

# 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 2115  
 www.folon.com

- **Quels sont les constats depuis l'entrée en vigueur du RGPD il y a 5 ans ?**
- **-Comment la réglementation actuelle sur la protection des données protège elle les individus ?**
- **-Comment la collecte, l'utilisation et le partage des données évoluent-ils dans notre société ?**
- **-Les problèmes posés par ChatGPT et les nouvelles AI**
- **-Quels sont les risques et les défis en 2023 liés à la protection des données ?**



CONSTATS  
APRES 5ANS



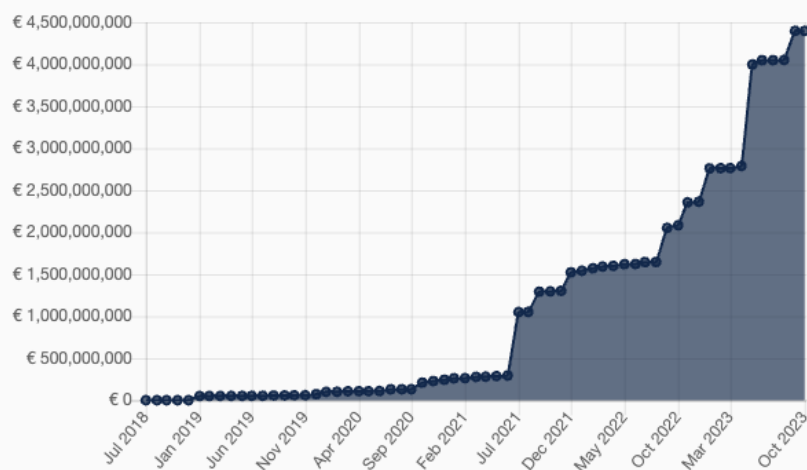
**1998 - 2013**  
**5 ANS DE RGPD**  
**PETIT RAPPEL**



# LES AMENDES QUI FONT PEUR !



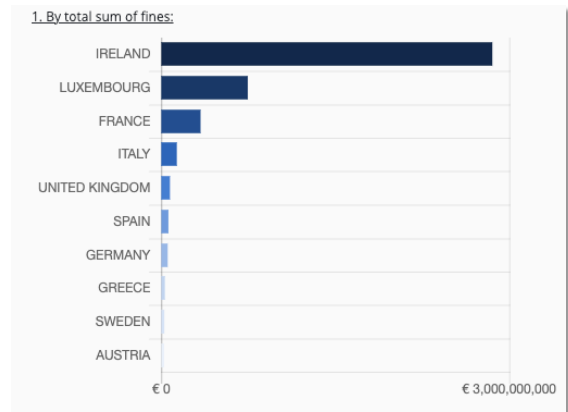
a) Course of overall sum of fines (cumulative):



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

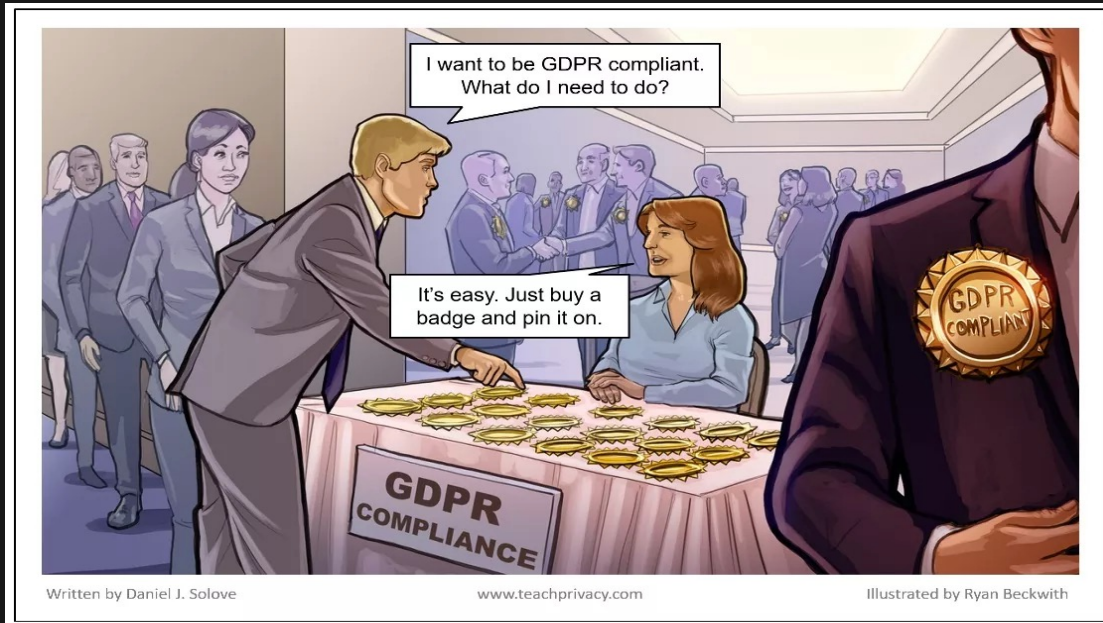
GDPR Enforcement Tracker - list of GDPR fines

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)

