

# LPD & RGPD risques ou opportunités pour les sociétés suisses ?



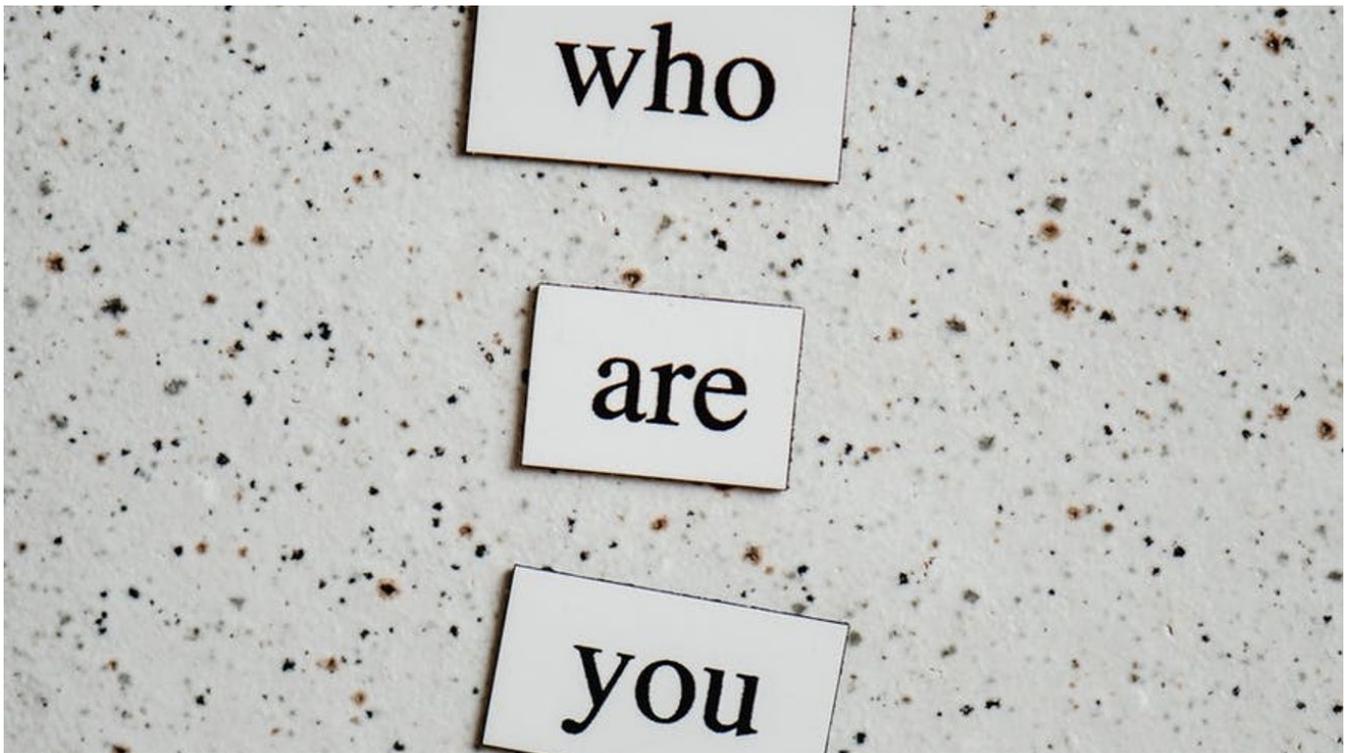
Genève

26 septembre 2023



Prof. Dr. Jacques Folon

-  Jacques@gdprfolder.eu
-  [www.linkedin.com/in/folon](https://www.linkedin.com/in/folon)
-  [www.gdprfolder.com](https://www.gdprfolder.com)
-  +32 475 98 21 15
-  [www.folon.com](https://www.folon.com)
-  <https://readmylips.be/fr/moderators/jacques-folon>



### Quelques questions avant de commencer

- Qui n'a aucun client ou prospect en dehors de la Suisse?
- Qui se considère parfaitement en règle avec le RGPD ?
- Qui a modifié ses traitements de données suite à l'arrivée de la LPD ?



# VOGUE

LE RGPD ET LA LPD SONT-ILS UNE MODE PASSAGERE ?



QUE RISQUE-T-ON A NE PAS RESPECTER LA PROTECTION DES DONNEES ?

USE AT OWN RISK

#### RISQUES DE

- PERTE DE REPUTATION
- RISQUE OPERATIONNEL (PERTE DE DONNEES)
- RISQUE D'AMENDES
- RISQUE DE DOMMAGES ET INTERETS
- DATA BREACH PUBLIC
- PERTE DE CLIENTELE
- INFORMATIQUE BLOQUEE
- CYBERCRIMINALITE
- ...



