Why GDPR?

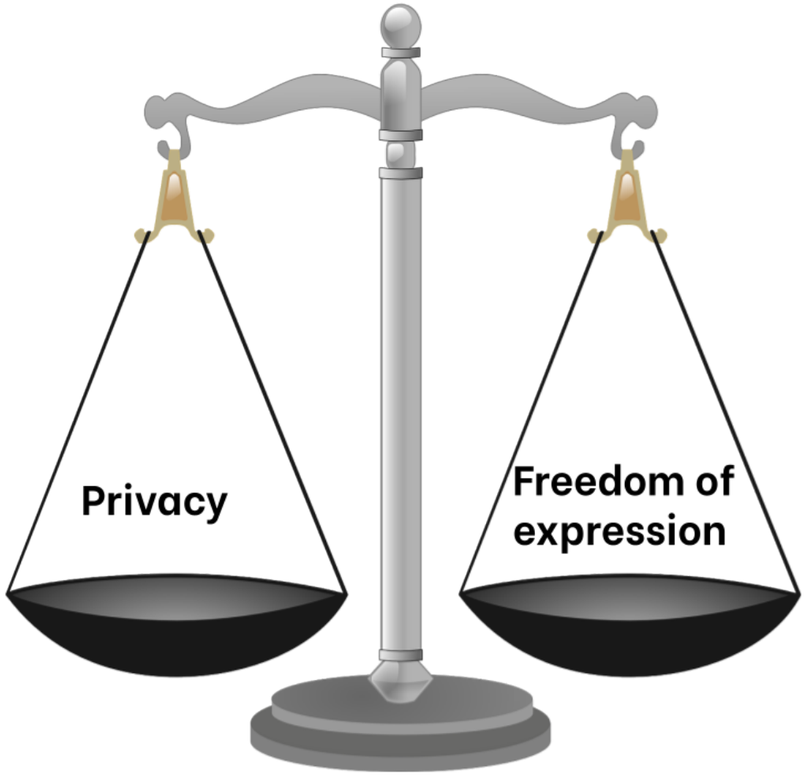
UNDERSTANDING GDPR

Shalini Kurapati, CIPP/E
Co-founder, Clearbox AI

Course overview

- GDPR context
- Principles, roles, responsibilities, and data subject rights
- Legal grounds/basis, data subject rights, storage and transfers outside of the EU
- Security of processing, privacy by design
- GDPR and Artificial Intelligence

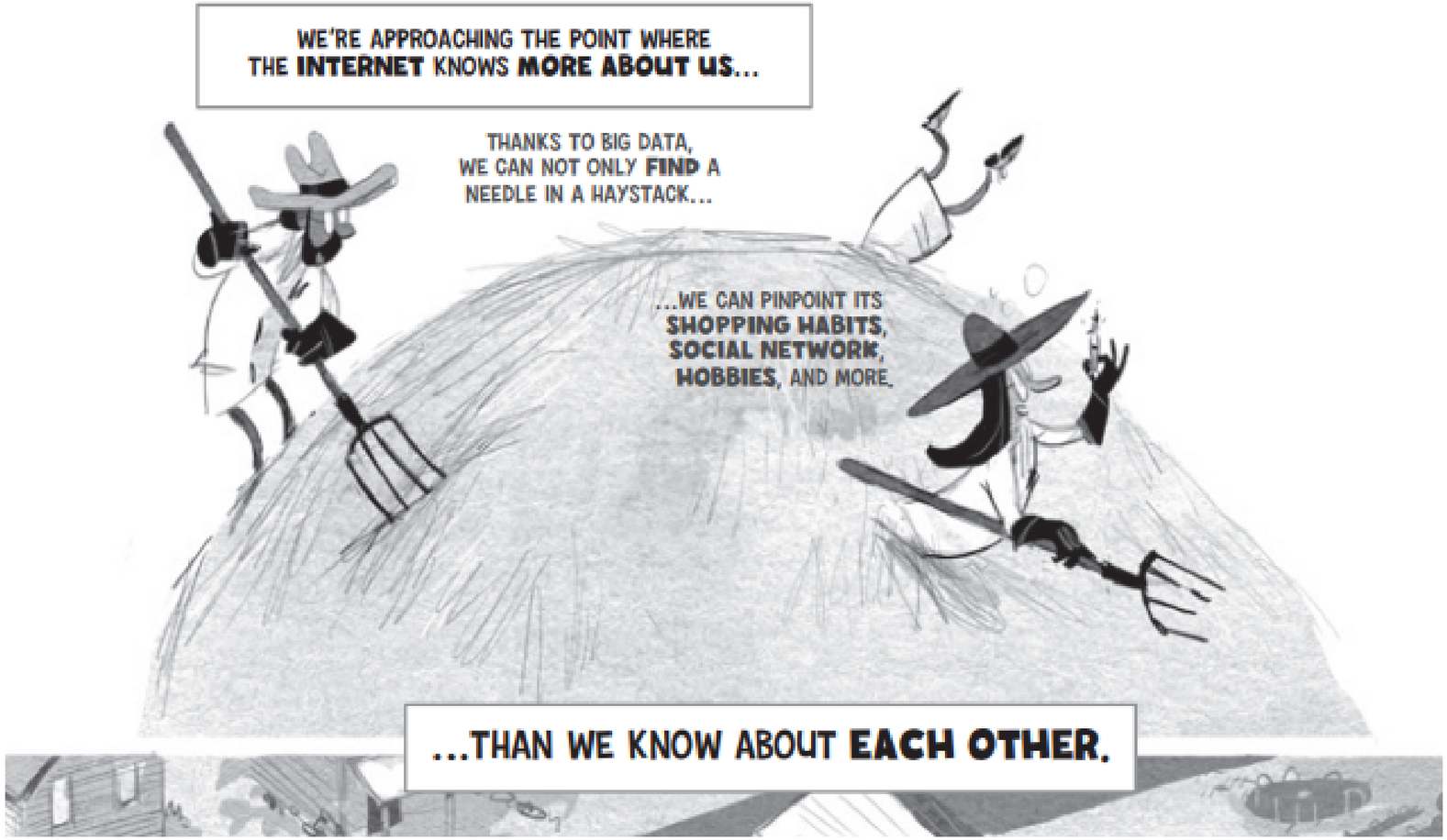
Why do we need laws like GDPR?



