



1

— Tour d’horizon Privacy & Security
Privacy Watch 2021

Webinaire 04/02/2021

— data privacy & security — — www.dps.expert — **D_P&S**

2

noyb

Max Schrems

THE TECHNOLOGY THAT CONNECTS US ALSO CONTROLS US

the social dilemma

Tristan Harris

EUROPEAN DATA GOVERNANCE
A NEW APPROACH FOR THE DIGITAL DECADE

November 2020

Setting up a new European way of data governance will facilitate data sharing across sectors and Member States. It will create wealth for society, and provide control to citizens and trust to companies.

The economic value of data sharing

- Data access and reuse can generate social and economic benefits of 1% to 2.5% of GDP¹.
- The new measures could increase the annual economic value of data sharing by up to €7-11 billion by 2028².
- In addition, the new rules will have a wider impact on the EU economy and society as a whole.

€ 1.3 trillion in increased productivity in manufacturing through Internet-of-Things data by 2027³

€ 120 billion of savings per year in the EU health sector⁴

The EU will boost the development of trustworthy data-sharing systems:

- Empower Europeans to decide what happens to their data, and what data they would like to share with whom.
- Facilitate data altruism to make it easier and safer for companies and individuals to voluntarily make their data available for the benefit of society.
- Enhance the reuse of public sector data that cannot be made available as open data.
- Create new EU rules on neutrality to allow novel data intermediaries to function as trustworthy organisers of data sharing.
- Set up a European Data Innovation Board to steer data governance and prioritise standards.

1. OECD (2019), Enhancing Access to and Sharing of Data: Reaping Data and Benefits for Data Reuse across Sectors, OECD Publishing, Paris.
2. European Commission (2020), Support Study to the Impact Assessment accompanying the proposal for a Regulation on European data governance, SWD(2020)004, endorsed by Directors.
3. McKinsey (2020), Shaping the Digital Transformation of Europe.

3

Ransomware




TECHNOLOGIE

Pour la première fois, une attaque informatique a tué

Une femme est décédée à Düsseldorf, l'hôpital allemand ayant été paralysé par un rançongiciel, ou «ransomware». Un événement qui illustre la fragilité du secteur de la santé face à ces agressions

The New York Times

Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack

A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.

4

– Amendes RGPD



GBP 18,4 mio – ICO, UK
Manquement au devoir d'implémentation des mesures de sécurité.

Cyber attaque



EUR 35.3 mio – Hamburg
Pratiques illégales de surveillance du personnel.

Divulgateur accidentelle



EUR 525/m – Hollande
Vente illégale de données de ses membres.

Plainte

D_

5

– RGPD amendes



EUR 250/m – cnil, FR **3 mois** délai pour mise en conformité, 250 / j. retard

Manquement à la minimisation des données

Manquement à l'obligation de minimisation de conservation

Manquement à l'obligation d'information des personnes concernées

Manquement à l'obligation d'assurer la sécurité

Audit

D_

6



— Révision totale LPD

Privacy Watch 2021

Webinaire 04/02/2021

data privacy & security www.dps.expert D_P&S

7

— Sur le fond...

- **Traitement est présumé licite si conforme aux principes.**
 - Consentement requis pour traitement de données sensibles.

- **Traitement licite uniquement si base légale applicable:**
 - Consentement
 - Contrat
 - Obligation légale (du responsable de traitement)
 - Intérêts vitaux (de la personne concernée)
 - Intérêt public ou relevant d'une autorité
 - Intérêt légitime du responsable de traitement

D_

8

– Votre entreprise est-elle concernée ?



Oui, si:

- Traitements de données personnelles en Suisse
- Traitements de données personnelles hors de Suisse déployant des effets en Suisse.

D_

9

– Quels types de données sont concernées ?



- Données personnelles**
 - Personne physique identifiée ou identifiable
- Données personnelles sensibles**
 - Opinions ou activités religieuses, philosophiques, politiques ou syndicales
 - Santé, sphère intime, origine raciale ou ethnique
 - Données génétiques
 - Données biométriques
 - Données sur poursuites, sanctions pénales ou administratives
 - Données sur des mesures d'aide sociale


D_

10

- Faîtes-vous du profilage ?