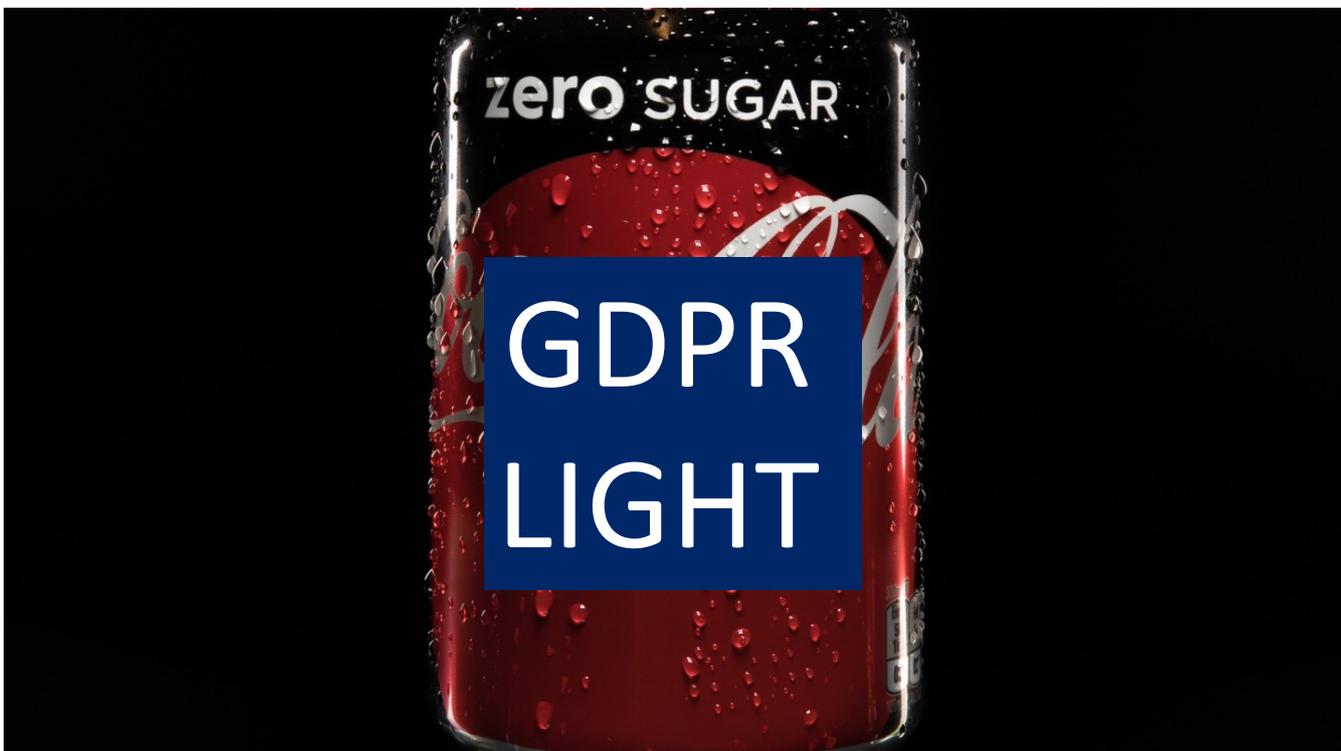
**Imaginez que le PFPDT vous annonce  
sa visite suite à une plainte.  
Comment et que préparez-vous?**

QUELLES EST LA DIFFERENCE  
ENTRE LA LPD ET LE RGPD?



zero SUGAR

GDPR  
LIGHT



# \_swissprivacy.law

Tableau comparatif entre  
La nouvelle Loi fédérale sur la protection  
des données du 25 septembre 2020  
(nLPD)  
et  
Le Règlement général sur la protection  
des données du 27 avril 2016 (RGPD)

<https://www.fedlex.admin.ch/eli/cc/2022/491/fr>

## Loi de protection des données personnelles



**Confédération:** LPD, 1992

- Dès septembre 2023 : nLPD (CONFÉDÉRATION, 2020)



**Cantons:**

- Vaud : LPrD (*ETAT DE VAUD, 2007*)
- Genève : LIPAD (*ETAT DE GENÈVE, 2001*)
- Valais : LIPDA (*CANTON DU VALAIS, 2008*)
- Fribourg : LPrD (*ETAT DE FRIBOURG, 1994*)
- Jura et Neuchâtel : CPDT-JUNE (*CANTON DU JURA et CANTON DE NEUCHÂTEL, 2012*)



**Union européenne:** RGPD (*UNION EUROPÉENNE, 2016*)

## Principales nouveautés

Avec l'entrée en vigueur de la nouvelle LPD, l'économie privée et les autorités fédérales doivent adapter leur traitement de données personnelles aux nouvelles dispositions. Le PFPDT a consigné à ce sujet les nouveautés les plus importantes :

### SITE DU PFPDT

#### Conseiller à la protection des données

Notification de conseillères et conseillers à la protection des données au PFPDT conformément à l'art. 10, al. 3 LPD pour les particuliers et à l'art. 10, al. 4 LPD pour les organes fédéraux.

#### Devoir d'informer

Le devoir d'informer garantit la transparence des traitements et contribue à renforcer les droits de la personne concernée.

#### Droit d'accès

Conformément à la loi fédérale sur la protection des données, toute personne peut demander au responsable du traitement si des données personnelles la concernant sont traitées.

#### Rôle du PFPDT

Des nouveautés non seulement pour les personnes traitant des données et pour les personnes concernées, mais aussi pour le PFPDT, dont elle modifie les tâches et les pouvoirs.