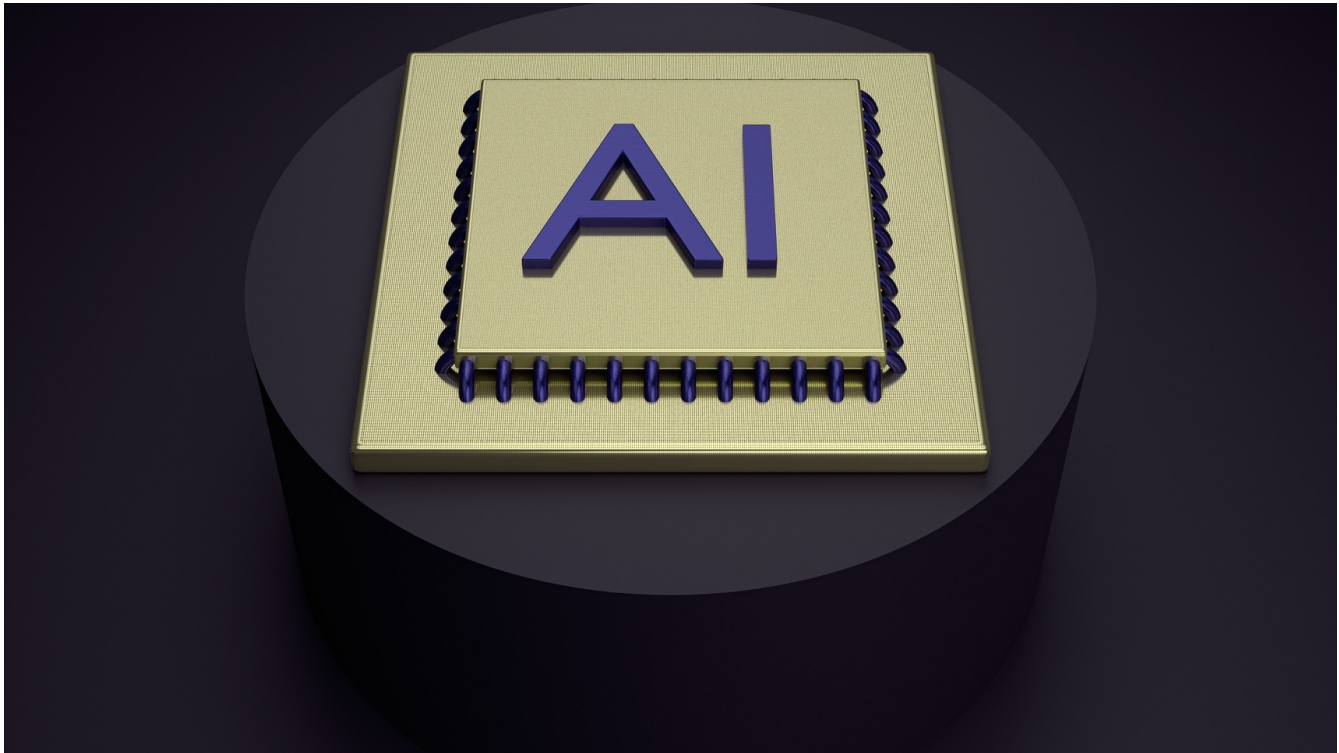
## MANQUE DE CERTIFICATIONS



## UN PEU COMPLEXE POUR DES STARTUPS OU DES PME ?









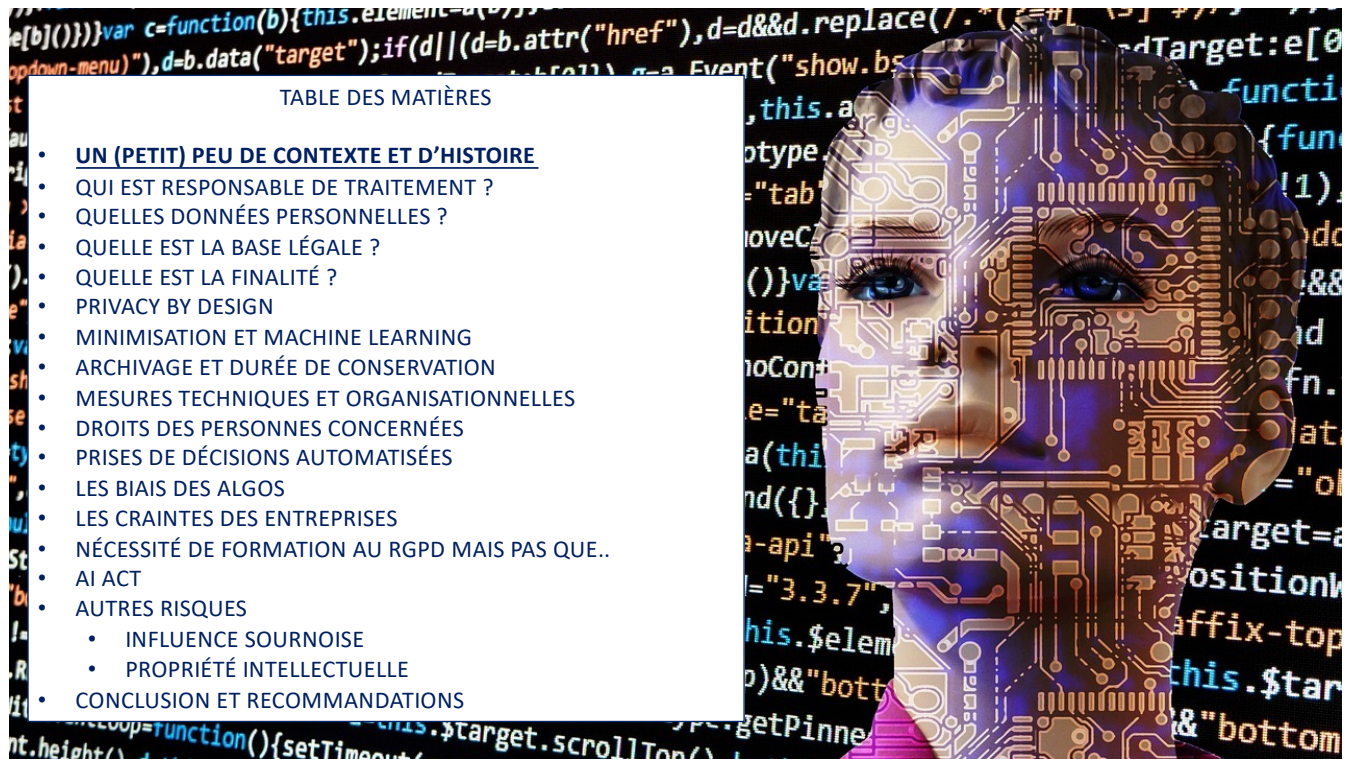
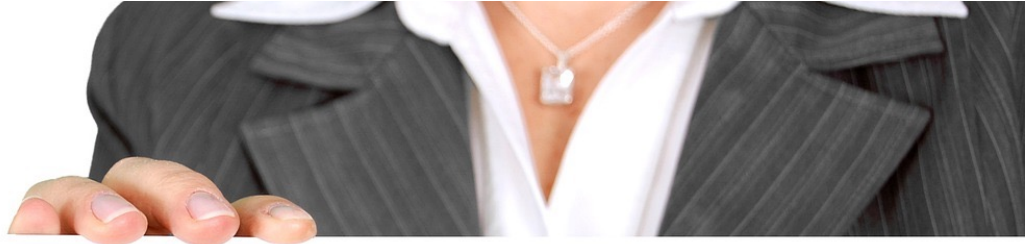


TABLE DES MATIÈRES

- **UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE**
- QUI EST RESPONSABLE DE TRAITEMENT ?
- QUELLES DONNÉES PERSONNELLES ?
- QUELLE EST LA BASE LÉGALE ?
- QUELLE EST LA FINALITÉ ?
- PRIVACY BY DESIGN
- MINIMISATION ET MACHINE LEARNING
- ARCHIVAGE ET DURÉE DE CONSERVATION
- MESURES TECHNIQUES ET ORGANISATIONNELLES
- DROITS DES PERSONNES CONCERNÉES
- PRISES DE DÉCISIONS AUTOMATISÉES
- LES BIAIS DES ALGOS
- LES CRAINTES DES ENTREPRISES
- NÉCESSITÉ DE FORMATION AU RGPD MAIS PAS QUE..
- AI ACT
- AUTRES RISQUES
  - INFLUENCE SOURNOISE
  - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

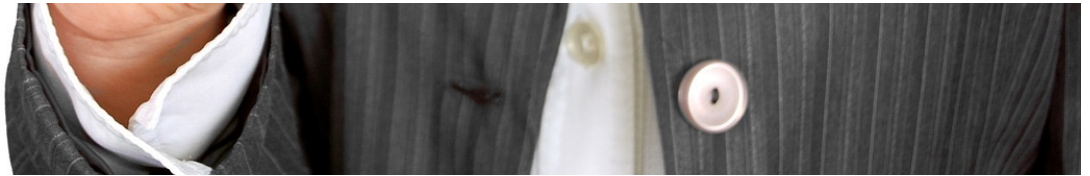


**EU-U.S.**  
**★ Data Privacy Framework**



# QUALITY CONTROL

## DPO AUTO-CERTIFIES



### CATEGORIES OF PERSONAL INFORMATION

The following are categories of information relating to an individual, whether it relates to their private, professional or public life. Categories are not exclusive. Data may transcend multiple information categories.

