EUROPEAN COMMISSION

PRESS RELEASE

Brussels, 24 June 2013

Digital Agenda: New specific rules for consumers when telecoms personal data is lost or stolen in EU

The European Commission is putting into place new rules on what exactly telecoms operators and Internet Service Providers (ISPs) should do if their customers' personal data is lost, stolen or otherwise compromised. The purpose of these "technical implementing measures" is to ensure all customers receive equivalent treatment across the EU in case of a data breach, and to ensure businesses can take a pan-EU approach to these problems if they operate in more than one country.

Telecoms operators and ISPs hold a range of data about their customers, such as name, address and bank account details, in addition to information about phone calls and websites visited. These companies have been operating since 2011 under a general obligation to inform national authorities and subscribers about breaches of personal data (IP/11/622).

Thanks to a Commission Regulation, companies will have extra clarity about how to meet those obligations, and customers will have extra assurance about how their problem will be dealt with. For example companies must:

- Inform the competent national authority of the incident within 24 hours after detection of the breach, in order to maximise its confinement. If full disclosure is not possible within that period, they should provide an initial set of information within 24 hours, with the rest to follow within three days.
- Outline which pieces of information are affected and what measures have been or will be applied by the company.
- In assessing whether to notify subscribers (i.e. by applying the test of whether the breach is likely to adversely affect personal data or privacy), companies should pay attention to the type of data compromised, particularly, in the context of the telecoms sector, financial information, location data, internet log files, web browsing histories, e-mail data, and itemised call lists.
- Make use of a standardised format (for example an online form that is the same in all EU Member States) for notifying the competent national authority.

The Commission also wishes to incentivise companies to encrypt personal data. As such, and in conjunction with ENISA, the Commission will also publish an indicative list of technological protection measures, such as encryption techniques, which would render the data unintelligible to any person not authorised to see it. If a company applies such techniques but suffers a data breach, they would be exempt from the burden of having to notify the subscriber because such a breach would not actually reveal the subscriber's personal data.

European Commission Vice-President Neelie Kroes said: "*Consumers need to know when their personal data has been compromised, so that they can take remedial action if needed, and businesses need simplicity. These new practical measures provide that level playing field.*"

The Commission is implementing these rules following its 2011 public consultation, showing widespread stakeholder support for a harmonised approach in this area. The rules were agreed by a committee of Member States and scrutinised by the European Parliament and Council. They are adopted in the form of a Commission Regulation, which has direct effect and requires no further transposition at national level, and will come into force two months after publication in the EU Official Journal.

Background

The 2002 ePrivacy Directive requires telecoms operators and Internet service providers to keep personal data confidential and secure. However, sometimes data is stolen or lost or accessed by unauthorised persons. These cases are known as 'personal data breaches'. Under the revised ePrivacy Directive (2009/136/EC), when a personal data breach occurs, the provider has to report this to a specific national authority, usually the national data protection authority or the communications regulator. Also, the provider has to inform the concerned subscriber directly when the breach is likely to adversely affect personal data or privacy. To ensure consistent implementation of the data breach rules across Member States, the ePrivacy Directive allows the Commission to propose "technical implementing measures" – practical rules to complement the existing legislation – on the circumstances, formats and procedures for the notification requirements.

To prepare the measures, the ePrivacy Directive requires the Commission to "involve all relevant stakeholders". This was done in the form of a public consultation in 2011. Responses were received from a wide range of respondents including national authorities, service providers and civil society. The results showed widespread support among stakeholders for harmonised rules and evidence of some divergences in national approaches. The Commission also consulted the European Network and Information Security Agency (ENISA), the Article 29 Working Party on Data Protection and the European Data Protection Supervisor (EDPS) in preparing the measures.

The measures are separate and distinct from the Commission's proposed revision of EU legal framework for data protection and the Commission's proposal for a Directive on network and information security.

Useful links

Commission Regulation on the measures applicable to the notification of personal data breaches under the ePrivacy Directive

The ePrivacy Directive.

Online privacy in the Digital Agenda

The EU Data Privacy Directive

Hash Tags: #eprivacy

Have Your Say

Digital Agenda

Neelie Kroes Follow Neelie on Twitter

Contacts :
Ryan Heath (+32 2 296 17 16), Twitter: @RyanHeathEU
Linda Cain (+32 2 299 90 19)