#### Analyse d'impact relative à la protection des données personnelles

Les responsables du traitement des données doivent effectuer une AIPD lorsque le traitement de données personnelles est susceptible d'entraîner un risque potentiellement élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

#### Émoluments

A partir du 1.9.2023, le PFPDT prélèvera des émoluments pour certaines prestations.

#### Enquêtes concernant des violations des prescriptions de protection des données

L'activité de surveillance comprend l'examen des violations des prescriptions de protection des données et, le cas échéant, l'adoption de mesures administratives pour faire respecter ces règles.

#### Dispositions pénales

Aspects pénaux attachés aux violations des obligations instaurées par la LDP.

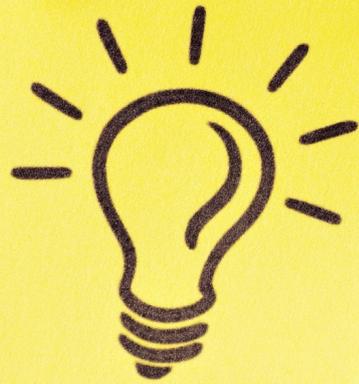
#### Certifications en matière de protection des données

La certification de systèmes, de produits et de services favorise la transparence du traitement des données.



## LES PRINCIPALES DIFFERENCES ENTRE LA LPD ET LE RGPD

- RESIDENTS SUISSES >< RESIDENTS DE L'UE
- AMENDES PLUS ELEVEES POUR LE RGPD
- AMENDES SOCIETE ><AMENDES DIRIGEANTS
- DPO OBLIGATOIRE >< CONSEILLE
- BASE LEGALE >< PAS PRECISE



# PETIT RAPPEL QUANT AU RGPD

Un petit  
résumé ?

GDPR

**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
- Trade Union Membership
- Sex Life
- Political Opinions
- Racial or Ethnic Origin
- Genetic Data
- Biometric Data
- Health

**RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS**

- Security
- Data Protection Officer (DPO)  
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.
- Record of Data Processing Activities  
Maintain a documented register of all activities involving processing of EU personal data.
- Data Protection by Design  
built in starting at the beginning of the design process.
- Data Impact Assessment  
For high risk situations.

**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  
"Right not to be subject to a decision based solely on automated processing, including profiling."
- Access and Rectification
- Right to Erasure
- Purpose Specification and Minimization
- Right to Data Portability

**ENFORCEMENT**

Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies  
compensation for material and non-material harm.

**INTERNATIONAL DATA TRANSFER**

- Adequate Level of Data Protection
- Binding Corporate Rules (BCRs)
- Privacy Shield
- Model Contractual Clauses

TEACHPRIVACY

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

Workforce awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute



### 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, what they know and don't know, what someone thinks.
  - AUTHENTICATING**  
Information used to authenticate an individual with something they know, i.e. Passwords, PIN, mobile authentication.
  - PREFERENCE**  
Information about an individual's preference or interests, i.e. Opinions, interests, profession or interests.
- 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, dialects, 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, likes, shares, retweets, health records, blood type, DNA code, prescriptions.
  - 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, drug test results, diagnoses, therapy or physical 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 to have or get around from which might have influenced them (WHO, BY, 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, creditworthiness, credit standing, credit capacity.
- SOCIAL**
  - PROFESSIONAL**  
Information about an individual's educational or professional career, i.e. Job titles, salary, work history, school experience, employee files, employment history, evaluations, references, reviews, certifications, disciplinary 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 affiliations, memberships, communications, advocacy.
  - FAMILY**  
Information about an individual's family and relationships, i.e. Family structure, siblings, offspring, marital status, divorce.
  - 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**  
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.

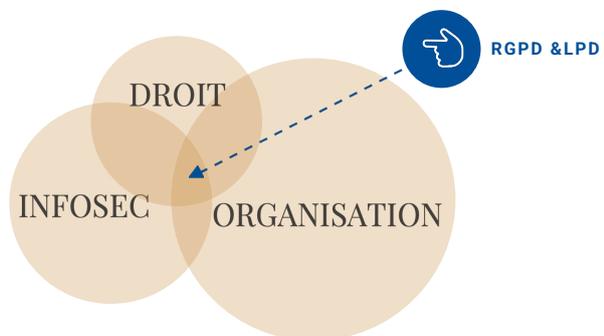
Come take our **FREE** **[VIDEO]** to come learn more about personal data!