- Profilage**
 - Traitement automatisé permettant d'évaluer certains aspects personnels relatifs à une personne physique

- Profilage à risque élevé** 
 - Traitement entraînant un risque élevé pour la personnalité ou les droits fondamentaux parce qu'il conduit à un appariement de données qui permet de d'apprécier les caractéristiques essentielles de la personnalité.
 - Requier le consentement explicite de la personne concernée.

D_

11

- Vos données sont-elles sécurisées ?



Responsables de traitement et sous-traitants doivent assurer la sécurité de leurs traitements

- Mesures de sécurité organisationnelles et techniques appropriées au risque

- Protection des données dès la conception et par défaut

D_

12

- Les données sont-elles sous-traitées ?



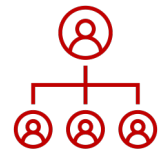
Sous-traitance autorisée pour autant qu'un contrat ou la loi le prévoit et à condition que :

- Seuls sont effectués les traitements que le responsable serait en droit d'effectuer lui-même.
- Aucune obligation légale ou contractuelle de garder le **secret** ne l'interdit.

D_

13

- Qui est responsable au sein de l'entreprise ?



Les responsables de traitement privés peuvent nommer un conseiller à la protection des données

- L'entreprise a-t-elle désigné un conseiller à la protection des données ?
- L'indépendance du conseiller est-elle garantie et ses obligations sont-elles clairement définies ?



<https://blog.unidistance.ch/quel-est-le-role-dun-data-privacy-officer-petit-guide-pratique>

D_

14

_ Tenez-vous en registre des activités de traitement ?



Nouvelle obligation pour les responsables de traitements et les sous-traitants

- Registre incluant l'identité du responsable de traitement, la finalité, les catégories de données, les destinataires, le délai de conservation, les mesures de sécurité, l'indication de l'Etat destinataire en cas de transfert à l'étranger.

D_

15

_ Qui doit désigner un représentant ?



Nouvelle obligation pour les responsables de traitement domiciliés à l'étranger si le traitement

- Est en rapport avec l'offre de biens ou services ou le profilage de personnes en CH
- Est régulier ou à grande échelle
- Présente un risque élevé

D_

16

_ Que faire en cas de transfert à l'étranger ?



Bases légales

- Décision d'adéquation du CF
 - Binding Corporate Rules (BCR)
 - Standard Contractual Clauses (SCC)
- Dérogations (art. 17)

D_

17

_ Devoir d'informer, quelles mesures ?



Extension & précision des obligations de transparence pour les responsable de traitements

- Déclaration de confidentialité contenant au minimum
 - Identité et coordonnées du responsable de traitement
 - Finalité du traitement
 - Destinataire(s) ou catégories de destinataires
- Communication à l'étranger
- Décision individuelle automatisée

D_

18

_ Quand faut-il faire une étude d'impact ?



Nouvelle obligation en cas de traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux

- Traitement de données sensibles à grande échelle
- Surveillance systématique du domaine public
- Description du traitement envisagé
- Evaluation des risques
- Evaluation des mesures de sécurité
- Documentation + registre PIA

D_

19

_ Annonce des violations de la sécurité

Nouvelle obligation du responsable de traitement

- Notification au PFPDT **dans les meilleurs délais**
- Nature de la violation, conséquences, mesures prises ou envisagées
- Informe les personnes concernées si nécessaire ou si le PFPDT l'exige

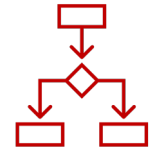
Nouvelle obligation du sous-traitant

- Notification au responsable de traitement **dans les meilleurs délais**



20

_ Comment traiter le droit d'accès ?



Disposons-nous de processus internes permettant de répondre efficacement aux demandes suivantes ?

- Droit aux informations et à la transparence
- Droit à la rectification
- Droit à l'oubli
- Droit à la portabilité des données

D_

21

_ Conclusion

Nos données sont elles correctement protégées ?

Conforme RGPD 🕶️

Au travail... 🕒

D_

22

Conseil

Privacy

- Legal mapping
- Data mapping
- Registre de traitement
- Etude d'impact
- Transparence & exercice des droits

&

Security

- Audit
- Data Privacy by Design & Default
- Plan de réponse en cas d'incident
- Data centric security
 - DLP, chiffrement, cloud

- Formation / sensibilisation du personnel

23

Mandats

- DPO
 - CIO
 - CSO
- } As a Service

Conseil d'administration

- ✓ Digital transformation
- ✓ Ethique digitale
- ✓ Dynamique du changement



24