

ISOC EUROPEAN REGIONAL BUREAU- EU issues overview

2 March – 8 March 2013

Data protection

MEP's amendment proposes to limit ISPs' data processing liability

- A tabled **amendment** (No. 405) to the draft Report of the European Parliament's Civil Liberties Committee (LIBE) on the proposed [General data protection Regulation](#), submitted by **MEP Frank Engel** (EPP, Luxembourg), proposes to **limit service providers' liability** with regards to data processing.
- The proposed amendment stipulates that a **service provider processing data without being able to access this data** by technically feasible means, and without disproportionate efforts, should be deemed to be '**a neutral intermediary or mere conduit**', thus not responsible for any personal data transmitted, processed or made available through them.

Next steps:

- *Following the LIBE Rapporteur Jan Philipp Albrecht (Greens, Germany) the committee should vote on the report in April.*
- *The so-called trialogue, i.e. the meetings between the European Commission, Council and Parliament with a view to reach final agreement on the Regulation, was originally planned for summer 2013.*
- *The Parliament plenary vote, which is to follow the conclusion of this trialogue, is unlikely to be scheduled before the start of 2014.*

EU Member States call for a risk-based approach to data processing

- The Irish Presidency of the EU has published a [note](#) on the **progress made** so far on the proposed data protection Regulation. The main issues for Member States concern the provisions on **controllers and processors responsibilities**.
- The document stressed that several EU Member States want more **risk-based** obligations on **data processors**: following this approach, the **risk** inherent in certain data processing operations **should be the main criterion for adapting data protection obligations**.
- The note also confirmed that in adapting the data processor's obligations, **the use of pseudonymous data** will be further explored, together with the proposed **mandatory impact assessment** prior to data processing that would represent specific risk.

Copyright infringement

TV broadcasters may block Internet transmissions of their programmes

- The Court of Justice of the EU, following a request submitted by the High Court of Justice of England and Wales regarding the retransmission of TV programmes by another company via the Internet, has [ruled](#) that under certain circumstances, **programme retransmission constitutes 'a communication to the public' of works and therefore, must be authorised by their authors**.
- The case involved TVC, which offers an Internet television broadcasting service, against several British commercial television broadcasters.

Cybersecurity

Series of cyber-attacks targets Czech online services

- Throughout this week, a [series of cyber-attacks](#) (DDoS) affected the functioning of the Czech Republic's **news websites, bank and financial institutions** (with Prague Stock Exchange) and **telecom companies**, including the leading search engine Seznam.
- So far, **no data leakages** have been signalled, in what seems to be the most important series of cyber-attacks in Czech Republic's history. The national cybersecurity teams are investigating who is behind the Internet. Some IPs involved in the attack are said to be Russian.
- In relation to the Czech attacks, the Slovakian SIS Intelligence Service stated it has been [closely monitoring](#) the disturbances as **Slovakia is said to face similar risks**.

EU cybersecurity update

- The proposed [Directive for a harmonised security network](#) across the EU, which is part of the EU [Cybersecurity Strategy](#), has been submitted to the European Parliament. As the complexity of the proposal requires scrutiny from different Parliamentary committees, this legislation is **not expected to be processed under the Parliament's current term** (the next elections are set for June 2014). Should this legislation fail to reach an advanced stage of agreement, a new proposal may be needed in the new Parliament.
- Internal reports of the **European Network and Information Security Agency (ENISA)** have pointed to the **shortcomings of EU Community Emergency Response Teams (CERTs)** with regard to underutilisation of the so called **honeypots**, designed to detect or deflect attempts at unauthorised use of information systems.
- In **Germany**, the government is expected to introduce a **proposal for a cybersecurity law** in the coming months, so that the Bundestag can adopt it before the federal elections in September. A draft version sent to industry associations would introduce mandatory reporting requirements for serious hacking attacks, among other provisions.