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



# RGPD & LPD = gestion des data !!

Combinaison de 3 éléments

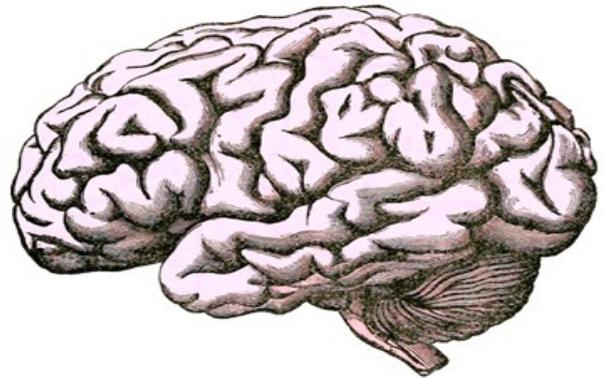


**LE GRPD/LPD CA PEUT ETRE POSITIF**

**MEILLEURE CONNAISSANCE DES PROCESSUS INTERNES**



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

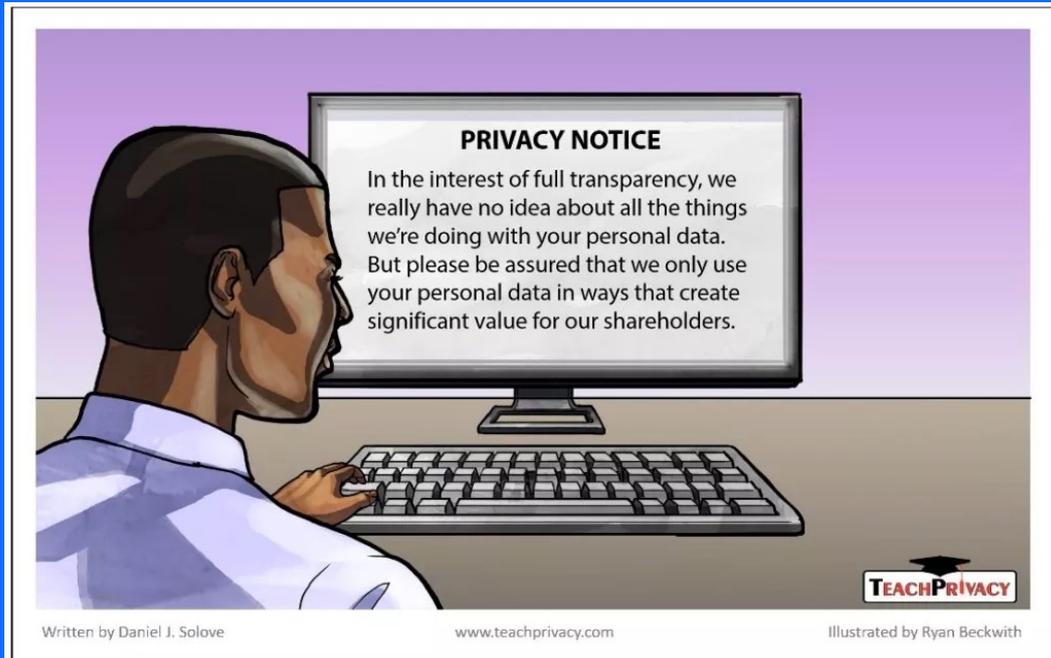


[www.teachprivacy.com](http://www.teachprivacy.com)

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



# 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/LPD

**PRÉSUMÉ  
COUPABLE**

**Obtenir une certification RGPD/LPD ?**





## 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](#)





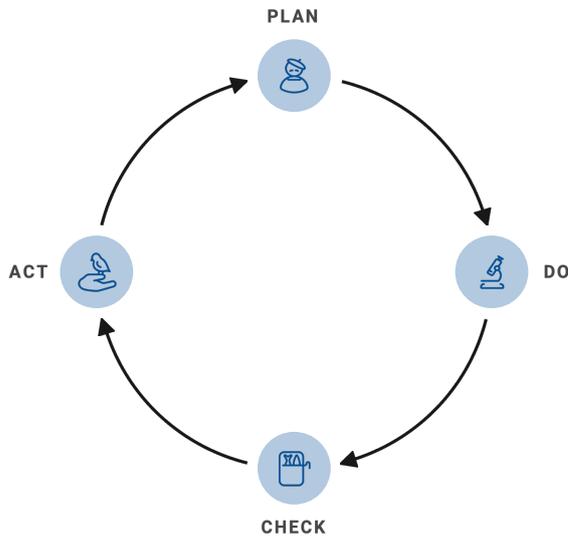
# le dossier LPD/rgpd pour l'accountability



## 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 NE SERA JAMAIS FINI !



## TABLE DES MATIÈRES

### Table des matières

<b>1 Introduction</b>	<b>2</b>
<b>2 Nomination du DPD</b>	<b>3</b>
<b>3 Mesures de sécurité organisationnelles</b>	<b>4</b>
3.1 Caméras de surveillance dans les zones accessibles au public	5
<b>4 Mesures de sécurité techniques</b>	<b>6</b>
<b>5 Site Internet</b>	<b>8</b>
<b>6 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 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 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 Vols et pertes de données</b>	<b>12</b>
<b>10 Sous-traitants</b>	<b>13</b>
<b>11 Analyse d'impact relatif à la protection des données</b>	<b>14</b>
<b>12 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

# 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 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



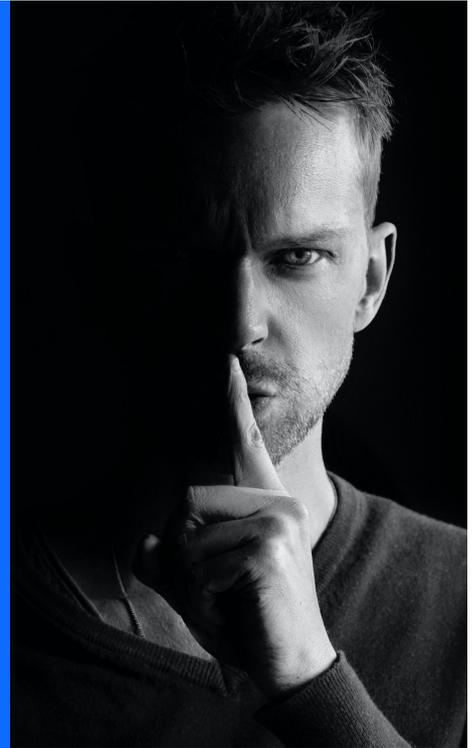


## Que met-on dans le dossier ?

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



## Le responsable de traitement



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”  
”