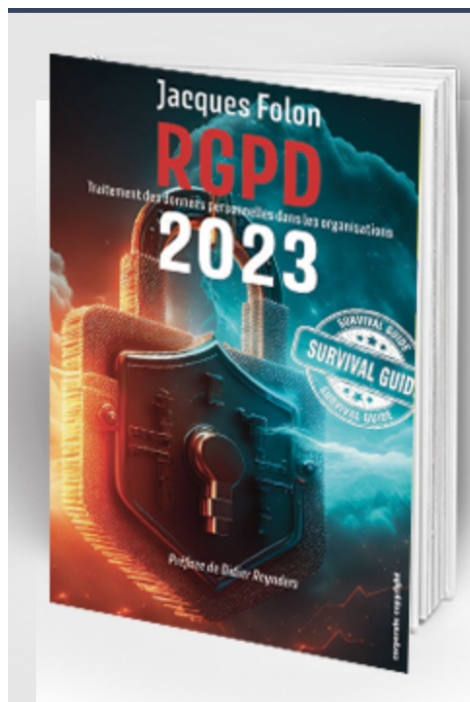
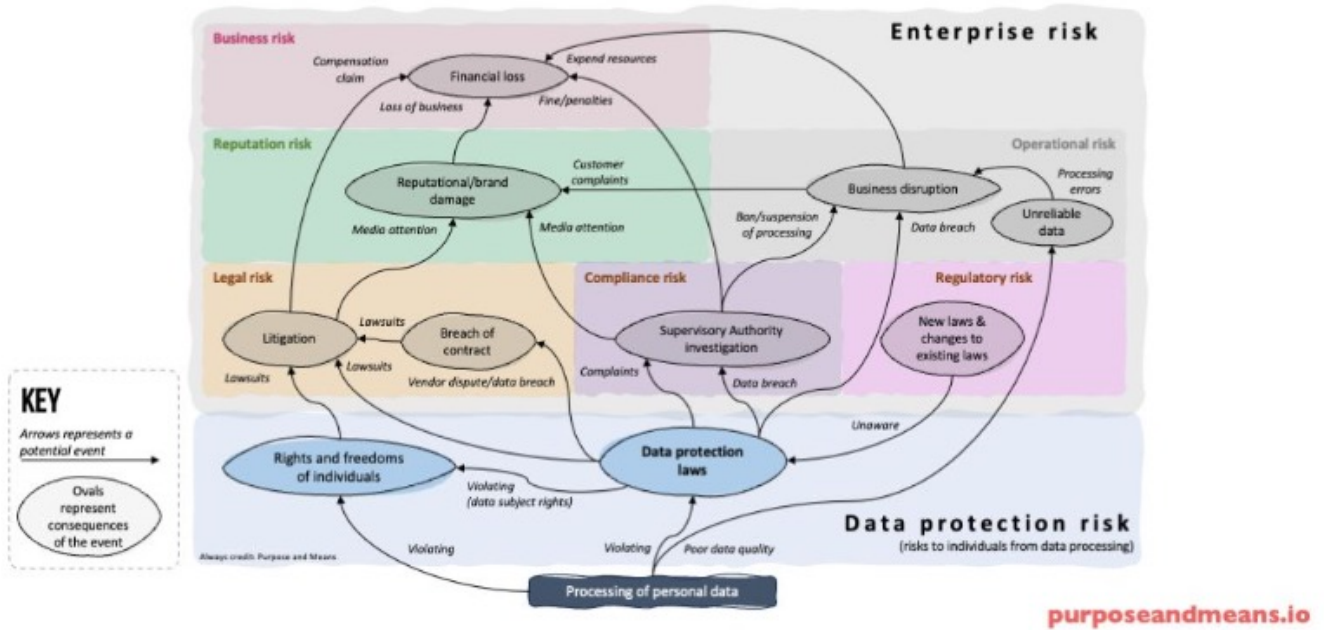
- INTERNAL**
  - KNOWLEDGE & BELIEF** **[SENSITIVE]** Information about what a person knows or believes, i.e. religious beliefs, philosophical beliefs, thoughts and things known and don't know, what someone thinks.
  - AUTHENTICATING** Information used to authenticate an individual with something they know, i.e. Passwords, PIN, mobile device passcodes.
  - PREFERENCE** Information about an individual's preference or interests, i.e. Opinions, interests, preferences.
- EXTERNAL**
  - IDENTIFYING** Information that uniquely or semi-uniquely identifies a specific individual, i.e. Name, username, unique identifier, government-issued identification number, biometric data.
  - ETHNICITY** **[SENSITIVE]** Information that describes an individual's origins and lineage, i.e. Race, national or ethnic origin, language spoken, accents.
  - SEXUAL** **[SENSITIVE]** Information that describes an individual's sexual life, i.e. Gender identity, preferences, practices, fetishes, history, etc.
  - BEHAVIORAL** Information that describes an individual's behavior or activity, online or off, i.e. Browsing history, search history, email, domain, attitude.
  - DEMOGRAPHIC** Information that describes an individual's characteristics shared with others, i.e. Age ranges, physical traits, income brackets, geographic.
  - MEDICAL AND HEALTH** **[SENSITIVE]** Information that describes an individual's health, medical conditions or health care, i.e. Physical and mental health, diagnosis, health conditions, family or individual health history, health records, blood type, DNA code, prescriptions.
  - PHYSICAL CHARACTERISTIC** Information that describes an individual's physical appearance, i.e. Height, weight, eye, hair color, skin tone, tattoos, gender, piercings.
- HISTORICAL**
  - HISTORY** Information about an individual's personal history, i.e. Events that happened in a person's life, when they were or just around from which might have influenced them (DNA, etc.).
- FINANCIAL**
  - ACCOUNT** **[SENSITIVE]** Information that identifies an individual's financial account, i.e. Credit card number, bank account.
  - OWNERSHIP** Information about things an individual has owned, rented, borrowed, or possessed, i.e. Cars, houses, sport items, personal possessions.
  - TRANSACTIONAL** Information about an individual's purchasing, spending or income, i.e. Purchases, sales, credit, income, bank records, transactions, bank purchases, and spending habits.
  - CREDIT** Information about an individual's reputation with regards to money, i.e. Credit records, underworkbooks, credit standing, credit capacity.
- SOCIAL**
  - PROFESSIONAL** Information about an individual's educational or professional career, i.e. Job titles, salary, work history, school attendance, employee files, employment history, evaluations, references, interviews, qualifications, regulatory actions.
  - CRIMINAL** **[SENSITIVE]** Information about an individual's criminal activity, i.e. Convictions, charges, pardons.
  - PUBLIC LIFE** **[SENSITIVE]** Information about an individual's public life, i.e. Character, general reputation, social status, marital status, religion, political affiliation, memberships, communicative activity.
  - FAMILY** Information about an individual's family and relationships, i.e. Family structure, siblings, offspring, marital, domestic partnerships.
  - SOCIAL NETWORK** Information about an individual's friends or social connections, i.e. Friends, connections, organizations, associates, group membership.
  - COMMUNICATION** **[SENSITIVE]** Information communicated from or to an individual, i.e. Telephone recordings, received, email.
- TRACKING**
- COMPUTER DEVICE** **[SENSITIVE]** Information about a device that an individual uses for personal use (even part-time or with others), i.e. IP address, Mac address, browser fingerprint.
- CONTACT** Information that provides a mechanism for contacting an individual, i.e. Email address, physical address, telephone number.
- LOCATION** **[SENSITIVE]** Information about an individual's location, i.e. Country, GPS coordinates, room number.

**[SENSITIVE]** label denotes categories of personal data that are more likely to be used by a third actor or where such use may be more impactful to a person. Many of these categories are designated as higher risk in laws and regulations, worldwide.

Version 7 (2023) <https://privacybydesign.training> **PRIVACY BY DESIGN**



# LINKING DATA PROTECTION RISK TO ENTERPRISE RISK



## LE RÔLE DU DPO DANS LE SECTEUR PUBLIC

Manuel pratique et retours d'expériences

Sous la coordination de Jacques Folon

- Florence Baumel
- Christophe Bierlaire
- Laetitia Di Cristofaro
- Jacques Folon
- Julie Godfrois
- Dominique Grégoire
- Frédérique Mathybe
- Loris Nicoletti

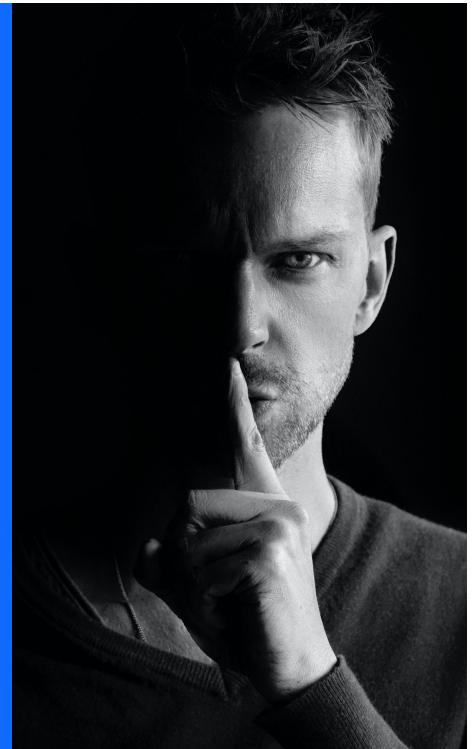


# Exercice introductif



Imaginez que l'APD vous annonce sa  
visite suite à une plainte.  
Comment et que préparez-vous?

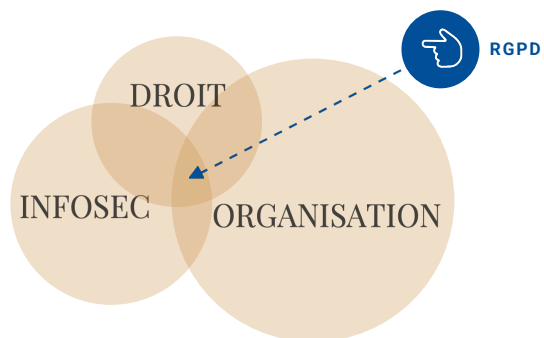
1. **Introduction**
2. Quelques définitions
3. Le but: le dossier GDPR
4. DPO or not DPO?
5. Le responsable de traitement
6. Le sous-traitant
7. Le site Internet
8. Les DB existantes
9. Les droits des personnes
10. Les mesures de sécurité tech. et orga.
11. Privacy by design
12. Data breaches
13. Les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





# RGPD = gestion des data !!

Combinaison de 3 éléments

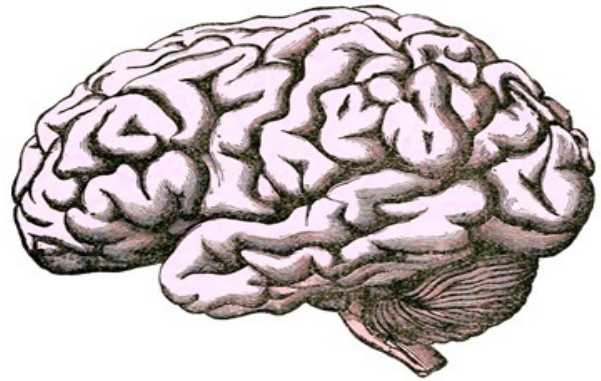


**LE GDPR CA PEUT ETRE POSITIF**

**MEILLEURE CONNAISSANCE DES PROCESSUS INTERNES**



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



[www.teachprivacy.com](http://www.teachprivacy.com)

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



# Un petit résumé ?

**TERRITORIAL SCOPE**  
EU Establishments  
Non-EU Established Organizations  
Offer goods or services or engaging in monitoring within the EU.

