POLYTECH DIJON

# Les données personnelles & sensibles en entreprise

Paul DUCOLOMB
Firmin LAUNAY
Théophile REY

31 mai 2024

# Donnée personnelle ?
# Donnée sensible ?

# Données personnelles

- Définition : Toute information se rapportant à une personne physique identifiée ou identifiable.
- Exemples : Nom, adresse, numéro de téléphone, adresse e-mail, numéro de sécurité sociale.

# Données sensibles

- Définition : Sous-catégorie de données personnelles, nécessitant une protection accrue en raison de leur nature.
- Exemples : Données de santé, opinions politiques, croyances religieuses, orientation sexuelle, données biométriques.

# Distinction entre données personnelles et sensibles

- Les données sensibles sont une sous-catégorie de données personnelles.
- Protection : Les données sensibles nécessitent des mesures de protection plus strictes.
- Exemples :

    - Personnelle : Nom et prénom.
    - Sensible : Dossier médical.

Cette distinction est cruciale pour assurer la conformité et la protection des droits individuels au sein de l'entreprise.

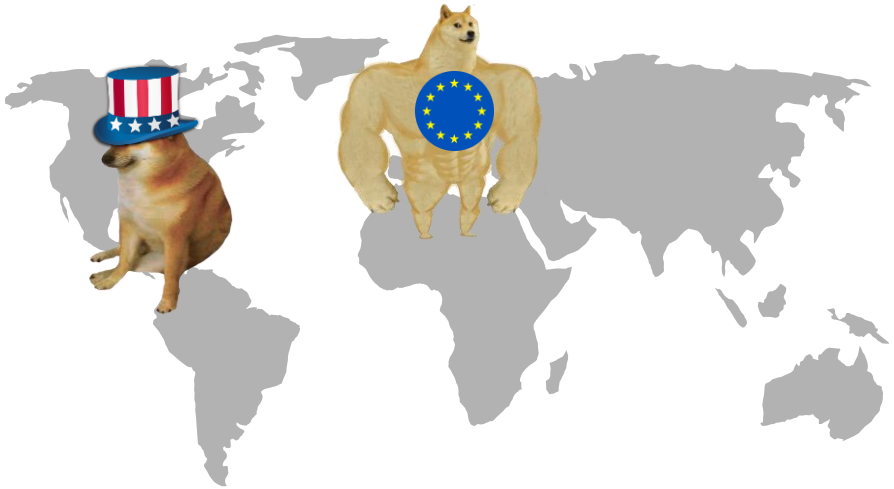
# Règles de traitement

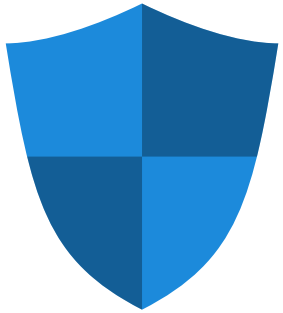
# Le RGPD, règlement européen

- **R**èglement **G**énéral sur la **P**rotection des **D**onnées
- Principale loi européenne régissant le traitement des données personnelles et des données sensibles
- Publié en avril 2016, applicable depuis mai 2018
- En France, peu de nouveautés (loi Informatique et Libertés, 1978)

# Les grands principes du RGPD








# Protection des données personnelles et sensibles par le RGPD

- Traitement des données personnelles fortement encadré.

- Traitement des données sensibles…

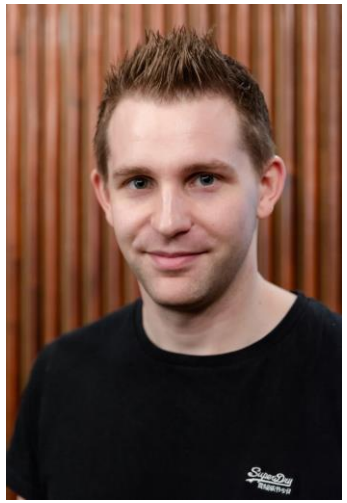
… **INTERDIT*** !

* sauf dans quelques exceptions

# Transfert extra-européen des données personnelles

- Pour permettre le transfert, accord à signer entre les deux pays.
- Confidentialité des données doit être garantie par législation locale.