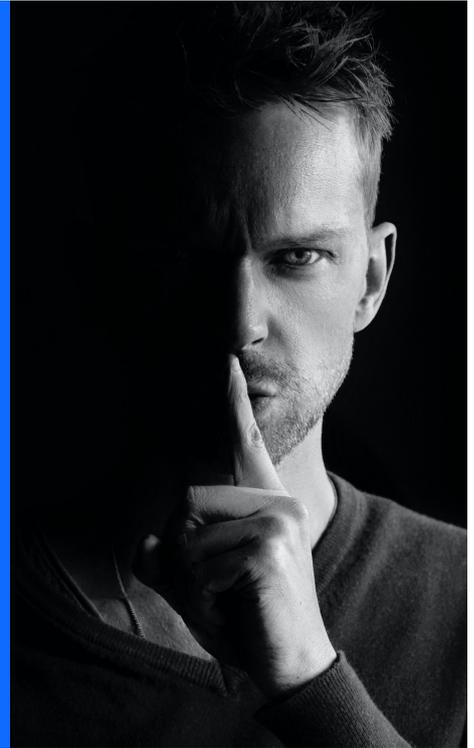
“le service ou le département”  
”

### Que met-on dans le dossier ?

- Décision motivée de la direction



## Le sous-traitant



## 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



QUID DES ST AMERICAINS ?

## Site internet



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



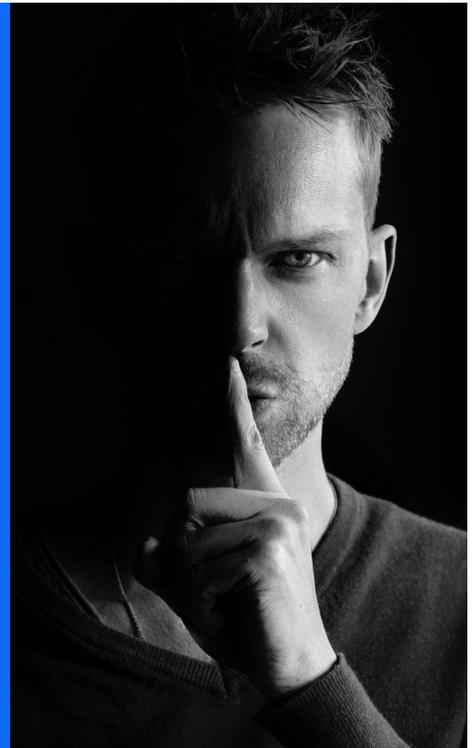
- Double opt-in
- Conservation des accords (contrat, consentement)
- Cookies
- Marketing digital
- Google analytics
- Durée de conservation
- Privacy policies (plusieurs finalités)
- Collaboration DPO – ICT – RSSI-marketing

Que met-on dans le dossier ?

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



**Les DB existantes**



## toutes les bases de données...



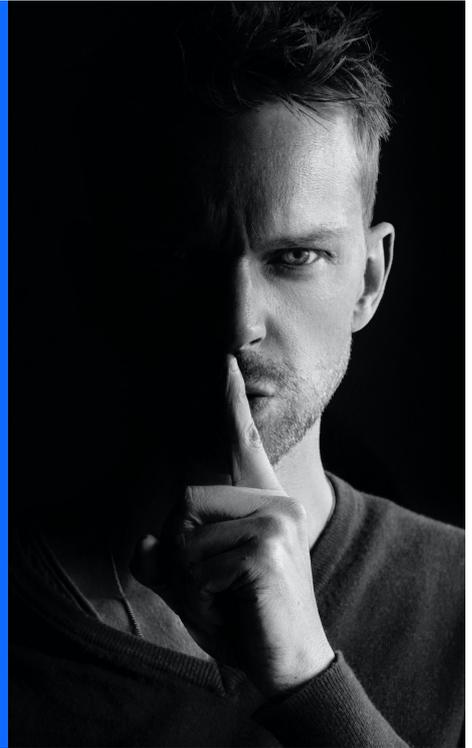
- Données sensibles
- RH
- Secrets d'affaires
- Identifier les départements à risques
- On commence par sécuriser les worst case
- Procédure en cas de vol/perte
- Shadow IT !
- Journalisation
- Back-ups
- Préparer réponse au droit d'accès