**THE PLAYERS**  
Data Subjects  
Data Controllers  
Data Processors  
Supervisory Authorities

**PERSONAL DATA**  
Identified  
Identifiable

**SENSITIVE DATA**  
Religious or Philosophical Beliefs  
Racial or Ethnic Origin  
Political Opinions  
Genetic Data  
Trade Union Membership  
Sex Life  
Health  
Biometric Data

**RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS**  
Security  
Data Protection Officer (DPO)  
Record of Data Processing Activities  
Data Protection by Design  
Data Impact Assessment

**LAWFUL PROCESSING**  
Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for:  
• performance of a contract  
• compliance with a legal obligation  
• to protect a person's vital interests  
• task in the public interest  
• legitimate interests

**CONSENT**  
Consent must be freely given, specific, informed, and unambiguous.

**RIGHTS OF DATA SUBJECTS**  
Transparency  
Automated Decision Making  
Access and Rectification  
Right to Erasure  
Purpose Specification and Minimization  
Right to Data Portability

**ENFORCEMENT**  
Fines  
Effective Judicial Remedies

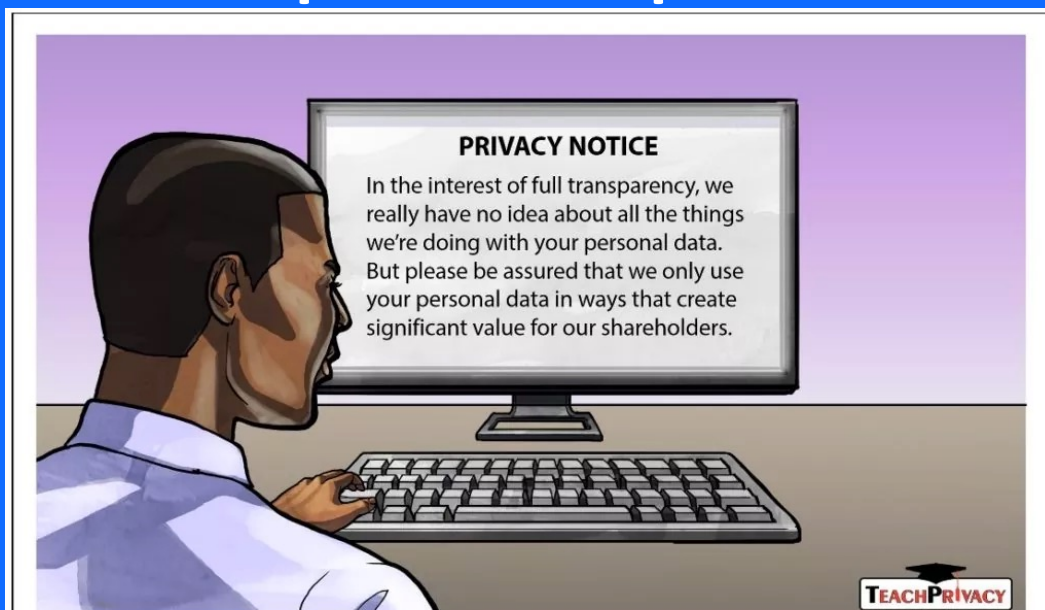
**INTERNATIONAL DATA TRANSFER**  
Adequate Level of Data Protection  
Binding Corporate Rules (BCRs)  
Privacy Shield  
Model Contractual Clauses

**DATA BREACH NOTIFICATION**  
A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."  
If likely to result in a high privacy risk → notify data subjects  
Notify supervisory authorities no later than 72 hours after discovery.

**GDPR**

TEACHPRIVACY [www.teachprivacy.com](http://www.teachprivacy.com) Workforce awareness training by Prof. Daniel J. Solove Please ask permission to reuse or distribute

# Principe de transparence !



Written by Daniel J. Solove

[www.teachprivacy.com](http://www.teachprivacy.com)

Illustrated by Ryan Beckwith



# 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

**PRÉSUMÉ  
COUPABLE**



## Obtenir une certification RGPD ?



## AUDIT AND CERTIFICATION IN DATA PROTECTION

Europrivacy™ to assess, document, certify, and value compliance with the European General Data Protection Regulation (GDPR).

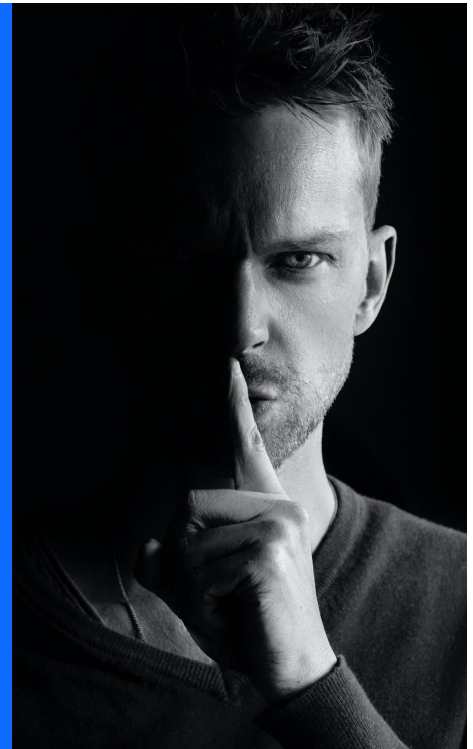
[LEARN MORE](#)

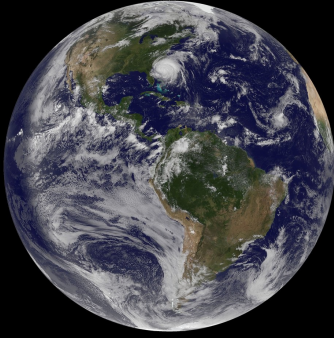
[CONTACT US](#)



GDPRfolder

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;

DEFINITION

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;



# DEFINITION

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;



# DEFINITION

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;

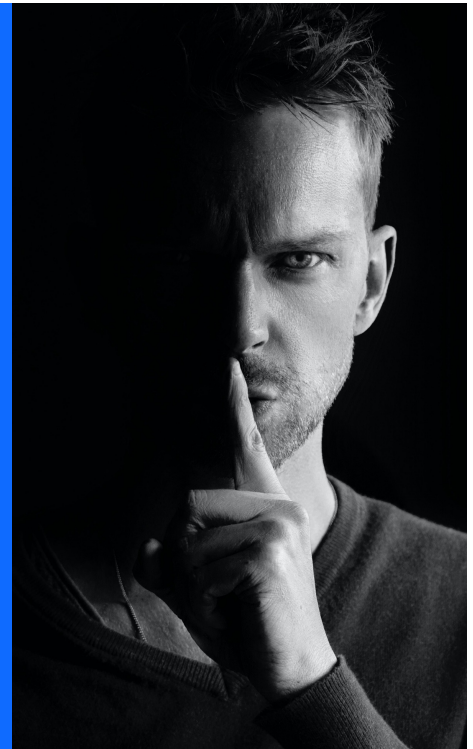
13. «données génétiques», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un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

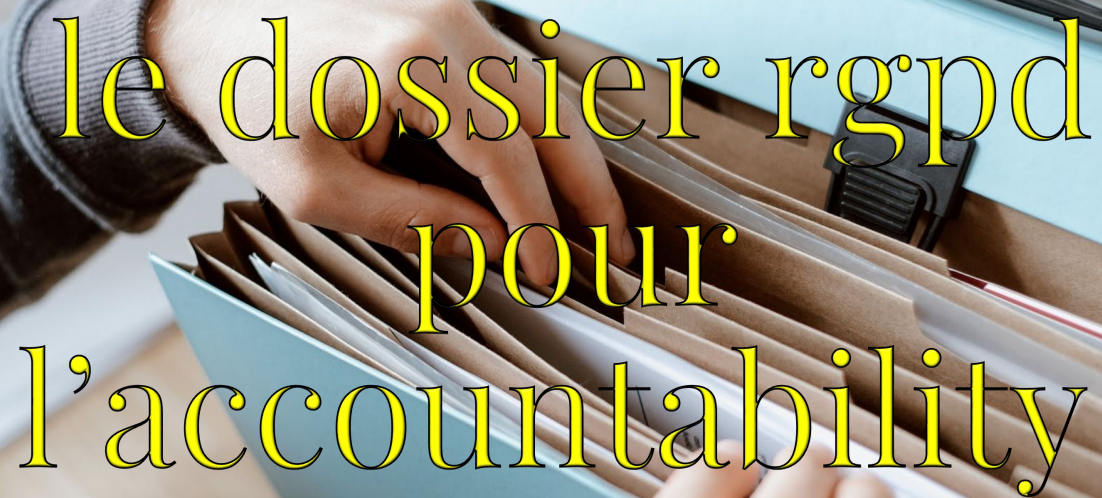
14. «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou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

