

ISOC EUROPEAN REGIONAL BUREAU - EU issues overview

22 - 28 June 2013

Data protection

Commission adopts rules on notifications by ISPs for personal data breaches

- The European Commission has adopted a [Regulation](#) on the measures applicable to the **notification of personal data breaches by providers** of publicly available electronic communication services to the competent national authorities.
- As explained in a Commission [press release](#), the Regulation requires **ISPs** to notify all personal breaches to the **national authorities no later than 24 hours** after the breach has been detected.
- ISPs are also required to notify **the affected person ‘without undue delay’**, in case the data breach is to adversely affect the personal data (based on the assessment of the breach and the likely consequences of the breach).
- The Regulation will enter into force on **25 August**. The rules are added to the existing ePrivacy Directive.

Advocate-General: No general right-to-be-forgotten under Data Protection Directive

- In an [opinion](#) on the application of the **EU Data Protection Directive** published on 25 June, an Advocate-General (AG) of the Court of Justice of the EU (CJEU) stated that **search engines are not responsible for personal data** that appears on web pages they process. Moreover, the **European data protection authorities cannot compel Google** to remove specific data from its index.
- The case concerns an appeal by **Google** against a Spanish ruling in favour of **AEPD**, the Spanish data protection authority, which claimed that the individual right for data removal was breached by the search engine. [Google](#) has argued that it should not be forced to erase lawful content which it did not create.
- The AG stated that **Google is not be considered as a data controller** since the provision of an information location tool does not imply any control over the content on third party web pages.
- The opinion also says that the **Directive does not establish a general right to be forgotten** for citizens. However, search engines are required to comply with local laws on the removal of links to websites hosting illegal or pirated material.

Comment: AG opinions are not binding but CJEU nearly always follows them in its rulings.

After the PRISM scandal, Britain's Tempora programme under scrutiny

- According to Edward Snowden, who previously revealed the existence of the US surveillance programme PRISM, the UK has a similar project named [Tempora](#) that **collects data from international fibre-optic cables**. Operated by **British Intelligence agency GCHQ**, Tempora is said to be able to intercept large amounts of data transferred over 40 cables.
- Reacting to this, [German Justice Minister](#) Sabine Leutheusser-Schnarrenberger voiced her concerns and called for the UK to clarify the situation and to launch a thorough investigation to assess the scope to which German citizens have been targeted. Following those demands, the **EU Justice Commissioner Viviane Reding** has sent a letter to UK Foreign Secretary William Hague also requesting clarifications on UK surveillance activities and their (non-)respect of EU citizens' fundamental rights.
- **UK Foreign Secretary** has defended the joint UK-US spying programmes, underlining that they were conducted within a strict legal framework.

Germany: Data protection commissioner supports international treaty

- Following the revelations about the **PRISM** operation, **German data protection commissioner Peter Schaar** has written an [article](#) in *Der Spiegel* in which he calls for the German government and the EU to push for an international agreement on data protection rights.
- Schaar believes that a first step should be to add a protocol to Article 17 of the UN Convention on Human Rights, which would only require the support of 20 countries to enter into force. He says that the task at hand is to 'drag the intelligence services globally out of their parallel world'.

Open Internet

Europol seizes domain names associated with selling counterfeits

- On 26 June, a [joint operation](#) of **Europol** and the US government's Homeland Security Investigations **seized 328 domain names** relating to **websites that sell counterfeit goods**.
- Europol participated alongside national authorities in many EU Member States, targeting 151 European top-level domains, of which [79 were blocked by the Belgian authorities](#) (with the addresses .eu or .be).
- The coordinated action followed complaints by trademark owners.

Germany: Internet Industry urges Commission to support child safety hotlines

- In an [interview](#) published on 25 June, **Oliver Süme**, Board Member of eco (Association of the German Internet Industry) urged the European Commission to continue supporting the **European Internet complaints hotlines** as they are deemed successful in combatting child pornography.
- In his view, the fact that the hotlines are not explicitly mentioned in the new guidelines on the **Connecting Europe Facility** (CEF – EU funding instrument) indicates that they are no longer considered as priority tools. The current EU support for this tool ends in June 2014.
- Süme underlined that four days after receiving a formal complaint with regards to child pornography, **91% of the incriminated websites** hosted within Germany had been shut down.

Cybersecurity

Council calls on Member States to protect ISPs from cyberattacks

- On 21 June, the **Council of the EU** published draft [conclusions](#) on the [Communication on the Cybersecurity Strategy of the European Union](#), which the Commission adopted in February. These underline the need for the EU to develop and implement a comprehensive cybersecurity approach that **respects freedom of expression** and privacy.
- The text also addresses **Internet governance**, calling on the EU to maintain a **multistakeholder model** of governance.
- The conclusions also underline that the EU's cyber legislation should remain **technology neutral** and encourage **net neutrality**.
- With regards to **ISPs**, the conclusions called for the Member States to support the owners and providers of ICT systems in protecting their systems and the vital services they provide.