## Que met-on dans le dossier ?

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



## Les droits des personnes



- ☑ 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



Les mesures de sécurité techniques et organisationnelles

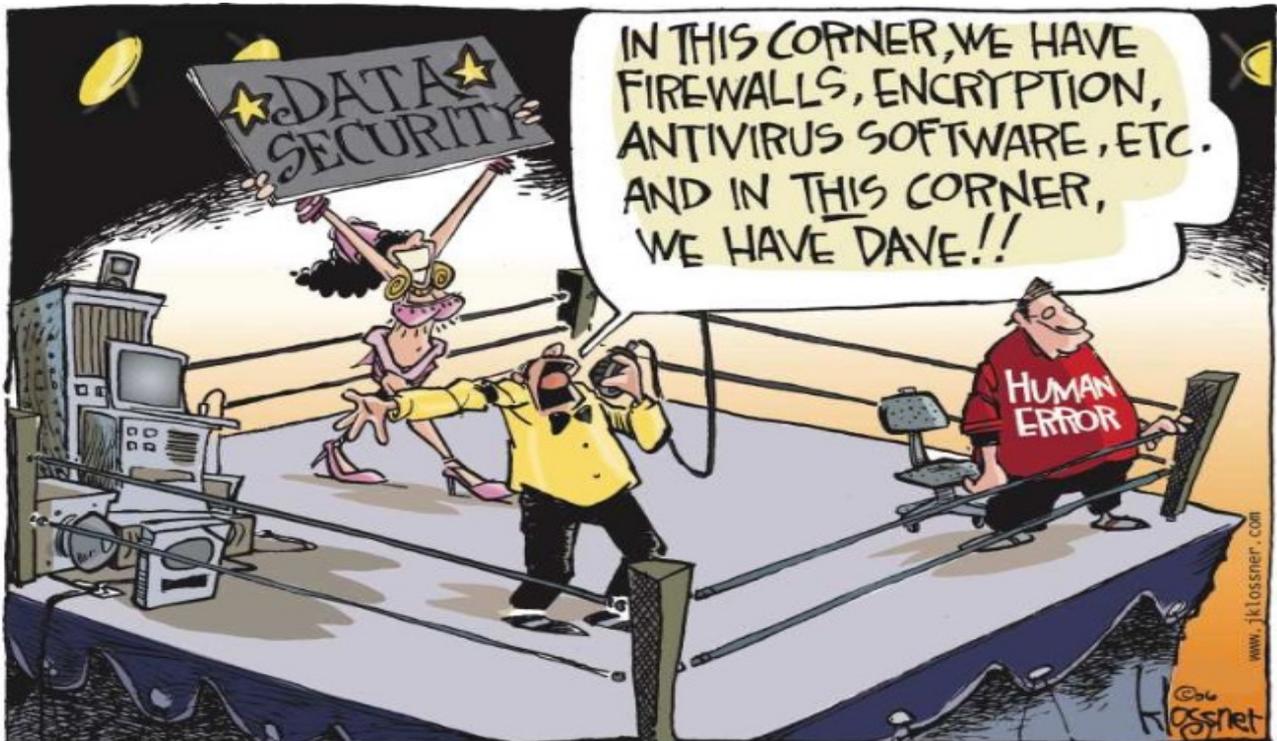
**CYBER SÉCURITÉ**

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



## Identity Access Management (GESTION DES ACCÈS)

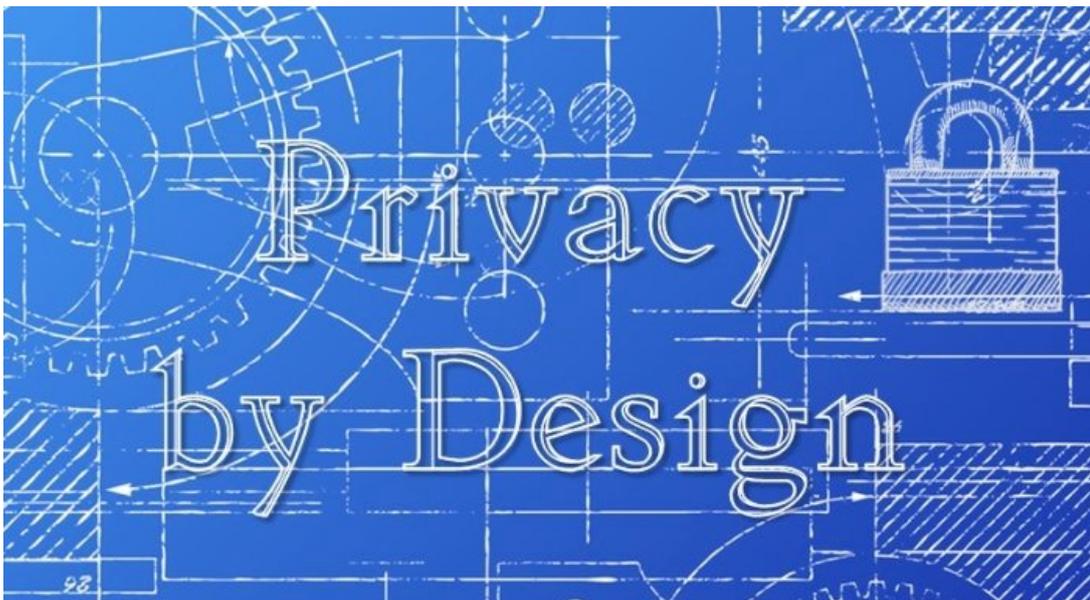


