Working group 21:

Protecting and promoting privacy in our data-driven societies

Background

We are in the middle of a major transformation in our society. Data and personal data, may be the new oil, but they also need protecting. Economy, science, public administrations, the way individuals communicate and build relations with each other, all produce, and need, vast amounts of data to offer personalised services and products.

Big data and the Internet of Things are the new paradigms based on interacting systems – for example, drones, autonomous vehicles and wearable cameras. These systems, alongside other sources – such as social networks, online platforms and databases – produce a huge amount of data which, when combined and then processed by big data analytics, can lead to unprecedented possibilities to give insight into individuals' behaviour, influence decisions on individuals and adversely impact their participation in society.

New technologies may change perceptions of privacy and serve our need to interact with others. However, this does not mean that individuals have per definition and consciously aborted the control over their data, practically over themselves and their right to an equal, non-discriminatory treatment. Nor have they consented to being subjected to constant surveillance. These technologies thus provide numerous opportunities for society. At the same time, it shall remain a society of values, as the EU Charter of Fundamental Rights prescribes.

The EU has committed itself to a high level of data protection, as demonstrated by case law of the Court of Justice of the EU and the new data protection rules. From 2018 onwards, these rules will apply to all data controllers and processors established in the EU or those that provide services to individuals residing in the EU. In the interim, regulators and data controllers should clarify how the regulation should work in practice, especially regarding thoroughly assessing privacy risks and ensuring compliance with the rules. Non-bureaucratic, creative, innovation-friendly solutions that respect and promote human dignity and consider the risks for individuals and society at large will therefore be needed.

Objectives

This workshop explored the fundamental rights implications of protecting and promoting respect for private life and the protection of personal data in our data-driven societies, as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights. Based on concrete examples, it aimed to raise awareness of the recent reforms of the EU's data protection rules and provided a platform for exchanging ideas and opportunities for applying good practices. The workshop will also feed into FRA's current and future work on data protection and new technologies.

Speakers

- Peter Hustinx, former European Data Protection Supervisor
- Marju Lauristin, Member, European Parliament
- Giuseppe Busia, Secretary General, Italian Data Protection Authority
- Bojana Bellamy, President of the Centre for Information Policy Leadership, Hunton & Williams
- Sarah Spiekermann, Institute for Management Information Systems, Vienna University of Economics and Business
- Thomas Zerdick, Deputy Head of Unit, Personal Data Protection Unit, Directorate-General Justice and Consumers, European Commission
- Zoe Kardasiadou, Data Protection Expert, FRA

Main messages

1. The focus should be on protecting people, not data. Participants called for responsible innovation and a value-based, human-centred design of personal data processing; and noted that the common good should not downplay individuals' rights.
2. Transparency of data processing is key for empowering individuals.
3. There is a need for targeted education and awareness raising; specifically, for business and IT engineers on human rights, and for rights holders and other stakeholders on the risks associated with data processing.
4. The new data protection framework is already adopted. This makes the right to privacy a reality for all and will require a multi-layered approach by the various stakeholders (business, data protection authorities, governments, civil society, EU institutions).

Next steps

- Data controllers (e.g. business) should make information easily accessible and intelligible for users. A so-called 'traffic light system' can help make risks and processing activities easily to understand. This system should be common for all, i.e. transnational. The European Commission could contribute to a harmonised traffic light system.
- Accountability goes beyond mere compliance. To this end, the business sector (managers/organisations) should embed innovative and values-driven thinking in business organisations instead of being just profit driven.
- Trust in new technologies is key. Effective data protection should be promoted as a competitive advantage. Regulators and business should build upon this point, including raising the issue in the context of awareness-raising activities.

- Certification and privacy seals create incentives for the business sector to make privacy a competitive advantage. Regulators, the European Data Protection Board, and Member States (governments) should support such efforts.
- The EU (the Commission) should develop common standards with respect to privacy-by-design.
- The EU (the Commission) should fund research by academia and NGOs on people's perception of privacy risks and harms, and how data are used by the markets.
- Regulators should engage in constructive dialogue with business and civil society.
- Member States should empower privacy associations that can promote rights' enforcement, and individuals should help further build such associations.
- Data protection authorities, the European Data Protection Supervisor and the business sector should translate the EU's new General Data Protection Regulation into an easy-to-use checklist, accompanied by best practices. FRA should contribute by collecting best practices.
- The business sector should empower data protection officers (DPOs) through training and by making their position more strategic rather than just acting as compliance officers. Instead of having one DPO, data protection teams could be set up, with members having different skill sets and backgrounds.
- Member States and business should promote targeted and multi-layered education and awareness raising. Privacy and fundamental rights should be mainstreamed into university curricula for IT engineers and other professional groups.