quoi?
- Actualisation?

1. Introduction
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les RH
14. Les DPIA
15. Le registre



Pour chaque traitement de données personnelles, posez-vous les questions suivantes :

QUI ?

- Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ;
- Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme ;
- Etablissez la liste des sous-traitants.

QUOI ?

- Identifiez les catégories de données traitées
- Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé ou les infractions)

POURQUOI ?

- Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données (exemple : gestion de la relation commerciale, gestion RH...).

OÙ ?

- Déterminez le lieu où les données sont hébergées.
- Indiquez quels pays les données sont éventuellement transférées.

JUSQU'À QUAND ?

- Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

COMMENT ?

- Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

GDPRfolder

- Quel format choisir?
- Comment faire?
- Anticiper les simultanéités
- Log de non-conformité
- Méthode de classement
- Il faut retrouver les preuves!

PRINCIPALE TÂCHE DO-CU-MEN-TA-TION

If you didn't
document
you didn't
do it.

COMMENT DÉMONTRER QU'ON EST EN RÈGLE? COMMENT RASSURER SES CLIENTS

Mises à jour permanentes

Le GDPR n'en finit pas d'évoluer !

JUST DO IT

GDPRfolder