## Que met-on dans le dossier ?

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



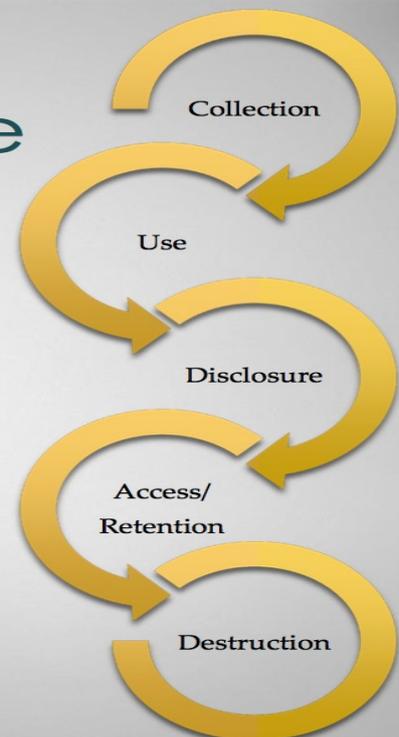
**PRIVACY BY DESIGN MEANS  
THINK PRIVACY FIRST !**



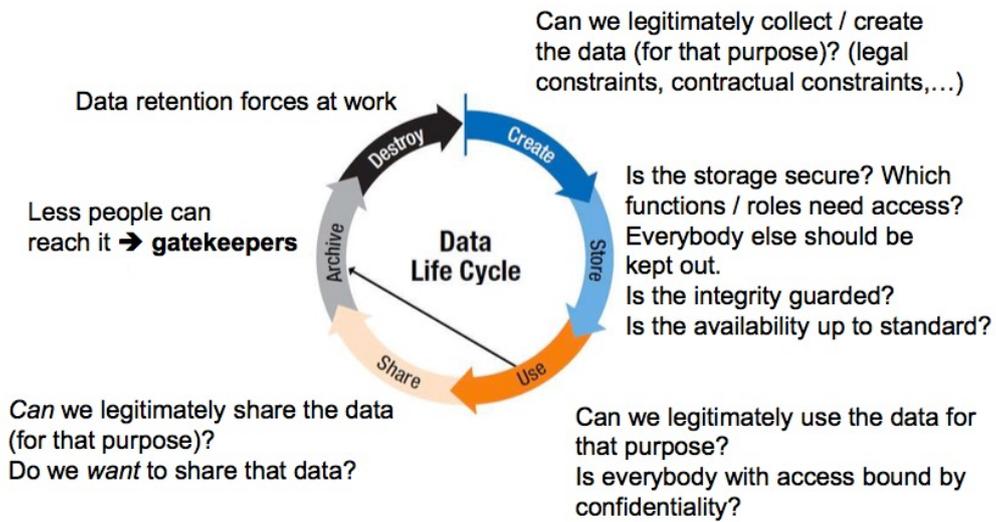
- **Privacy by design?**
- **Il faut documenter !**
- **Comment faire?**
- **Comment le démontrer?**
- **Comment convaincre les développeurs?**

## Core Principles: Information Lifecycle

Privacy by Design  
requires  
contemplating each  
phase of the  
information lifecycle