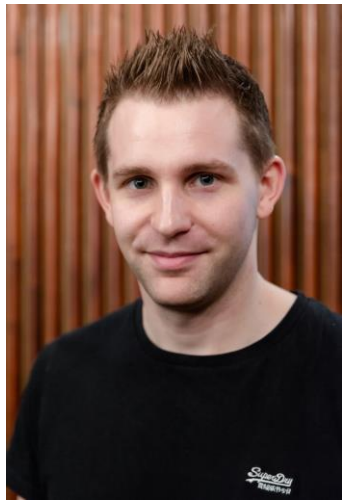
# Le cas *intéressant* des États-Unis



Max Schrems

- Attaque Meta en justice, lui reprochant de stocker ses données personnelles aux États-Unis → cela entraînerait selon lui un manque de confidentialité.
- À la clef, une amende de 1,2 Md € pour Meta.
- **Obtient l'invalidation tour à tour des deux accords de transferts entre l'Union Européenne et les États-Unis.**

# Le cas *intéressant* des États-Unis



Max Schrems

- FISA : « autorise l'administration américaine à collecter, utiliser et partager des données personnelles étrangères stockées sur des serveurs américains ».

- CLOUD Act : « autorise l'administration américaine […] à saisir […] sans procédure tous documents et communications électroniques […] localisés dans les datacenters d'entreprises américaines, situés au États-Unis et à l'étranger ».

**Manifestement incompatibles avec le RGPD !**

# Et en dehors du RGPD ?


ISO 27701 : mesures de sécurité à mettre en place pour traiter des données personnelles

- Ensemble de bonnes pratiques à mettre en place…
- … pour tout simplement respecter la loi, et notamment le RGPD.

→ pas réellement d'apport, plutôt une méthodologie à suivre.

# Gestion en entreprise

# Traitement des données en entreprise

- CNIL 2023 : 43 sanctions (amendes et rappels à l'ordre)

| | | | |
|---|---|---|---|
| 27/12/2023 | MEDECIN PEDIATRE (procédure simplifiée) | Défaut de coopération avec la CNIL | Amende de 1 000 euros |

# Traitement des données en entreprise

| | | | |
|---|---|---|---|
| 09/11/2023 | MINISTERE | Détournement des finalités | > Rappel à l'ordre |
| 09/11/2023 | MINISTERE | Détournement des finalités | > Rappel à l'ordre |

# Traitement des données en entreprise

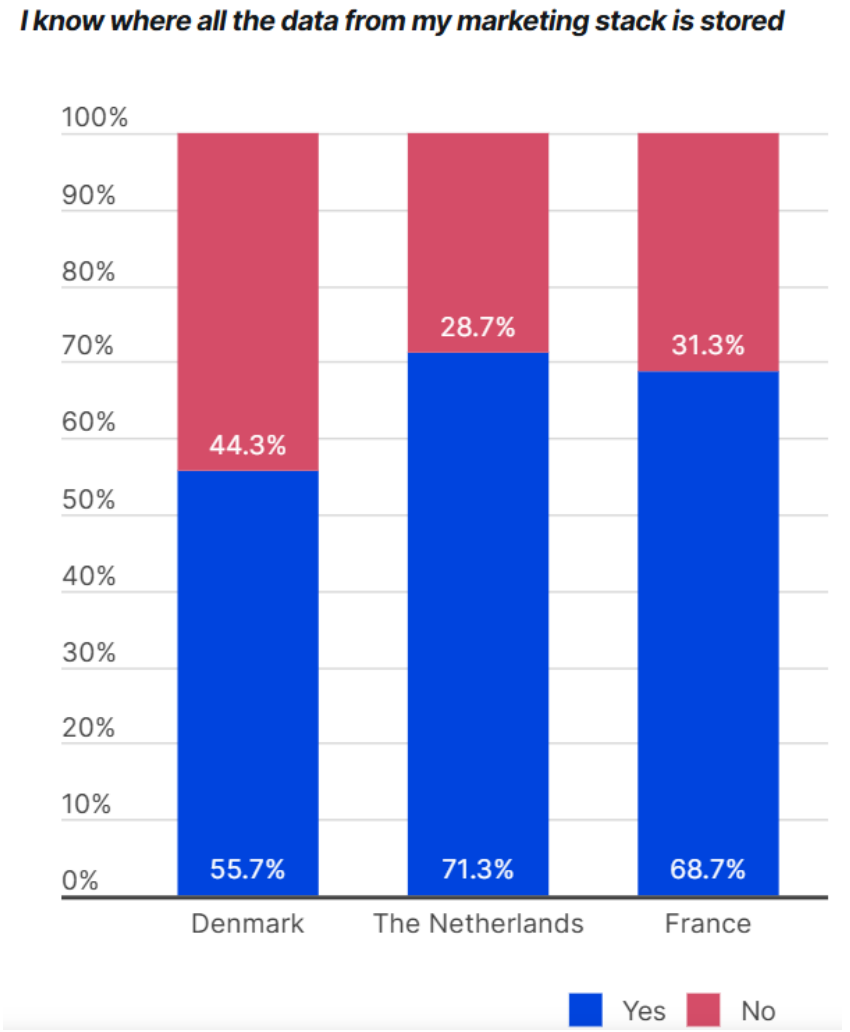
| | | | |
|---|---|---|---|
| 27/12/2023 | SOCIETE DE SUPPORT LOGISTIQUE | Défaut de base légale<br>Minimisation des données<br>Information des personnes et transparence<br>Défaut de sécurité des données | > Amende de 32 millions d'euros |