# DEFINITION

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





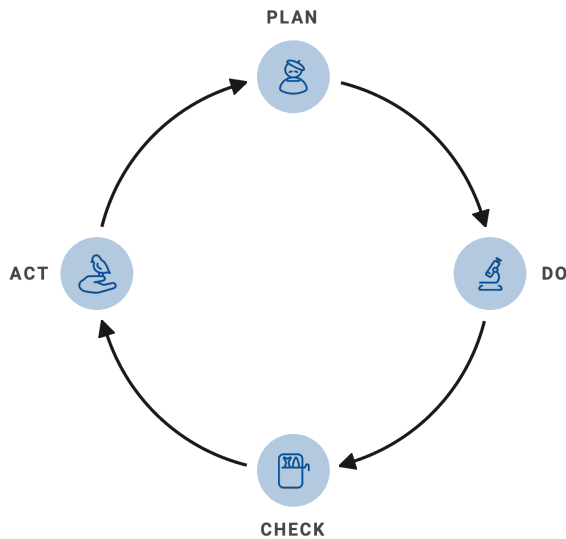
# le dossier rgpd pour l'accountability



## 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

### Table des matières

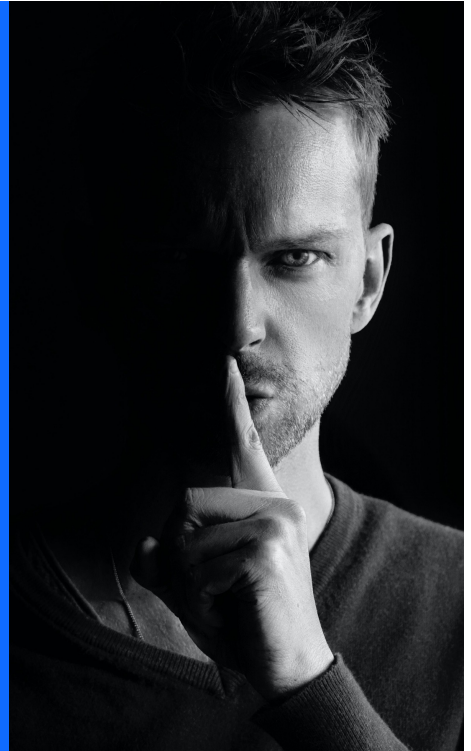
<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Nomination du DPD</b>	<b>3</b>
<b>3</b>	<b>Mesures de sécurité organisationnelles</b>	<b>4</b>
3.1	Caméras de surveillance dans les zones accessibles au public	5
<b>4</b>	<b>Mesures de sécurité techniques</b>	<b>6</b>
<b>5</b>	<b>Site Internet</b>	<b>8</b>
<b>6</b>	<b>Documents concernant les ressources humaines</b>	<b>9</b>
6.1	Clause de confidentialité	9
6.2	Charte informatique	9
6.3	Droits à l'image des collaborateurs	9
6.4	Autres aspects liés aux Ressources Humaines	9
<b>7</b>	<b>Procédures quant aux droits des personnes concernées</b>	<b>10</b>
7.1	Droit d'accès	10
7.2	Droit de rectification	10
7.3	Droit à l'effacement	10
7.4	Droit à la limitation	10
7.5	Droit à la portabilité	10
<b>8</b>	<b>Bases de données existantes</b>	<b>11</b>
8.1	Licéité du traitement concernant les clients des courtiers	11
8.2	Données des tiers	11
8.3	Bases de données fournies par des tiers	11
<b>9</b>	<b>Vols et pertes de données</b>	<b>12</b>
<b>10</b>	<b>Sous-traitants</b>	<b>13</b>
<b>11</b>	<b>Analyse d'impact relatif à la protection des données</b>	<b>14</b>
<b>12</b>	<b>Registre des fiches de traitement</b>	<b>15</b>
12.1	Gestion du personnel employé	15
12.2	Gestion de candidatures	17
12.3	Prospection commerciale	19
12.4	Gestion des fournisseurs	21
12.5	Gestion des clients	23
12.6	Listes de prospects achetées	25
12.7	Comptabilité	27
12.8	Accès aux bureaux	29
12.9	Accès de visiteurs aux bureaux	31
12.10	Gestion du pointage des employés	33
12.11	Surveillance vidéo dans l'espace public	35

Exemple  
gdprfolder.com

## TABLE DES MATIÈRES

12.12	Campagnes de marketing	37
12.13	Archivage et destruction des données personnelles	39
12.14	Analyse statistique	41
12.15	Utilisation de cookies	43
12.16	Documents des conseils d'administration/gérance/assemblées	45
12.17	Gestion des assurances incendie	47
12.18	Gestion générale des assurances vie	49
12.19	Gestion générale des assurances voyage	51
12.20	Gestion des assurances marchandises transportées	53
12.21	Gestion des responsabilités civiles	55
12.22	Gestion générale des assurances "multi" (package d'assurances diverses)	57
12.23	Gestion générale des assurances individuelles	60
12.24	Gestion d'assurances diverses (marchandises transportées, pertes pécuniaires diverses, protection juridique)	62
12.25	Assurance auto	65
12.26	Assurances Assistance	67
12.27	Assurances accidents de travail et collective	69

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

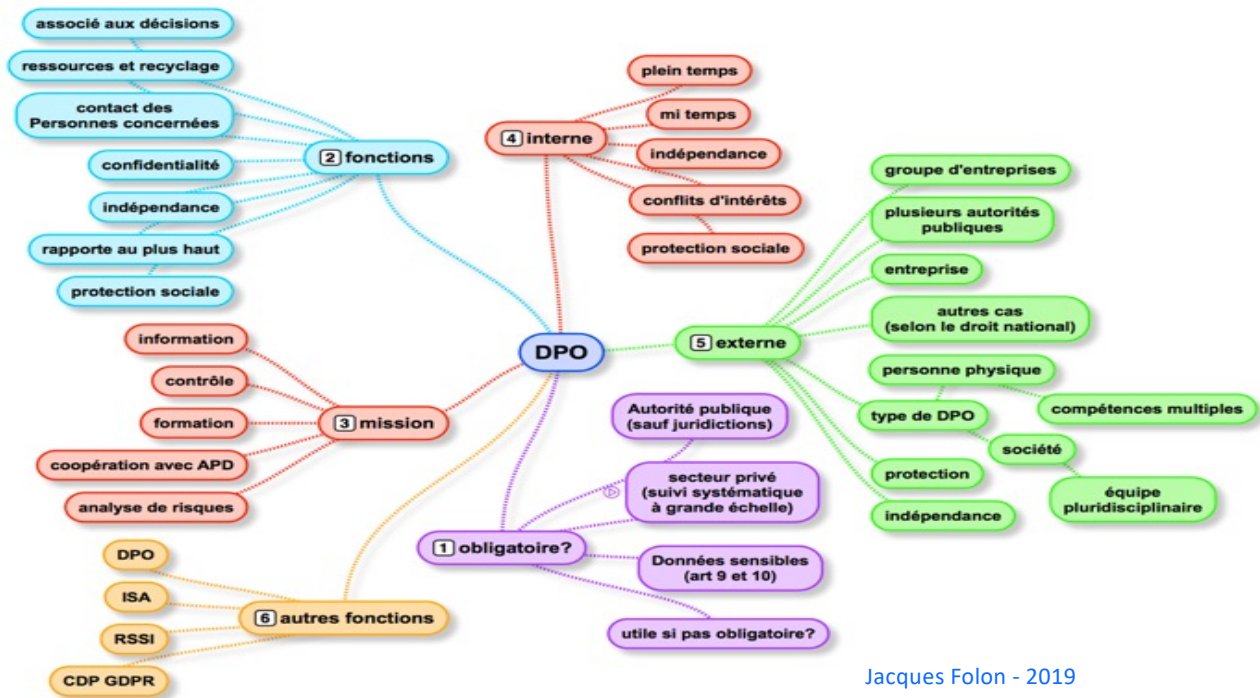


A quoi ça sert un DPO ?

