

European digital policy: fostering the European data economy

Introduction

- After missing the first digital revolution, Europe is becoming a regulatory leader in digital policy.
- GDPR, personal data and the right to privacy
- Data flow for growth
- Data access and reuse
- The next big thing: the AI revolution and how not to miss it

GDPR: a privacy revolution

What is GDPR

- The General Data Protection Regulation (GDPR) is giving back control of their personal data to individuals.
- Applicable since 25 May
- Directly applicable
- Establishes high level of protection for personal data, making the EU a pioneer in this field and having a direct impact on any undertaking using personal data of clients located in the EU.
- Aim: bringing back trust in digital services and products.

To whom does it apply

- Any establishment (undertaking, organisation) processing data in the context of an activity in the EU.
- Any processing of personal data linked to an individual in the EU
 - **Any foreign company processing personal data of clients located on EU soil is subject to the Regulation.**

What is a personal data?

*“Any information relating to an **identified or identifiable natural person** (‘data subject’); an identifiable natural person is one who **can be identified, directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”*

- Even an IP address can be considered a personal data.

Main principles: consent and transparency

- Personal data shall be “processed lawfully, fairly and in a transparent manner”
- Consent of the data subject must be free, informed & unambiguous (opt-ins). It can be withdrawn.
- Consent must be given after the data subject has been informed of which data will be processed, when, why and for how long.
- Terms of processing must be understandable, clear and simple.
- The data subject has rights to access, modify, limit & delete his data.

Main principles: proportionality and security

- Proportionality: data processing must be adequate, relevant and limited (including in time) to what is necessary.
- Security: the processing must guarantee the security of personal data. It implies privacy and cybersecurity measures to be implemented.

Sanctions

- Up to 10 million € or 4% of global turnover (whichever is higher)
- + class action by consumer organisations



"Before I write my name on the board, I'll need to know how you're planning to use that data."

A legal framework for non-personal data: the next frontier

Non-personal data flow, access and reuse for growth

According to a study by data analyst IDC

- European data economy in 2015 = 272 bn € → 1,87% of GDP
- If right reforms adopted 643 bn € by 2020 → 3,17% of GDP

The free flow of non-personal data: the 5th freedom of movement?

- European Commission regulation proposed in September 2017
- Free flow of personal data provided for in GDPR, soon to apply to non-personal data
- Forbids Member states to keep unjustified data localisation requirements.
- Only exception: public security

The free flow of non-personal data: data portability

- A self regulatory code of conduct adopted by the industry should allow businesses to know in advance:
 - Where their non-personal data will be stored
 - Under which format
 - How much it would cost and how long it would take to change data service provider (storage, analysis)

Data access and reuse for growth

The European Commission's 3rd data package

- Proposed in April 2018
- Revision of the directive on the reuse Public Sector Information (PSI)
 - Provides conditions under which non-personal data already opened by public bodies and public undertakings can be accessed and reused.
 - Public bodies & undertakings must give access to their dynamic data via APIs.
 - Public undertakings are banned from taking part in exclusive agreements and similar measures regarding access to their data. i.e. they cannot provide data to an undertaking while restricting access to these data to other undertakings.
 - The European Commission will be able to adopt delegated act that provides lists of data sets (among documents to which the directive applies) that must be opened free of charge.

The European Commission's 3rd data package

- A communication and a guidance document addressing B2B (business-to-business) and B2G (business to government) data sharing
 - European Commission encouraging sectorial self-regulations, in particular through code of conducts.
 - Codes of conducts can be purely voluntary and non-binding, or created under the initiative of the Commission with a more constraining effect.
 - If this soft law approach is insufficient, the European Commission leaves all options open to propose legally binding texts.

The next big thing: the AI revolution and how not to miss it

The European strategy for artificial intelligence

- Investments and public support: EU funding for research & innovation, access to AI solutions for non-specialised bodies (creation of AI-on-demand platform, Digital Innovation Hubs, industrial data platforms).
- Education & digital skills: fostering digital training in Member States and dialogues between public authorities and social partners on the consequence of digitisation, robotization and AI for the job market.
- Regulation of emerging issues: ethical and responsibility problems arising from automated machinery, vehicles and decision-making software.
- Access to data: see 3rd data package.

Thank you for your attention!