# Statistiques

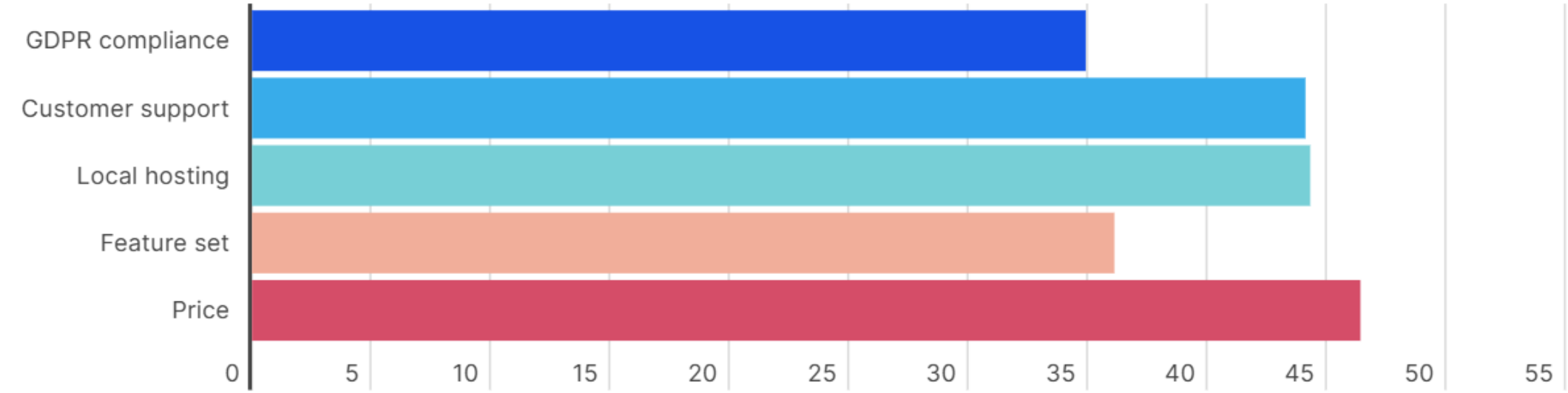
- 1000 personnes interrogées
- 70 % RGPD → attendent des décisions claires
- 74 % ont connaissance de « violations pertinentes » au sein de leur entreprise moyenne
- 61,5 % pourraient être dissuadés par des amendes conséquentes

« Max Schrems, président honoraire de noyb : "*Il est extrêmement alarmant de constater que 74 % des professionnels de la protection des données au sein des entreprises déclarent que les autorités trouveraient des violations importantes dans une entreprise moyenne. De tels chiffres seraient inimaginables s'il s'agissait de se conformer à la législation fiscale ou à la réglementation en matière de sécurité incendie. La non-conformité ne semble être la norme que lorsqu'il s'agit des données personnelles des utilisateurs.*" »