DATA PROTECTION OFFICER

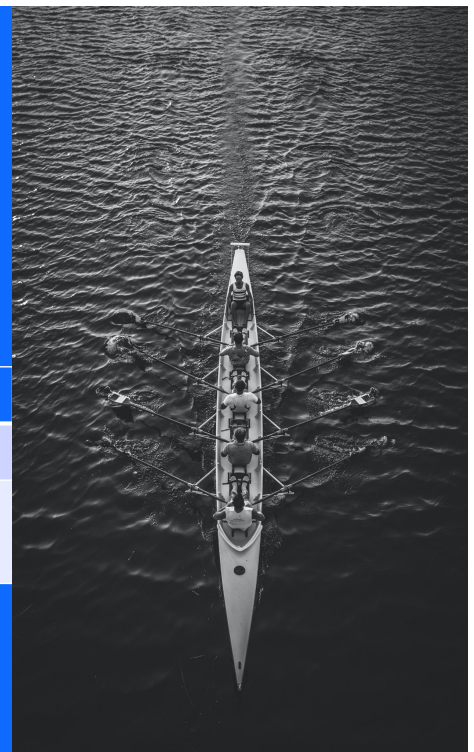






# Rôles et fonctions

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 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.

La base de référence est le RGPD et les normes ISO 2700x

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 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 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



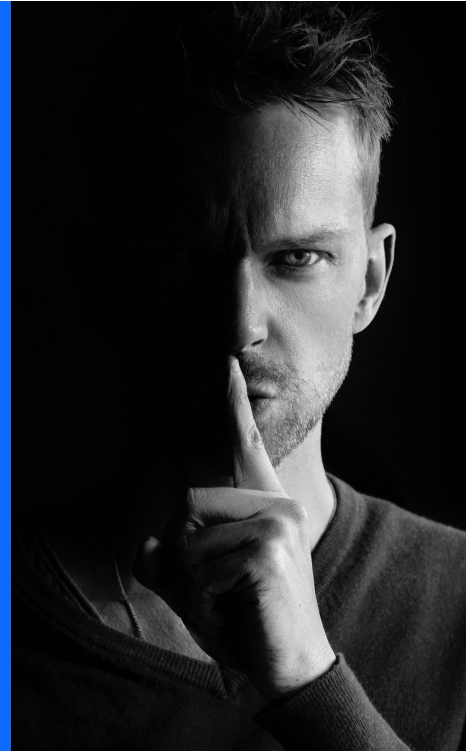


## Que met-on dans le dossier ?

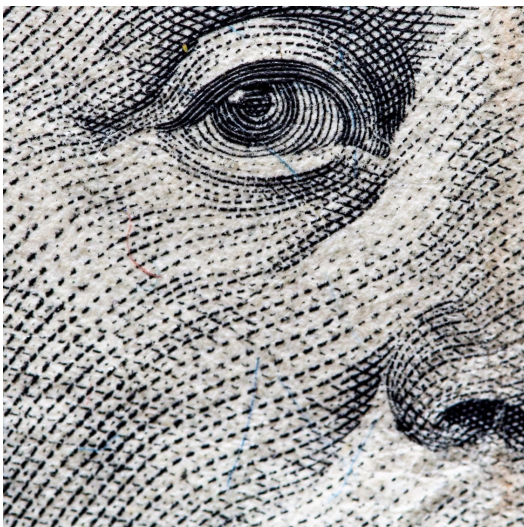
- Décision de nomination motivée de la direction
- Ou
- Décision motivée de ne pas avoir de DPO
- Information de l'APD
- Les « avis du DPO »



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”  
”

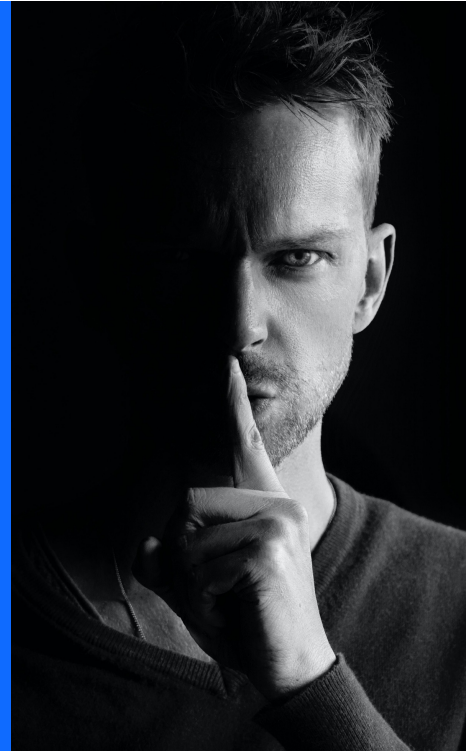
“le service ou le département”  
”

### Que met-on dans le dossier ?

- Décision motivée de la direction



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 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.





Written by Daniel J. Solove

Illustrated by Ryan Beckwith

For personal use only. Please ask us for permission for other uses.

## 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

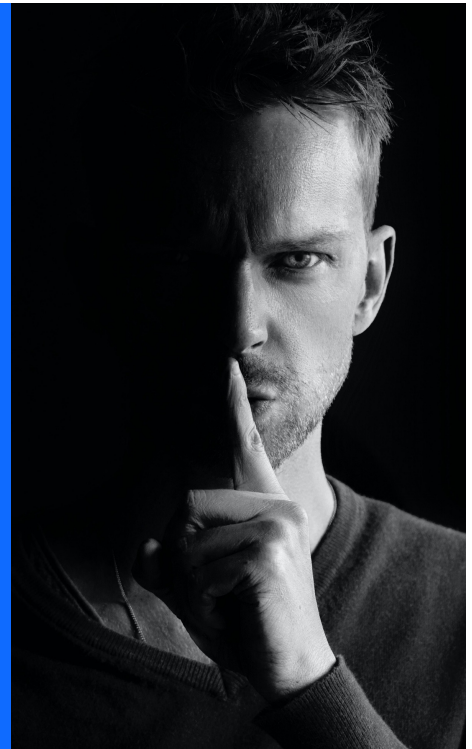


## Que met-on dans le dossier ?

- 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

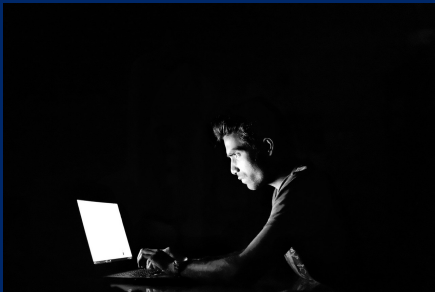




## Site internet



### le site internet est très visible...



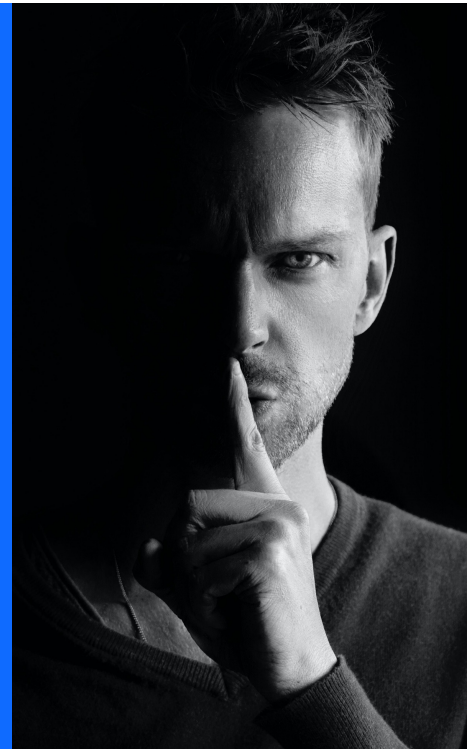
- Double opt-in
- Conservation des accords (contrat, consentement)
- Cookies
- Marketing digital
- Google analytics
- Durée de conservation
- Privacy policies (plusieurs finalités)
- Collaboration DPO – ICT – RSSI-marketing

