

23/03/2012

EPR01/2012

www.enisa.europa.eu

Privacy – a fundamental right – between economics and practice. ENISA releases two new reports on privacy economics and case studies of online practices in collecting & storing personal data in the EU

ENISA launches two reports with recommendations on personal data protection.

Privacy is recognised within the EU as a fundamental right, but what is the current economic reality? Are online customers willing to pay for privacy? Do individuals value their privacy enough to pay more to service providers that protect their information better? The '[Study on monetising privacy - An economic model for pricing personal information](#)' 'connects the dots' between the interaction of personalisation, privacy concerns and competition between online service providers.

Consumers benefit from personalisation of products, but might also be 'locked-in' to services. Moreover, personalisation bears a privacy risk, i.e. that data may be compromised once disclosed to a service provider. The ENISA study's experimental results reveal that a vast majority of the experiment's participants, up to 83%, chose to pay a 'premium' for privacy. They did so to avoid disclosure of more personal data.

The cases focus on registration to *social networking* sites, on *online ticket booking in the transportation sector* and the collection of customer data and retention of traffic data in the *telecommunications sector*. These cases form the background for an analysis of the principle of *minimal disclosure* (when collecting personal data) and the principle of *minimal storage period* (when storing data), and the fundamental EU-principle of *proportionality*.

The [Executive Director of ENISA](#), Professor Udo Helmbrecht, comments: "*Our '[Study on data collection and storage in the EU](#)' is a pivoting point for a pan-European view on the rules on collection and storage of personal data in the EU.*"

The studies recommendations conclude that:

- the Member States should identify and eliminate conflicting personal data provisions;
- the national Data Protection Authorities should provide clear guidelines to data controllers; and to the Article 29 Data Protection Working Party, the European Data Protection Supervisor and ENISA to do the same when processing personal data with pan-European impact; and
- the Data Protection Authorities should improve user awareness regarding the rights stemming from the data protection legislation and how to exercise these rights, in cases of excessive collection and storage of personal data.

The findings of the studies will be discussed at the Cyber Security & Privacy EU Forum, [ENISA's panel](#), 24/04 in Berlin. This work was conducted in collaboration with [ABC4Trust](#), and is in line with the new EU data protection [regulation](#).

Background:

<http://www.enisa.europa.eu/act/it/library/deliverables/monetising-privacy>

<http://www.enisa.europa.eu/act/it/library/deliverables/data-collection>

For interviews: Ulf Bergstrom, Spokesman, ENISA, press@enisa.europa.eu, Mobile: + 30 6948 460 143 or, Rodica Tirtea, Expert, ENISA, rodica.tirtea@enisa.europa.eu.