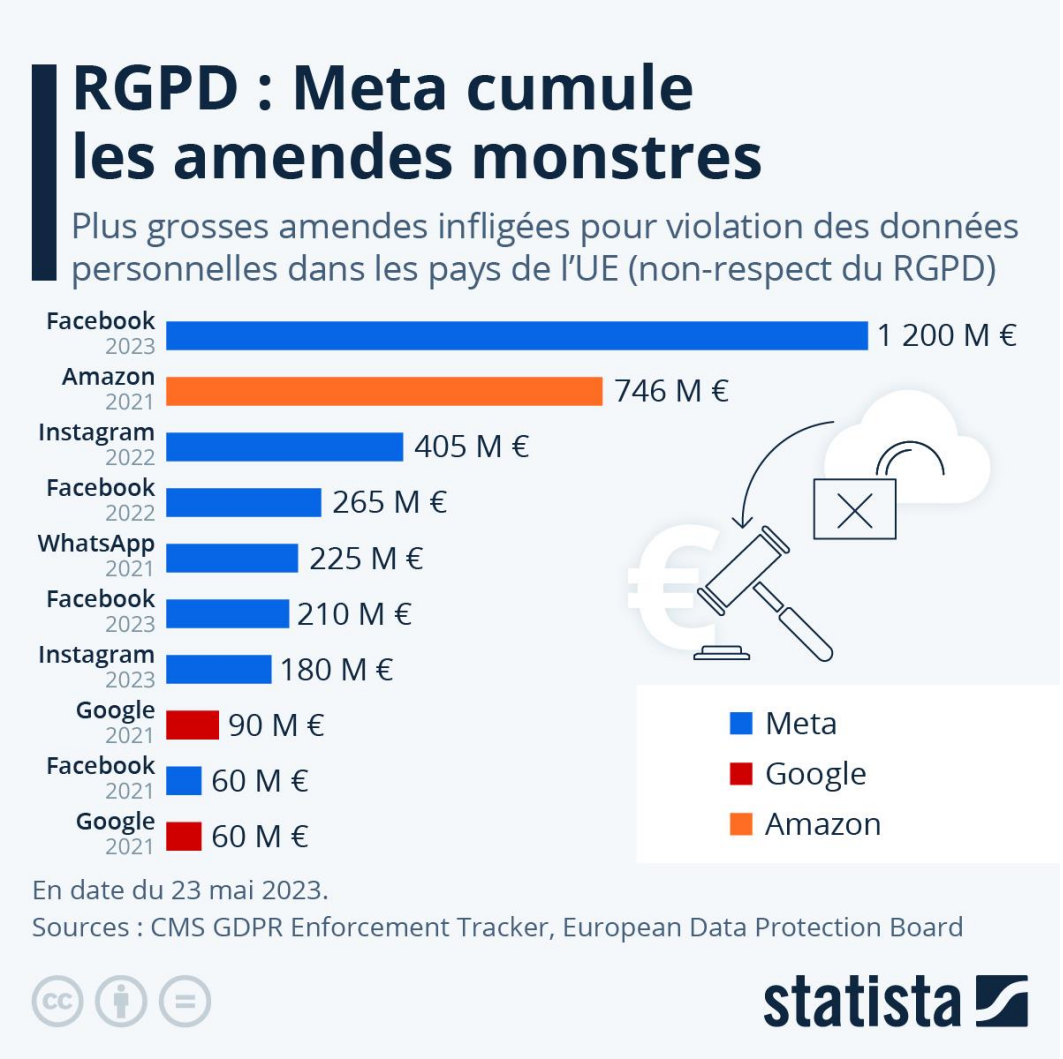
# Statistiques



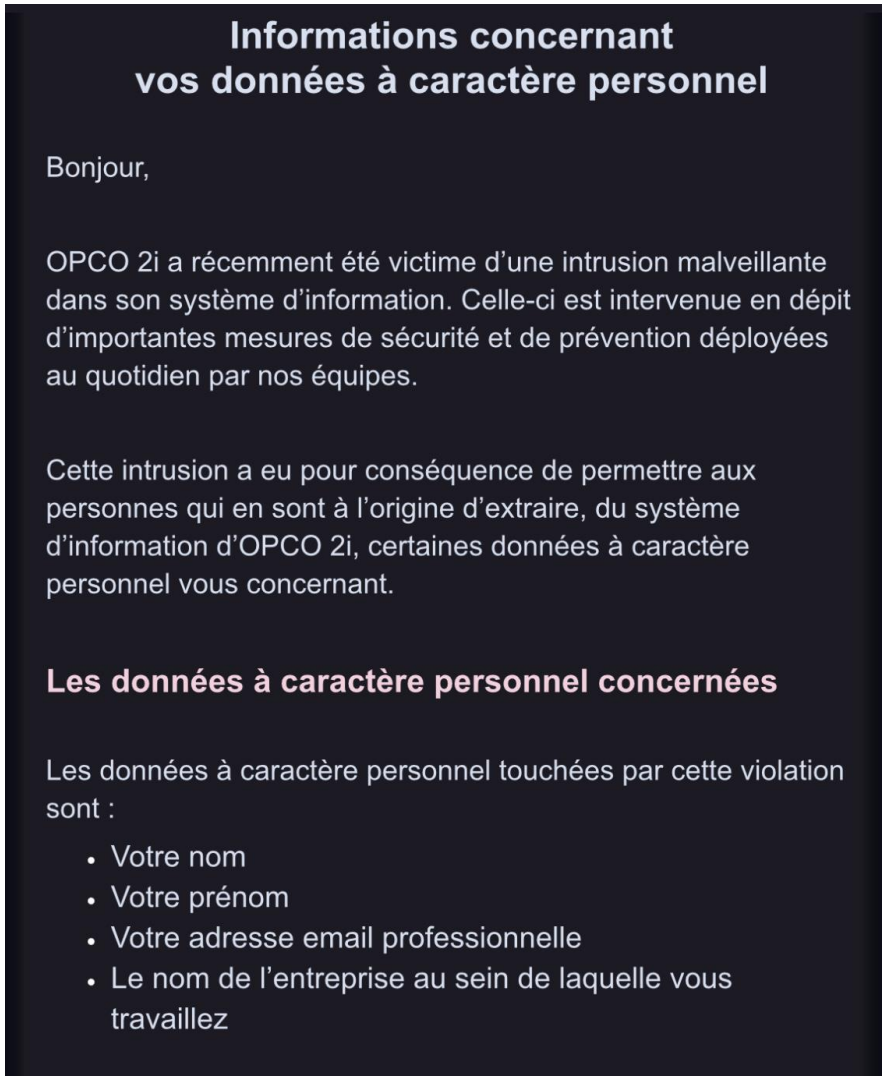
***What would motivate you to choose a European marketing platform over a big tech product?***



# Des amendes pour les GAFA



# Exemple 1 : Fuite de données personnelles



**Informations concernant vos données à caractère personnel**

Bonjour,

OPCO 2i a récemment été victime d'une intrusion malveillante dans son système d'information. Celle-ci est intervenue en dépit d'importantes mesures de sécurité et de prévention déployées au quotidien par nos équipes.

Cette intrusion a eu pour conséquence de permettre aux personnes qui en sont à l'origine d'extraire, du système d'information d'OPCO 2i, certaines données à caractère personnel vous concernant.

**Les données à caractère personnel concernées**

Les données à caractère personnel touchées par cette violation sont :

- Votre nom
- Votre prénom
- Votre adresse email professionnelle
- Le nom de l'entreprise au sein de laquelle vous travaillez

# Exemple 2 : Fuite de données sensibles

- 2024 : Change Healthcare, fournisseur de gestion des revenus et du cycle de paiement qui relie les payeurs, les fournisseurs et les patients au sein du système de santé américain a été victime d'une fuite de données sensibles.
- Type de données : noms, numéros de sécurité sociale, dates de naissance, adresses, et numéros dossier médicaux, ...
- Coût de la fuite : estimé à plus de 850 millions de dollars en amendes et compensations et chute significative du prix des actions suite à la divulgation de la fuite et une rançon payée (350 BTC ~ 25M de dollars).

# Merci de votre attention.

Paul DUCOLOMB

Firmin LAUNAY

Théophile REY