## Look at the entire data lifecycle



## Que met-on dans le dossier ?

- La documentation
- L'avis du DPO



Data breaches

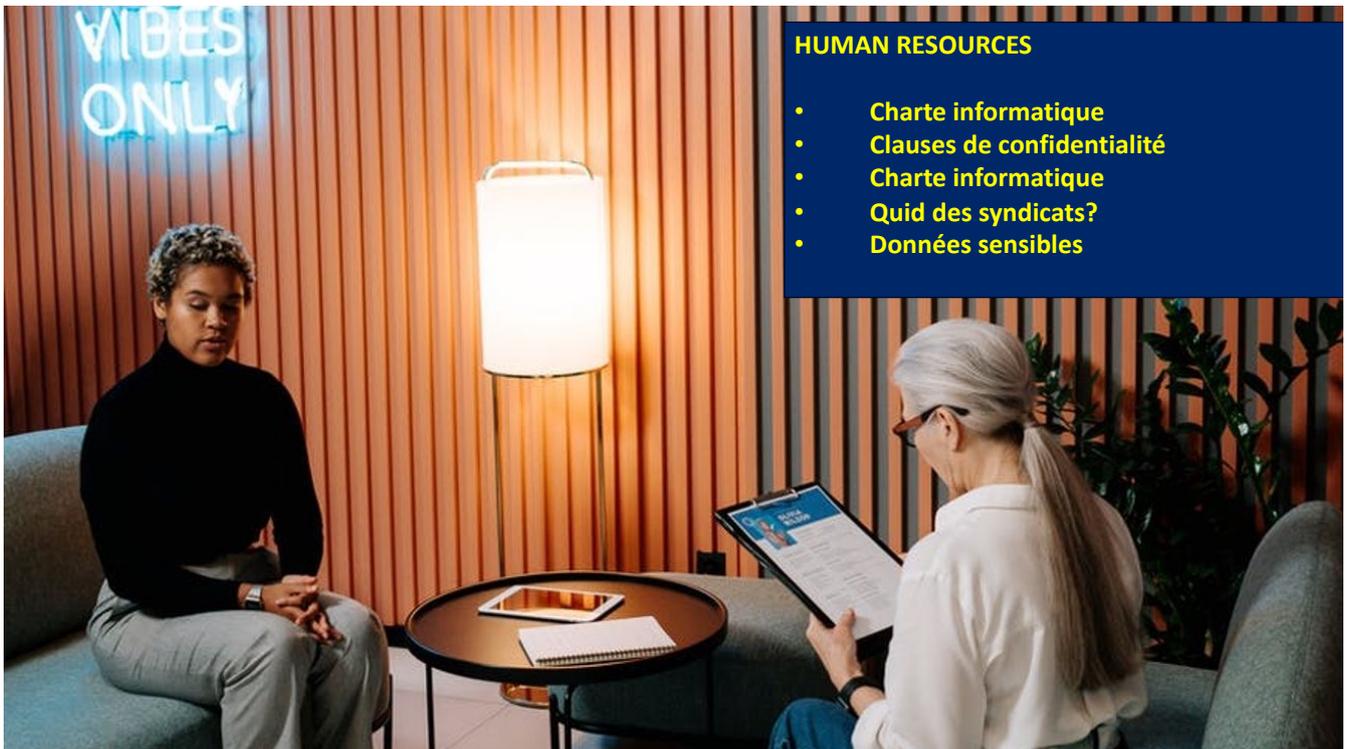


ANTICIPATION DE LA  
COMMUNICATION  
DE CRISE



## Que met-on dans le dossier ?

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



## Que met-on dans le dossier ?

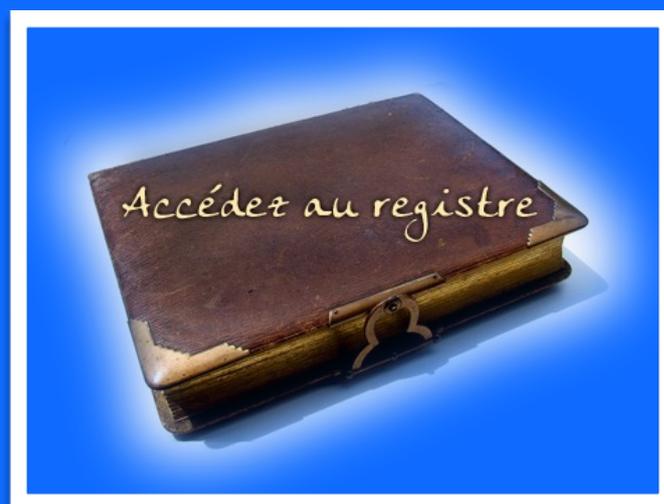
- Toutes les procédures
- La preuve des information
- La preuve de la distribution des procédures
- La preuve des formations



**DATA PRIVACY IMPACT ASSESMENT  
RISK ANALYSIS**



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



## 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!

## Les risques de l'IA face au RGPD/LPD

START DANGER  
ZONE

We should not underestimate the real threats coming from AI, mostly GenAI.

13/9/2023





**Leonardo Cervera Navas**  
*Director of the European Data  
Protection Supervisor.*



## **“Nous devons 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

*"Les menaces associées à l'essor de cette technologie sont multiples : peur de voir disparaître certains emplois, crainte d'une utilisation à des fins malveillantes, atteintes à la propriété intellectuelle, exploitation illicite de données personnelles..."*

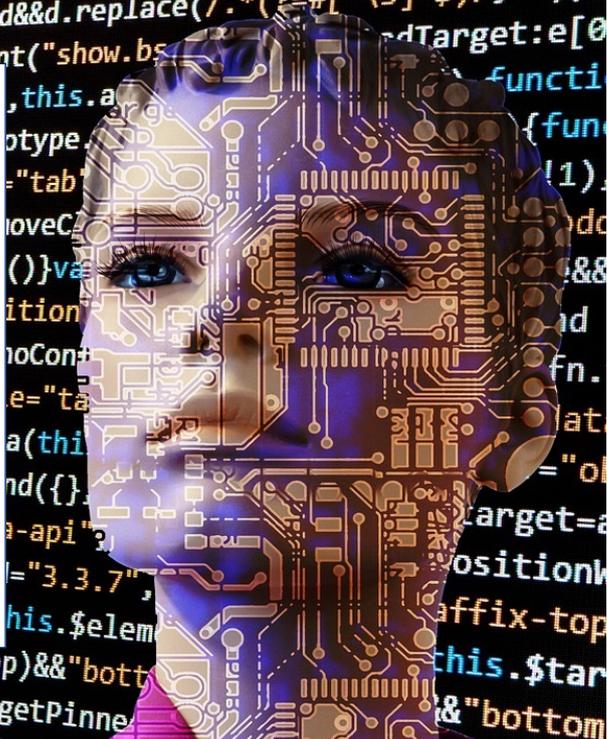
*Pour créer les conditions d'une utilisation éthique, responsable et respectueuse de nos valeurs, il faut comprendre, accompagner et contrôler. On ne peut bien réguler qu'un objet que l'on comprend*



Présidente de la Cnil Marie-Laure Denis  
18/9/2023

IA ET RGPD/LPD

- 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



## 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/LPD n'en finit pas d'évoluer !



© 2018 GDPRFOLDER.EU SPRL All Rights Reserved.

Pour créer la confiance => **ETAT**

- **E**tat des lieux
- **T**out documenter
- **A**nalyser les risques
- **T**ransparence

