July 2015

ERT

ERT TRILOGY ON THE DIGITAL ECONOMY
Paper #1 “Data Protection/Privacy/Security”

Overarching principles that ERT suggests to guide the discussion:

1. **Principles based protections** – Regulations must focus on the desired outcomes, not detailed, prescriptive and administrative requirements. How those outcomes are achieved should be left to the market, standards bodies and codes of conduct.

2. **Risk based restrictions and enforcement –** Restrictions and enforcement must focus on the activities that are harmful to the rights and freedoms of individuals, based on objective criteria. The greater the harm to the individual, the more protections are needed. Where risks are effectively mitigated, fewer restrictions should apply.

3. **Technology and business model neutrality –** Similar services and similar risks warrant similar protections, irrespective of the technology or business model in question.

4. **Harmonisation across the EU and interoperability globally** – To enable the free flow of information while ensuring accountable collection and use of personal data.

Key responses to the Commission's questions

Question 1: Free movement of both personal and business data is essential: the issue of free flow of personal data is covered in the data protection framework (to be adopted rapidly) and ensuring the free flow of business data to help drive innovation is the objective of the DSM initiative on "free flow of data" (interlinked questions)…

General Data Protection Regulation

We are supportive of the Council's approach; however, we think further work is still needed before the end of the year, especially in the following areas:

1. **The "one stop shop":** The proposal does not lead to a "one stop shop" and it is overly bureaucratic, increases uncertainty and cost to business. Furthermore, the data subject is likely to experience lengthy resolution times.
2. **Profiling and the requirement for consent**: Clarity of the kind of profiling that "significantly affects" the individual, and thus requires consent, is required. Consent should be required only when profiling significantly impacts the rights and freedoms of the individual.
3. **Consent:** Consent should be "unambiguous" as opposed to "explicit" to retain flexibility on how consent is acquired. Requirement for consent should not be overly complex[1].
4. **Personal data and Pseudonymisation**: Clear incentives and lighter obligations to use pseudonymised data should be foreseen in the revised regulation. Given the broad definition of personal data, many beneficial uses of data will be severely curtailed unless pseudonymisation of data results into a significant lift of limitations to analytics.
5. **Purpose limitation:** Without sacrificing the existing principle of purpose limitation, more work is needed to ensure that innovation based on Big Data Analytics is not prohibited, for example through better recognition of pseudonymisation.
6. **Accountability obligations:** Companies should continue to have flexibility on how they demonstrate compliance with the law. Audit cannot be the only means. Data processors cannot be subject to documentation requirements. E.g. in a multiparty environment it would be very burdensome, bordering on impossible while delivering little in the way of real data protection.
7. **No burdensome requirements for processing agreements:** Rules and regulations between controllers and processors must be adapted to the demands of the modern IT-world, e.g. formal requirements related to the conclusion of the processing agreements should be limited to the required minimum.

[1] Examination reserve by one company.

Free movement of both personal and other types of data within the EU and globally

The free flow of personal and business data should be ensured. The international free flow of data is a prerequisite for European industry to optimise global business operations through digital technologies. The transfer of data between the EU and third countries should be facilitated, provided that adequate rules and safeguards are in place. Data localisation policies that restrict the international free flow of data should be limited to legitimate measures, mainly for the protection of national security and public order.

It is crucial to ensure that European personal data is subject to adequate protection no matter where it is transferred to or in which part of the world the service provider may be established. Many European companies have invested considerable time and effort to ensure compliance by, for example, negotiating the use of European Commission Model Clauses or implementing Binding Corporate Rules within their group of companies.

Recommendations for action:

1. EU should ensure full harmonisation of European data protection laws and the creation of globally interoperable data protection regimes that provide effective protection of personal data wherever it is processed.
2. The Commission should review all existing international data transfer mechanisms to determine whether they result in a simple, globally interoperable and effective compliance framework. Where this is not the case, overly formalistic regulations should be simplified to foster international business without compromising on data privacy.
3. Decisions and authorisations to allow cross-border transfers of personal data that have been adopted under the Data Protection Directive (95/46/EC) should remain in force.
4. Use of technology to limit the sensitivity of information, such as pseudonymisation, should be encouraged. Where such technologies are effectively used, the limitations for the free flow of data should be largely lifted.
5. Public procurement should be used to create demand for such technologies and, where organisations would want their information to be stored only in Europe, also for European cloud solutions.