## 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...



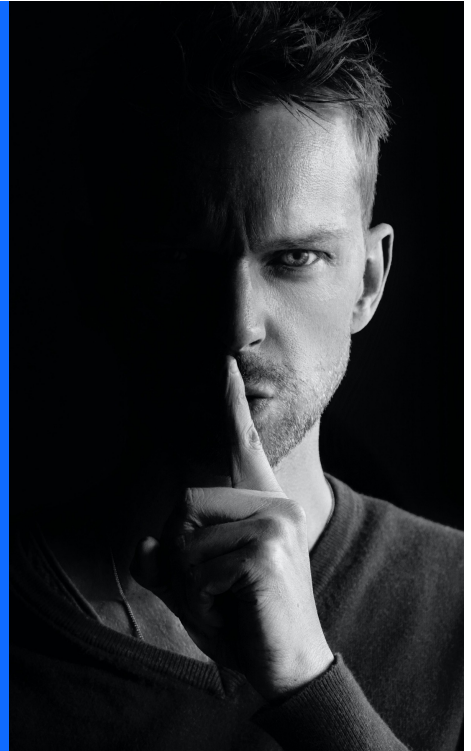
- Données sensibles
- RH
- Secrets d'affaires
- Identifier les départements à risques
- On commence par sécuriser les worst case
- Procédure en cas de vol/perte
- Shadow IT !
- Journalisation
- Back-ups
- Préparer réponse au droit d'accès

## 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**



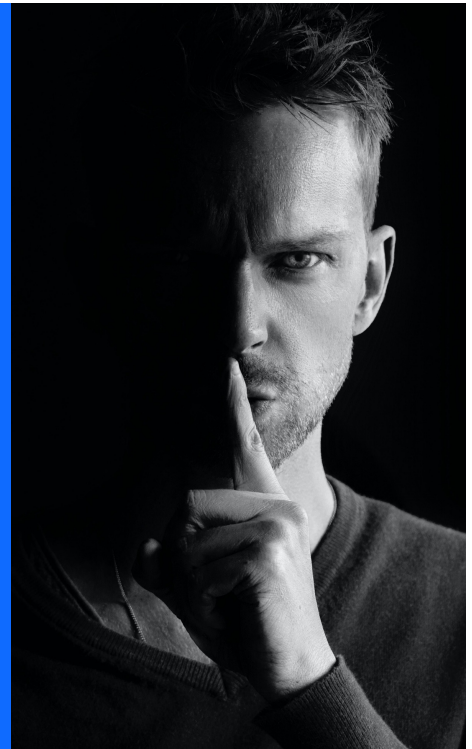


## Que met-on dans le dossier ?

- 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

**CYBER SÉCURITÉ**

A hand is shown shattering a glass surface. The words "CYBER SÉCURITÉ" are written in a metallic, textured font across the glass. The background is dark, and the lighting highlights the hand and the shattering glass.

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

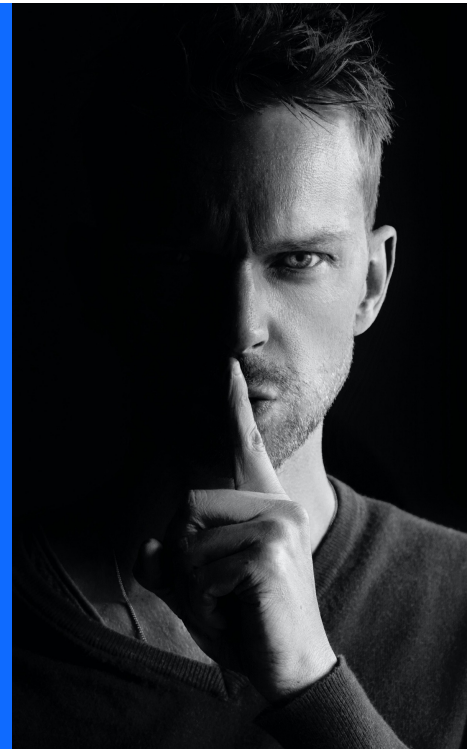


## Que met-on dans le dossier ?

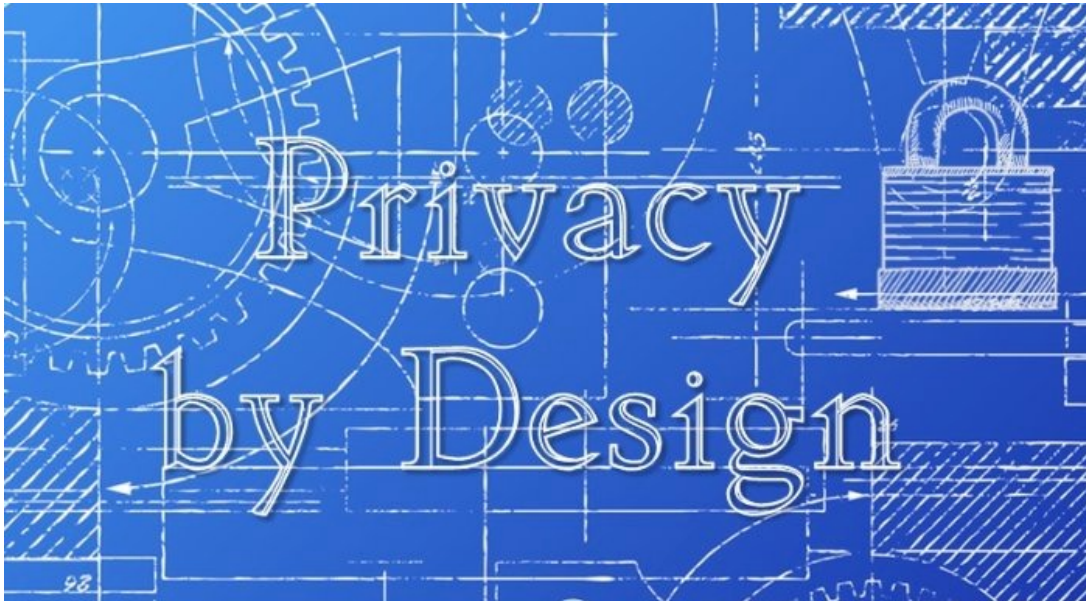
- Le plan de sécurité
- Les mesures de sécurité
- Les éventuelles certifications ISO ou autres



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







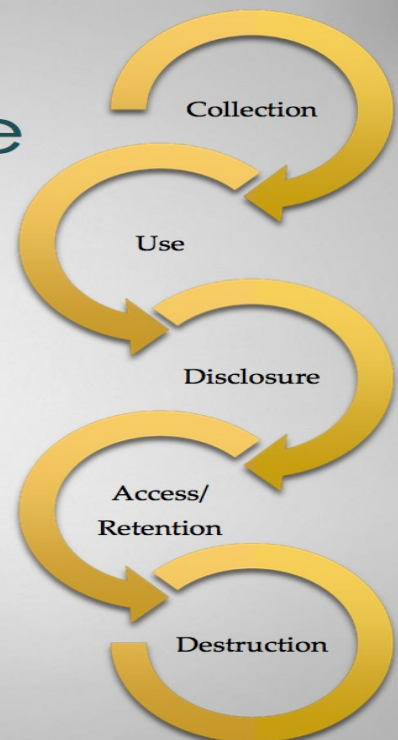
- **Privacy by design?**
- **Il faut documenter !**
- **Comment faire?**
- **Comment le démontrer?**
- **Comment convaincre les développeurs?**