- General Data Protection Regulation of the EU, since 25 May 2018

- Other data protection laws and directives before GDPR
- Privacy versus freedom of expression: Proportionality
- Right to privacy: human right, control over information
- Growth of trade, exchange of goods, services, and data

Privacy in the digital age



[1] European Data Protection Supervisor, Klein, G., Bauman, Y., The European Data Protection Supervisor presents the cartoon introduction to digital ethics, Publications Office, 2018, https://data.europa.eu/doi/10.2804/534765

Why is it special?

- Replaces national laws on data protection in EU
- Iceland, Norway and Liechtenstein (in EEA) also fully adopted GDPR
- Harmonized set of rules for data protection
- To compare: the US has more than 51 laws on the topic

[1] Council of the European Union, The Member States of the European Union, Publications Office, 2020, https://data.europa.eu/doi/10.2860/082123 [2] www.ncsl.org

GDPR: The key features

- Regulation to protect human rights in the digital age
- Harmonized rules to avoid confusion for businesses
- Global scope: to do business with EU/EEA citizens
- Increased transparency and client trust

Let's practice!

UNDERSTANDING GDPR

What is GDPR?

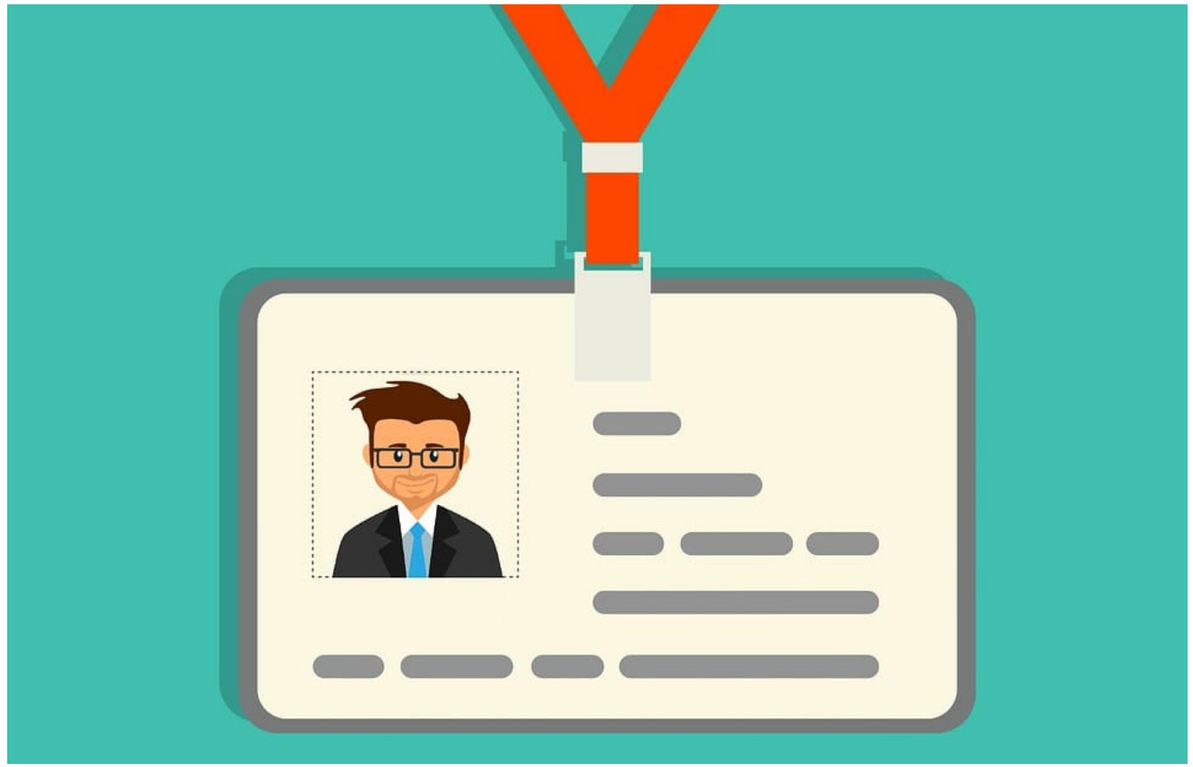
UNDERSTANDING GDPR

Shalini Kurapati, CIPP/E
Co-founder, Clearbox AI

GDPR scope

- Covers people and companies in the EU
- Global scope: Data of EU citizens
- Personal data:
  - processed by automated means
  - manual: part of a filing system
- Belongs to natural persons/ data subjects

Personal data under GDPR



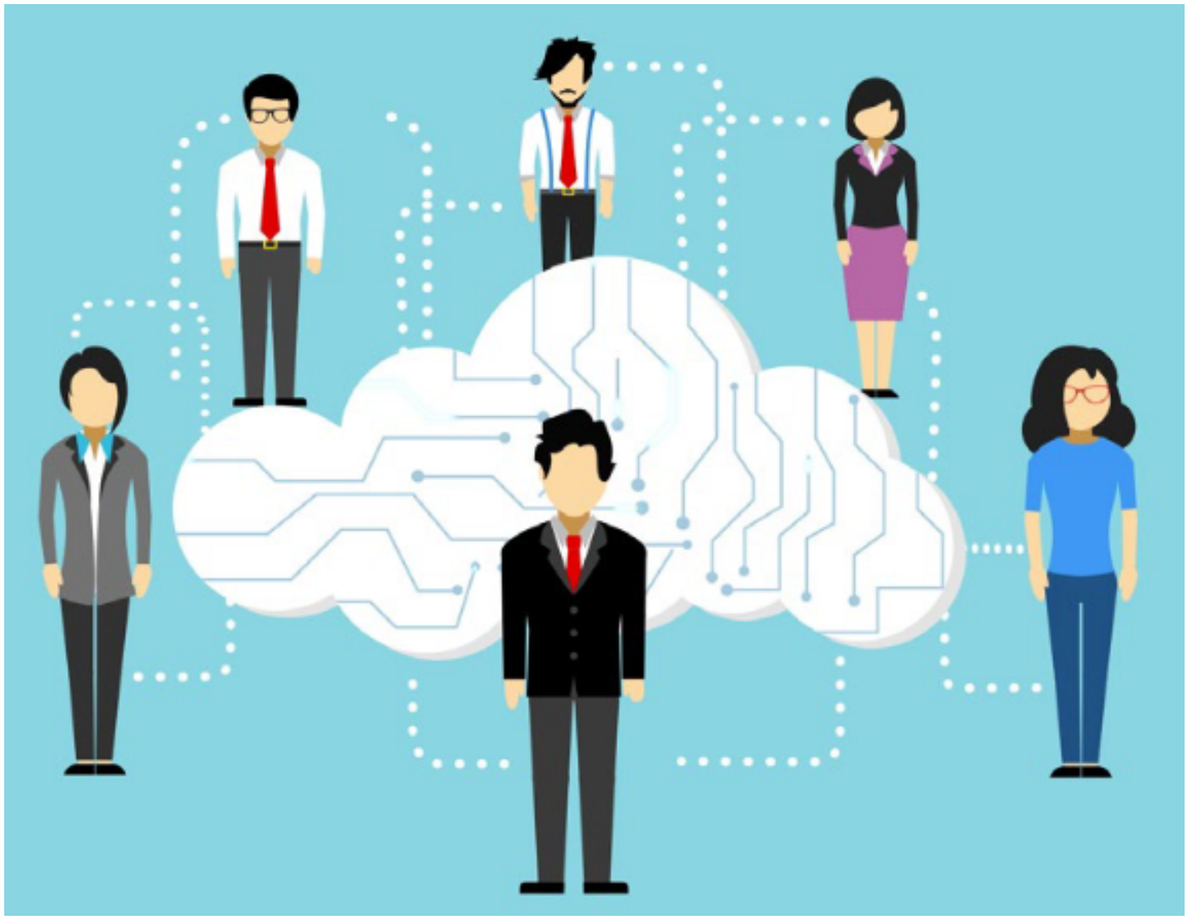
- Identified or identifiable: directly or indirectly
- Natural person or the data subject
- Names, photos, SSN, and unique ids etc.
- Cultural identity, socio-economic status etc.
- Special categories