Is data ownership and defining "non-personal" data, as well as limitations to these definitions, useful avenue to pursue for the Commission?

The same data may be subject to multiple independent uses by multiple players. Therefore, introducing “data ownership” and defining “non-personal” data would not be a useful avenue for the Commission to pursue. Personal and other types of data are subject to well-established existing legal frameworks tailored for specific needs, e.g. copyrights, database rights, notice and take down as well as data protection laws.

Question 2: How useful would it be for industry to have rapid and further official guidance on "privacy by design" (consent, anonymisation, pseudonymisation…) and its interaction and impact on IoT, M2M and business generated data as an essential part of the free flow of data initiative? What are the parameters or issues to keep in mind for the Commission?

Meaningful "privacy by design" guidelines are going to be challenging to define in a timely manner given the variety and volume of players and industries, data and speed of developments. Regulators should avoid stifling innovation by defining prescriptive measures and instead focus on defining the desired outcomes. More guidance could be beneficial for, for example, processing personal data in a complex multiparty environment, such as IoT and cloud, where the roles of controllers and processors get blurred. If "privacy by design" guidelines are adopted, compliance with such guidelines should be incentivised and honoured by regulators.

Recommendations for action:

To fill existing gaps in the market place, following actions are needed:

1. Education programmes to create privacy professionals, especially privacy engineers.
2. The industry, standardisation bodies and academia should be encouraged to introduce privacy engineering and risk management methodologies, such as the ongoing work by IPEN (Internet privacy Engineering Network), AIOTI (Alliance for Internet of Things Innovation) and NIST (National Institute of Standards and Technology).
3. Industry, academia and regulators should be encouraged to come up with publicly available guidance which should happen in an open and consultative fashion or other industry driven measures (codes of conduct, certifications…).
4. Bodies responsible for technology standardisation need to conduct a Privacy Impact Assessment for the technology to ensure the right privacy considerations support the information society infrastructure.

Question 3: The industry view on data location requirements, improving portability of data (including "cloud switch" i.e. the possibility of change cloud providers in particular for SMEs without losing essential data or meta-data) as well as cloud security as key features of the free flow of data initiative?

"Cloud" is not a monolithic concept. There are many different types of cloud services, for example Infrastructure as a Service, Platform as Service, Software as a Service (examples encompass cloud based billing and enterprise solutions as well as various consumer and other services such as games, social media and email), and the issues are not the same across these various services.

All companies are likely to use different data models. For this reason there is no need for a common comprehensive standard for data portability. Larger organisations may have multiple different data models in use due to different generations of systems and processes. There are, however, good examples of specific industry standards and efforts to make portability possible in specific cases, such as standards to enable transfer of contacts.

Recommendations for action:

1. More wide spread adoption of specific data portability standards should be encouraged.
2. Blanket rights to retrieve data from service provider should be avoided: existing legal structures and the possibility of agreeing on contractual arrangements allow a differentiated and more balanced outcome.
3. Competition law remedies should be used as a tool to balance dominance where harmful dominance prevails.

Asymmetric regulation – Level playing field

Due to outdated definitions in the current telecommunications regulation, a significant and growing share of communications, now being served by Over the Top players (OTTs), do not enjoy any specific privacy protections. For example, telecommunication companies' ("telcos") use of traffic data and location data is heavily restricted while OTT's use of such data is not. Telcos are bound by administrative rules and mandatory investments to features and capabilities such as lawful interception, in each and every country, whereas OTT players are not.

The rules today are not technology neutral. European citizens cannot rely on European rules to consistently protect their personal data and privacy and the competition landscape is not level.

