Bird & Bird

New data breach rules for Telcos and ISPs

On 25 August 2013, a new European Regulation 611/2013 ("**Regulation**") came into effect, changing and expanding the procedure for breach notification laid out in the E-Privacy Directive 2002/58/EC as amended ("**E-Privacy Directive**"). It applies to "providers of publicly available telecommunications services" (e.g. telecommunication companies, ISPs, email providers, often collectively known as "**PECS providers**"). However, as the draft General Data Protection Regulation promises to introduce general breach notification requirements, it is also of general interest as a sign of things to come.

As a Regulation, the instrument is already legally binding and directly effective in all Member States. Its rules take the place of the Member State specific requirements in this area.

The Regulation outlines two breach notification obligations: (i) to the relevant national authority (which is not necessarily the local data protection authority), and (ii) to affected individuals. We have highlighted the main obligations from the new Regulation, as compared with the E-Privacy Directive. We have also collated online forms for all Bird & Bird countries, to provide an easy-to-use resource for PECS providers.

E-Privacy Directive	Regulation	
Previous requirements	New requirements	Limitations
Obligation to notify relevant local authority		
Notification without undue delay	Notification within 24 hours after detection of personal breach, where feasible (Article 2)	Firstly, notifications are only to be made where feasible. The Recitals of the Regulation are silent on the notion of feasibility. This term remains to be interpreted. Different scenarios could be foreseen (e.g. if the person with the responsibility to act on behalf of the company is not available, does this mean notification cannot takes place?). Secondly, notification only has to be made once there is real knowledge of a breach - distinct from mere suspicion: a simple suspicion or detection of a singular incident "*without sufficient information being available, despite a provider's best efforts to this end*" does not justify notification (Recital 8). As a result, this gives PECS providers additional time to look into the issue. If all the information is not available within the first 24 hours of detection, a two-step process may be used; initial notification within 24 hours, followed by a second notification with the remaining information as soon as possible and at the latest within three days after the initial notification. The Regulation goes on to say that "*where the provider, despite its investigations, is unable to provide all information within the three-day period from the initial notification, [it] shall notify as much information as it disposes within that timeframe and shall submit to the competent national authority a reasoned justification for the late notification of the remaining information. The provider shall notify the remaining information to the competent national authority and, where necessary, update the information already provi*ded, *as soon as possible*" (Article 2.3). It will be interesting to see how this two-step process will be aligned with the on-going General Data Protection Regulation discussions which also provide a general data breach notification regime.

E-Privacy Directive	Regulation	
Previous requirements	New requirements	Limitations
No prescriptive provisions	Notification to include a specific list of information as set out in Annex I of the Regulation	N/A
	Relevant national authorities to establish secure electronic means for notification (see table below)	
	Where the personal data breach affects subscribers or individuals from Member States other than that of the competent national authority to which the personal data breach has been notified, the competent national authority shall inform the other national authorities concerned. It is worth mentioning that unlike BCR procedures, there is no concept of a lead authority to deal with pan-European breach issues.	
Obligation to notify affected individuals		
When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the PECS provider shall also notify the subscriber or individual of the breach without undue delay However, notification to individuals is not required if the PECS provider has rendered the data "unintelligible"	Same obligation (Article 3). However, the Regulation provides prescribed circumstances to be taken into account to assess the adverse effect: • the nature and content of the personal data concerned, in particular where the data concerns financial information, special categories of data referred to in Article 8(1) of Directive 95/46/EC, as well as location data, internet log files, web browsing histories, e-mail data, and itemised call lists; • the likely consequences of the personal data breach for the subscriber or individual concerned, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation; and • the circumstances of the personal data breach, in particular where the data has been stolen or when the provider knows that the data are in the possession of an unauthorised third party.	Encryption: Notification to subscribers or individuals is not required if the PECS provider has rendered the data unintelligible through encryption or hashing. The EC may, after having consulted the competent national authorities via the Article 29 Working Party, the European Network and Information Security Agency and the European Data Protection Supervisor, publish an indicative list of appropriate technological protection measures to render data unintelligible.
Notification without undue delay	To be notified without undue delay after a data breach has been detected. This obligation is independent of the obligation to notify the relevant national authority.	Investigations: Notification can be delayed with the agreement of the relevant national authority for reasons of on-going investigations.
Notification to subscribers to include the nature of the breach, contact points for further information and recommended measures to mitigate the adverse effects of the breach	Notification to include information set out in Annex II of the Regulation. The notice must be in clear and easily understandable language. Information about the breach must be dedicated to the breach and not associated with information about another topic. For example, inclusion of information about a breach in a regular invoice would not be adequate, nor can the notice be used to advertise new or additional services.	See above. In addition, "*where the provider having a direct contractual relationship with the end user, despite having made reasonable efforts, is unable to identify within the [above] timeframe (...) all individuals who are likely to be adversely affected by the personal data breach, [it] may notify those individuals through advertisements in major national or regional media (...) within that timeframe. These advertisements shall contain the information set out in Annex II, where necessary in a condensed form. In that case, the provider shall continue to make all reasonable efforts to identify those individuals and to notify to them the information set out in Annex II as soon as possible*".

E-Privacy Directive	Regulation	
Previous requirements	New requirements	Limitations
No prescriptive provisions	Where another provider is involved to provide the service without having a direct contractual relationship with individuals or subscribers, it must immediately inform the contracting provider in charge of the contractual relationship. PECS providers and their sub-processors must therefore review existing agreements to make sure that appropriate provisions are in place.	N/A

The following table outlines where the new online notification procedures can be found in different Member States:

Country	New online notification procedure
Belgium	Not yet available. In the interim, PECS providers should contact the Belgian data protection authority via this contact form
Czech Republic	Available here
Denmark	Available here
France	Available here
Germany	Not yet available
Hungary	Not yet available. Until then, the relevant authority is the National Media and Communications Authority (NMHH). PECS providers to email their breaches to: info@nmhh.hu
Italy	Available here
The Netherlands	Available here
Poland	Available here
Slovakia	Available here
Spain	Not yet available
Sweden	Available here
United Kingdom	Not yet available. According to the data protection authority (ICO) website, updated guidance is to follow shortly. Until then, PECS providers should continue to follow the existing guidance on breach notification

Contact details

Ruth Boardman
Partner
ruth.boardman@twobirds.com
Tel: +44 (0)20 7415 6018

Ariane Mole
Partner
ariane.mole@twobirds.com
Tel: +33 (0)1 42 68 6304

Gabriel Voisin
Associate
gabriel.voisin@twobirds.com
Tel: +44 (0)20 7905 6236

twobirds.com