Skip all front matter: Jump to Page 1 ▼

RAND EUROPE

Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies

Neil Robinson, Jan Gaspers

Sponsored by Microsoft Europe

The research described in this report was sponsored by Microsoft Europe.

RAND OFFICES
SANTA MONICA, CA • WASHINGTON, DC
PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA
DOHA, QA • CAMBRIDGE, UK • BRUSSELS, BE
www.rand.org • www.rand.org/randeurope

Summary

This study examines the legal and policy frameworks that govern and regulate the use of information and communications technology (ICT) by European Union (EU) institutions and agencies. Specifically, it maps and reviews these frameworks in terms of the extent to which they account for information security and data privacy.

The study pursues a two-fold research approach. First, it offers a largely descriptive account of the existing legal and policy frameworks that govern and regulate the use of ICT by EU institutions and agencies, summarising in particular those legal provisions and policy documents that address information security and data privacy issues.

Second, the study offers some general observations based on the summary of legal and policy frameworks that regulate and govern the use of ICT by EU institutions and agencies. Significantly, these observations are neither intended to amount to a comprehensive analysis of existing EU legal and policy instruments on information security and data privacy, nor are they meant to provide any recommendations for EU policy-making. Instead, they aim to build a general understanding of the way in which relevant EU legal and policy frameworks might affect the adoption of new technologies by EU institutions and agencies. More fundamentally, it is hoped that by mapping and summarising, in an accessible format, the canon of relevant EU legal and policy frameworks, this study will create a greater awareness of the conditions under which ICT is used within EU institutions and agencies.

The first set of findings is presented in Chapter 2, which shows that the specific ICT usage requirements of different EU institutions and agencies also impose specific information security and data privacy requirements on ICT infrastructure. These ICT usage requirements relate to a wide range of different policy domains, including:

- Support to information exchange and cooperation between Member States on EU internal policies with external components (such as the internal market, customs, etc.).
- Big data challenges relating to the collection and processing of geospatial imagery data.
- The processing of police and criminal justice data.
- The protection of classified information in multinational environments.

While vital EU ICT infrastructure (such as sTESTA, OPSWAN and SIS II) has specific in-built resilience frameworks, it often lacks in security incident notification mechanisms.

More generally, Chapter 2 finds that legacy equipment, path dependency when it comes to law and policymaking, and the natural conservativeness of a large and complex administrative machine may act as inhibitors to building greater information security in EU institutions and agencies.

Examining legal and policy frameworks that govern and regulate the use of ICT across EU institutions and agencies, Chapter 3 finds that:

- The overall tone of EU policy and legal frameworks governing and regulating information security resonates with a model of security based on an internally secure organisation and insecure external environment, which appears to be inconsistent with the latest evolving canon of best practice concerning inter-organisational security, as, for example, codified by the International Standards Organisation.
- Key EU information security and data protection frameworks would appear poorly aligned with many modern models of technology service delivery and use, including cloud computing, the consumerisation of IT ('bring your own device'), service-orientated architectures (SoA), and an open model of IT services mediated through cyberspace. For example, although the e-Commission Communication flags up the involvement of the European Commission in the Cloud Computing Strategy, it is not clear that existing security frameworks are also aligned.
- The potential for security and privacy requirements to be built in from the start through Security Engineering or Privacy by Design principles appears to have little visibility in many of the EU legal and policy frameworks this study covers.

Mapping legal and policy frameworks, which cover policy domains that are unique to EU institutions and agencies, such as the management and processing of sector-specific data, the processing of personally identifiable nominal data for intelligence, border management and criminal justice cooperation, or the processing of sensitive classified information for EU-led crisis management operations, Chapter 4 reveals that:

- There is a complex landscape of very specific information security and data protection requirements for different EU policy domains.
- The unique nature of some of these policy domains and their attendant security or privacy considerations seem difficult to reconcile with the appetite for more innovative types of technology provision (e.g. through greater consumerisation of corporate IT assets or greater use of cloud computing).
- Understanding information security governance and data protection remains a challenge within many EU frameworks, which are often managed in a federated fashion through obligatory standards and rules set at a strategic EU level (either through the EU Council or Council of Europe) and implementation at the national level.