## DATA QUALITY IS ESSENTIAL

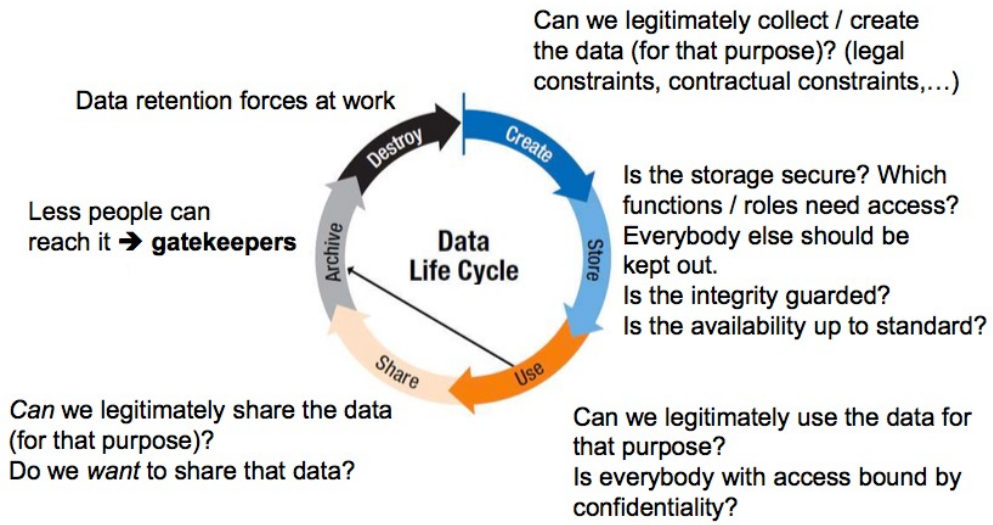


## Core Principles: Information Lifecycle

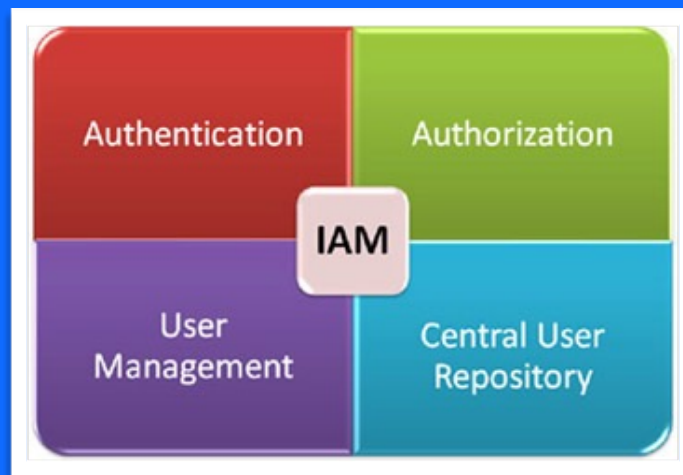
Privacy by Design  
requires  
contemplating each  
phase of the  
information lifecycle



Look at the entire data lifecycle



## Identity Access Management (GESTION DES ACCÈS)



## 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?



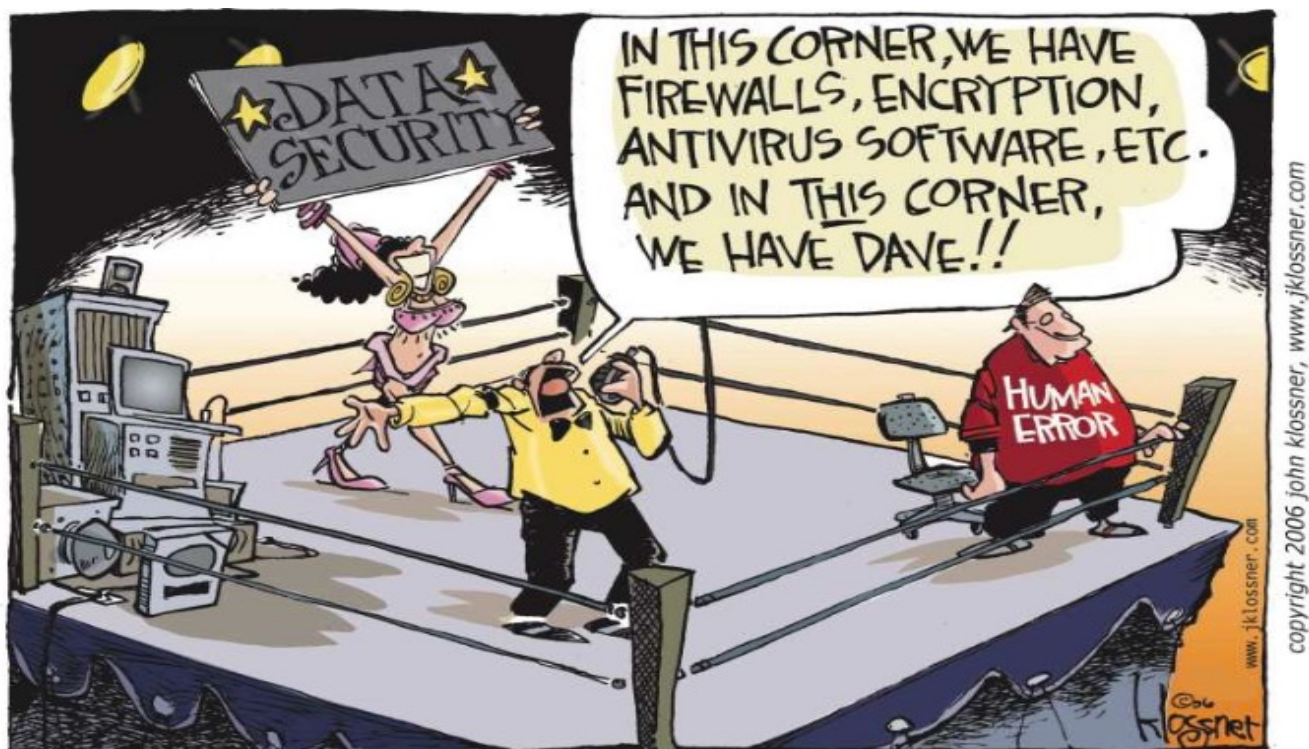
8 7

## 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?



8 8

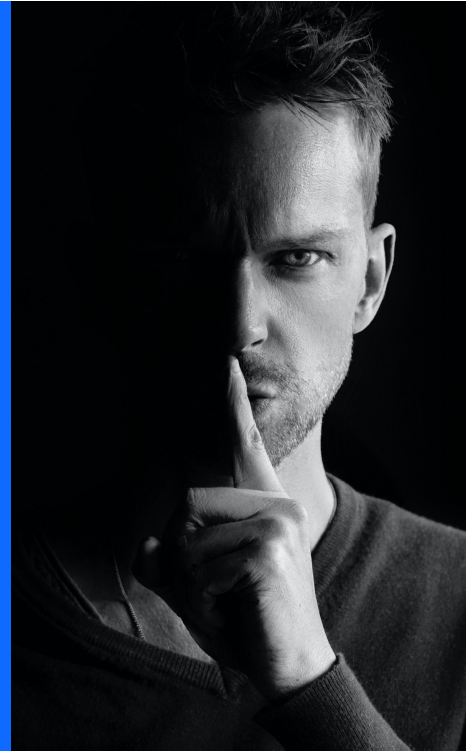


## Que met-on dans le dossier ?

- 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



## Data breaches

YOU'VE BEEN HACKED!



## ANTICIPATION DE LA COMMUNICATION DE CRISE

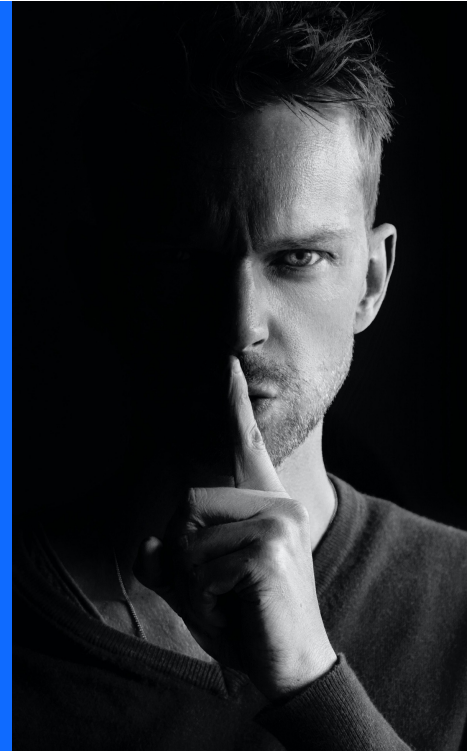
9  
3

## 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

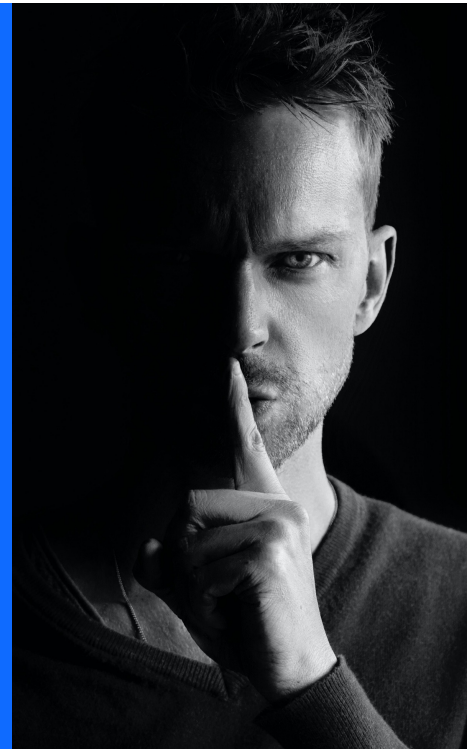


## Que met-on dans le dossier ?

- 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 simultanités
- Log de non-conformité
- Méthode de classement
- Il faut retrouver les preuves!

# CONCLUSION



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