The ePrivacy Directive only contains six data protection related articles, namely articles governing:

i) traffic data and confidentiality of communications;

ii) location data;

iii) data breach notification;

iv) cookies and other tracking technologies;

v) unsolicited communications.

Given the broad spectrum of various types of data and activities covered by the proposed GDPR, it is difficult to justify retaining those articles at all or retaining them outside the GDPR.

Recommendation for action:

1. The ePrivacy Directive and other electronic communications regulations need to be reviewed, in context of the GDPR review, with the objective of combining all relevant privacy protections under one framework and ensuring that similar services are subject to similar protections.

Big Data, Internet of Things and Analytics

Big Data and the Internet of Things (IoT) challenge some of the traditional concepts of data protection. Powerful analytics tools enable the creation of new insights, often resulting in new personal data being created. Many IoT devices don't have user interfaces and they may be observing their surroundings without being visible. Providing meaningful privacy notice and preventing excessive collection of data will be challenging. However, a significant proportion of the societal benefits from Big Data can be achieved through use of anonymised and aggregated data.

Recommendations for action:

1. Existing privacy principles should remain relevant in Big Data and IoT.
2. Restrictions on analytics must be risk-based and minimal: Analytics with pseudonymised data must be possible as long as the privacy impact on individuals is minimised. Limitations on profiling should focus on automated decision making with significant impacts to fundamental rights and freedoms.
3. The creation or use of sensitive personal data (religion, health, sexual preferences etc.) through analytics should remain subject to special restrictions. However, if aggregated anonymous statistics of such nature are created, there is no privacy concern.
4. Organisations need to be held accountable for having effective privacy programmes in place to protect the data against unlawful processing, applying all relevant privacy principles.

Question 4: How can the industry interact with the research community and the H2020 projects on data and cloud as well as the open science research cloud (a project planned by the Commission)?

In Horizon 2020 industry (small & large), research institutes and academy are already involved in collaborative R&D & Innovation proposals and projects in consortia related to the use of data and cloud, like e.g. in the R&D PPPs FoF (Factories of the Future) and in the Big Data Value PPP initiative. Further strengthened R&D cooperation is needed and welcomed.

Specific areas where future collaborative R&D actions related to **big & smart data** would need to be addressed under Horizon 2020 include:

1. Prediction models.
2. Model Applications.
3. Data Handling (Data Mining).
4. Architecture of system analysis.
5. Appropriate visualisation methods.

In the area of cloud, possible research issues suited for support under Horizon 2020 include:

1. Accounting and payment procedures in the Cloud and in a distributed Cloud.
2. Big Data applications in the cloud.
3. Legal and compliance issues in the cloud.
4. Improving the performance of cloud applications.
5. Cloud computing with agile workload placement at the edge of networks.

For the Open Science Data Cloud, from industry perspective the same rules and safety standards should apply as to any other clouds. In particular with respect to personal data or other sensitive data types, there should not be any legal vacuum where scientists can store and process all kinds of data. Also in these cases the right questions need to be addressed regarding protection concepts, control environments and retention periods. Otherwise this Data Cloud could quickly be used not only for scientific purposes, but also for other (e.g. criminal) purposes. Without adequate protection/security concepts this Data Cloud could quickly become a "self-service shop" for e.g. intelligence services in the world.

Further to the question, how the industry can interact with the research community and the H2020 projects on data and cloud, as well as the open science research cloud; various ways exist or can be imagined:

1. Direct participation of industry players in research projects of academic institutions and in H2020 projects.
2. Improved communication from the research community (in particular universities) towards the industry on i) achievements and ii) research in progress.
3. More open information exchange and discussion forums between research projects and vertical industry sectors (automotive, manufacturing etc.). Often it appears there is a wide gap between the research on fundamental technologies and the awareness and needs of vertical industries.
4. H2020 projects could arrange for effective outreach events/conferences to convey findings, results and highlight future developments.
5. Outreach of H2020 projects, where possible, to industry forums (e.g. GSMA for the mobile telecoms industry, something else for manufacturing etc.) in order to present interim and final findings and raise awareness for results.