Fundamental Rights Forum
connect.reflect.act

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Working group 27:

Respecting privacy rights in the commercial use of personal data

Background

Technological developments, such as the Internet of Things and Big Data, are at the heart of the data-driven economy. They boost innovation and create vast opportunities for growth according to the EU's Digital Single Market Strategy. Digital services transform our society and become personalised; this very often requires the collection and further processing of personal data. Similarly, scientific research benefits from the use of big data to establish correlations. The high level of personal data protection in the EU, and the other fundamental values with respect to dignity and non-discrimination, requires business to implement practices in compliance with these rules. Compliance, flexibility, creativity and respect for the individual are pivotal for sustainable growth. The UN Human Rights Council and the Council of Europe have endorsed the responsibility of business, as an organ of our society, to uphold fundamental rights, including respect for the protection of personal data. The Digital Single Market Strategy builds upon trust in digital services as a condition for their growth.

By mid-2018, the data-driven economy should have implemented the new data protection rules. The main aspects of these rules are well-known principles, such as purpose limitation and data minimisation; informed consent; privacy by design and by default; and individuals' rights. They also include new pivotal aspects, such as accountability by data controllers and data processors, the data protection impact assessment, the right to data portability and the right to be forgotten. All these require technical and organisational solutions, adapted to the new technologies, and include the continuous monitoring of risks due to technological developments.

Finally, child protection is a particular area that needs responsible data handling by the business sector. The new data protection rules cover parental consent for children between the ages of 13 and 16. The EU Strategy for a Better Internet for Children, as adopted by the European Commission in 2012, covers the creation of a safe environment for children through age-appropriate privacy settings and wider use of parental controls.

Objectives

This workshop sought to explore how the business sector can contribute to a sustainable data-driven economy. It looked at how business can grow and innovate in a fundamental rights-compliant manner and promote our common values based on dignity and non-discrimination. In reference to promoting respect for private life and protection of personal data, as enshrined in Articles 7 and 8 of the EU's Charter of Fundamental Rights, the

workshop aimed to raise awareness about the EU's recently-released data protection rules and provide a platform for exchanging ideas for good business practices. It will also feed into FRA's current and future work on data protection and new technologies.

Speakers

- Bojana Bellamy, President of the Centre for Information Policy Leadership, Hunton & Williams
- Athena Bourka, ENISA
- Lucy Purdon, Project Manager, Institute for Human Rights and Business
- Marit Hansen, Commissioner of the Data Protection Authority of Schleswig Holstein
- David Wright, Founder and Managing Partner of Trilateral Research and Consulting
- Stephen Deadman, Facebook, Deputy Global Chief Privacy Officer
- Diego Naranjo, Advocacy Manager, European Digital Rights
- Zoe Kardasiadou, Data protection expert, FRA

Main messages

1. Data protection is not about protecting data, but about protecting people.
2. There is no need for trade-offs between privacy and data-driven businesses.
3. Trust is essential for doing business, and is based on transparency and user control.
4. Companies need further incentives to promote privacy.
5. Business should engage in accountability-"plus", which builds upon ethical considerations (e.g. risk analysis is not limited to privacy, but includes risks to human dignity, non-discrimination, equality, etc.).

Promising practices

- The Binding Corporate Rules for data transfers to third countries within the framework of the EU's current Data Protection Directive 95/46/EC. This successful practice has been recognised as a legal instrument for data transfers in the General Data Protection Regulation. Main actors include businesses and Data Protection Authorities (DPAs).
- Compass – an online tool available for business to self-assess their compliance with data protection rules (supporting awareness raising), Danish Ministry of Business.
- Google's advisory board to deal with the CJEU Google case on the right to be forgotten.
- Training for smaller companies by big companies. Mastercard was cited as an example.
- Businesses have published reports on governmental requests to access personal data (transparency reports). Examples include Facebook, Google, Vodafone, and Microsoft.

Next steps

- For businesses, privacy by design should not be a merely technical process, but should allow for strategic changes in companies and continue throughout the life-cycle of data processing activities.
- Businesses should switch from classic data security objectives to ethical objectives, i.e. include transparency, intervenability and unlinkability as additional objectives to confidentiality, integrity, availability.
- Businesses should include ethical aspects in data protection impact assessments (DPIAs).
- National DPAs should conduct random audits of companies' DPIAs.
- National DPAs should showcase best practices as an incentive for other companies.
- EU institutions and Member States (DPAs) should foster harmonisation of DPIAs by way of guidelines.
- Businesses should foster transparency and accountability by publishing information on DPIAs and privacy processes in place.
- EU institutions, Member States, businesses, and academia should work on making certification/privacy seals a reliable tool for the benefit of individuals.
- Large companies, EU institutions and Member States (DPAs) should develop guidelines on compliance with the General Data Protection Regulation to assist SMEs.
- European institutions should promote training to assist SMEs in complying with the General Data Protection Regulation.
- EU institutions, Member States, businesses, and academia should assess privacy tools and do more research on what works.
- EU institutions, Member States, businesses, and academia should work on visualisation of information to be provided to individuals.
- With respect to parental consent, businesses should implement technical measures that can work in practice, i.e. are easy to use and accessible to all. EU institutions should develop guidelines for data controllers on the appropriate level/granularity of consent. Member States should educate parents to strengthen their data literacy.
- Businesses should get involved in educating parents.
- Businesses should ensure consent in cases where the terms of use regarding personal data are amended.
- FRA should map best practices in Member States.