[1] GDPR text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (http://data.europa.eu/eli/reg/2016/679/oj)

Special categories

- Highly sensitive data
- Types:
  - Health, biometric data
  - Sexuality and sexual orientation
  - Criminal records
  - Religious beliefs, political affiliations, union memberships
  - Vulnerable groups, children under 13
- Special considerations including additional obligations

Data processing



Activities include: Collection, organization, analysis, storage, sharing, retrieval, erasure, and many more.

Examples include:

- Video recording/CCTV cameras
- Sharing or selling personal data
- Payroll/HR
- Accessing databases
- Shredding

[1] Documenting data processing:The EDPS guide to ensuring accountability, doi:10.2804/717377

What the law says

- Don't process personal data
- Unless you have a legal basis (Article 6)
- Follow GDPR principles (Article 5)
- Ensure data subject rights (chapter III, articles 12-21)
- Sensitive data: extra measures
- Data Protection Impact Assessment
- Don't worry; we will clarify these articles in chapter 2

[1] GDPR: Regulation (EU) 2016/679 http://data.europa.eu/eli/reg/2016/679/oj

GDPR fines

- Fines are deterrents for non-compliance
- Up to €20,000,000 or 4% of turnover, whichever is higher
- Roles, responsibilities and enforcement

Let's practice!

UNDERSTANDING GDPR

Who is responsible?

UNDERSTANDING GDPR

Shalini Kurapati, CIPP/E
Co-founder, Clearbox AI

Key GDPR roles

- Data controller
- Data processor
- Data Protection Officer or DPO
- Supervisory Authority (SA)/ Data Protection Authority(DPA)

Data controller

- Decides data processing purposes and means
- Joint decisions means joint controllers
- Ultimately accountable

Example: boutique pastry shop outsources payroll management

- Data controller: Boutique shop
- Data processor: Payroll company

Data processor

- Usually, a third party/sub-contractor who processes personal data on behalf of the controller
- No direct responsibility
- Terms agreed by Data Processing Agreement
- Align with controller obligations for compliance

Data protection officer or DPO

- Monitors, advises, helps comply
- Cooperation with SA and contact point
- Both controllers and processors
- Mandatory for:
  - Public bodies
  - High risk processing
- Risk matters, not company size

[1] Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)

Supervising authority or data protection authority

- Independent public authority
- Fines for non-compliance
- All members have a SA/DPA
  - *Garante per la Protezione dei Dati Personali* (ITA)
  - *Autoriteit Persoonsgegevens* (NL)

[1] https://edpb.europa.eu/about-edpb/about-edpb/members_en

Data breaches: what to do?

What is a data breach?

- Loss, unlawful access or disclosure
- Confidentiality, integrity, availability

What to do?

- Notify SA/DPA without delay
- Within 72 hour window
- If high risk inform data subjects, follow-up actions

Example: Online marketplace hacking

- DPO: important role
- Record of data breaches
- Data breach policy

[1] Guidelines on personal data breach notification under regulation 2016/679, WP250 rev.01

Coordination across countries

- Consistent application of rules
- Cooperation across members
- EU27 Supervisory Authorities
- EDPS, European Data Protection Supervisor
- Iceland, Norway, and Liechtenstein have no voting rights

[1] https://edpb.europa.eu/about-edpb/about-edpb/members_en

Let's practice!

UNDERSTANDING GDPR