Privacy standards for information security

Over the last decade, there has been a significant development of privacy standards, which aim at contributing to the integration of privacy requirements into information processes, systems and services.

Published on March 15, 2019



© Copyright: Shutterstock

Tagged with

* [Standards](https://www.enisa.europa.eu/search?Subject%3Alist=Standards)

Such integration is fundamental to protect personal identifiable information, particularly in digital environments and it may support the implementation of relevant privacy and data protection legislation.

This ENISA study, explores how the standards-developing world has been responding to the fast-changing and demanding realm of privacy. This study provides insights into the state-of-the-art of privacy standards in the information security context by mapping existing standards available and standardisation initiatives alike.

The main findings of this study include the following:

* There is an increasing need to analyse the mapping of international standards and European regulatory requirements, as references to standards in the EU legislation are becoming recurrent and there are considerable differences from jurisdictions outside of the EU;
* Proving compliance with privacy standards in information security is not as straightforward as expected. Some approaches for conformity assessment are available in specific sectors, others are still lacking appropriate mechanisms;
* A coherent analysis of sector-specific needs for privacy standardisation is essential, especially in the context of information security, before moving ahead with the adoption or development of new standards;
* Standardisation focuses mainly on covering technological approaches and solutions. Many such solutions address the introduction of privacy-preserving technologies throughout the whole lifecycle of a product or a system. The concept of privacy-by-design and its implementation are still not presented clearly, despite a general common agreement on perceived benefits.

ENISA complements this information with a range of additional recommendations, which aimed to support the prioritisation of potential areas of action for the near future:

* EU policy makers and European Standards Organisations should promote the development of European content and input to privacy and cybersecurity standards;
* EU policy makers and European Cybersecurity Certification Group members should promote the endorsement and adoption of privacy and information security standards, including conformity assessment standards specific to privacy;
* EU bodies and competent authorities in the Member States should promote the adoption of a structured approach on the analysis of sector-specific needs with regard to privacy standardisation, especially in information security context and then proceed with the adoption or development of new standards;
* EU policy makers and relevant EU bodies need to be further involved in the standardisation process, so as to define, endorse or affirm potential standardisation goals in the areas of privacy and information security;
* Competent bodies at EU and Member State level should further promote their research and standardisation activities to support the meaningful implementation of the ‘Privacy by Design’ principle.

For full report: [Guidance and gaps analysis for European standardisation](https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation)