GOWLING WLG

RECENT DEVELOPMENTS IN PERSONAL DATA SECURITY AND THE WIDER EUROPEAN SECURITY LEGISLATIVE LANDSCAPE

07 August 2013

On 25 August 2013 a new data protection regulation (Regulation no. 611/2013) comes into force in all EU member states. It requires speedier mandatory notification of personal data breaches by telecommunications companies and internet service providers (providers) to their local data protection authority (the Authority).

The 2013 Regulation also specifies content of notifications given to Authorities, effected subscribers or other individuals. At the same time, it provides more detailed information on levels of technical measures for a breach to be exempt from notification.

The 2013 Regulation builds on the existing obligation for providers to notify the UK's Information Commissioner of personal data breaches under the Privacy and Electronic Communication (EC Directive) Regulations 2003, as amended in 2011 (the 2003 Regulation implements Directive 2002/58/EC into UK law). Unlike the Directive, the new 2013 Regulation will be directly effective (so there will not be a further implementation into national law.

By using a directly effective Regulation, the European Commission aims to harmonise the notification process across the EU by establishing commonly applicable 'technical measures' for notification. These new technical measures include specific timescales within which a notification must be made and more description about encryption than has previously been given. This should assist providers operating in more than one Member State adopting a uniform policy regarding personal data security breaches across all group companies.

Application of the Regulation

The 2013 Regulation only applies to providers, not the wide range of companies that

provide online services which primarily deliver content, (such as e-banking and online shopping). It also does not apply where companies offer Wi-Fi as an additional service (e.g. where the primary offering is a café or shop and Wi-Fi is a supplemental service).

New speedier notification requirements

The 2013 Regulation requires providers to notify their Authority within 24 hours of detection of a personal data breach, where this is feasible. The 2013 Regulation also lists the specific details relating to the breach that must be given in notifications to an Authority and to effected subscribers or other individuals (users).

One thing that hasn't changed is that all breaches must be reported to the Authority, regardless of size, even if the number of users and/or the quantity of compromised data is very small.

If reporting the full details of the breach is not feasible within 24 hours of discovery, then an initial report (including date and time of the breach, circumstances of the breach, nature and content of compromised personal data and relevant use of other providers) must still be submitted within 24 hours.

The remainder of the information about the breach must be submitted within72 hours of the initial report. It should include a summary of the breach, number of users affected, any potential consequences/adverse effects, mitigating action taken and, if relevant, details of communications with users and of cross-border breaches and notifications to Authorities in other countries. A full list of the notification requirements for Authorities is given below.

The 2013 Regulation requires that Authorities provide a secure channel through which to report breaches. Until now, the ICO published a monthly log sheet (in Word) on which breaches should be reported. It would seem though that the Regulation is now hinting at a more sophisticated and co-ordinated system being set up between Europe's Authorities to maximise the benefits of harmonisation.

The triggers for notifying users are largely unchanged. If the breach is likely to have adverse consequences for users (e.g. where sensitive personal information is involved or the breach could result in theft, fraud, distress, or damage to reputation), those users must also be notified directly without undue delay.

Where the 2013 Regulations provides an added layer of detail is in the content of the notification to users, which must be in clear, easy to understand language and include a list of details about the breach, the data involved, potential consequences and mitigating

steps. The 2013 Regulations specify a much more detailed list of requirements than before. See the full list for more details.

The 2013 Regulation also specifies that users must be prominently notified (e.g. no hiding it in an invoice or putting it alongside marketing materials).

In the event that a data breach is detected by a service provider to the provider, they are required to report the breach to the provider, which should then follow the reporting measures outlined above.

Encryption

If a provider can demonstrate to the Authority that the compromised personal data was rendered unintelligible, notification to users is not required. The 2013 Regulation goes further than any other current legislation in describing what is acceptable in terms of rendering data unintelligible. Unintelligible data is defined in the 2013 Regulation as that which has:

- been securely encrypted with a standardised algorithm where the decryption key is uncompromised by the security breach, and is not ascertainable by any unauthorised person or by available technological means; or
- been replaced by its hashed value, calculated with a standardised cryptographic keyed hash function, where the key used to hash the data is uncompromised by the security breach and was generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access the key.

The 2013 Regulation does not specify appropriate technological protection measures, as such details would be liable to change as technology advances, but there is a suggestion in the 2013 Regulation that a list of such protection measures - according to the current practices - may be published in the future.

Wider breach and security legislation landscape

From the point of view of users, the 2013 Regulation does not change the position much although they might now get a speedier, more detailed and prominent breach notification. However, it will be interesting to see whether this will trigger more or different user reactions.

What also remains to be seen is whether feedback from providers will shape the draft

Data Protection Regulation, which will replace the Data Protection Directive. In the current form of the draft Data Protection Regulation, all data controllers (not just providers) will have to report breaches within 24 hours. Authorities should be able to learn from experiences in certain sectors, before mandatory breach notification is rolled out to all data controllers when the draft Data Protection Regulation becomes effective.

This new 2013 Regulation is also part of a wider EU initiative to encourage companies to focus on cyber security in general, not just security of personal data. The proposed Network and Information Security Directive (or 'Cyber Security Directive') will mandate certain security measures and processes to improve network and information security for public bodies and some private sector companies such as financial services, banks, health, transport and any 'enabler' of electronic communication services. (The exact meaning of 'enabler' is unclear but appears to be any company that provides a platform for online services to be delivered - a list of examples are included in the Directive).

Security and breach notification are clearly rising up the European legislative agenda. The potential downside for organisations caught by the various new pieces of legislation are cost and effort in meeting prescribed levels of security (offset by the benefit of clarity of defined standards) and transparency and accountability to customer (offset by reputational impact if breaches are frequently reported). There is some way to go before the Cyber Security Directive will become law in the UK. There is an obvious overlap between cyber security and the draft Data Protection Regulation and it is unclear how the two proposed pieces of legislation work together. However, security breaches are a common headline article in the national press, alongside the increasing sophistication of cyber-attacks, organisations must all open their eyes to the inevitable onset of regulation for security of all types of data.

For more information, please see the full Regulation.

Content of notification to Authorities

Identification of the provider

- Name of the provider
- Identity and contact details of the data protection officer or other contact point where more information can be obtained
- Whether it concerns a first notification (i.e. within 24 hours) or second notification (i.e. within 72 hours)

Initial information on the personal data breach (for completion in later notifications, where applicable)

- Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident
- Circumstances of the Breach (e.g. loss, theft, copying)
- Nature and content of the personal data concerned
- Technical and organisational measures applied (or to be applied) by the provider to the affected personal data
- Relevant use of other providers (where applicable)

Further information on the personal data breach

- Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved)
- Number of users concerned
- Potential consequences and potential adverse effects on users
- Technical and organisational measures taken by the provider to mitigate potential adverse effects

Possible additional notification to users

- Content of notification
- Means of communication used
- Number of users notified

Possible cross-border issues

- Personal data breach involving users in other Member States
- Notification of other competent Authorities

Content of notification to users

- Name of the provider

- Identity and contact details of the data protection officer or other contact point where more information can be obtained
- Summary of the incident that caused the Breach
- Estimated date of the incident
- Nature and content of the personal data concerned, particularly where the data concerns financial information, sensitive personal data, location data, internet log files, web browsing histories, e-mail data, and itemised call lists
- 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
- Circumstances of the personal data breach in particular where the data has been stolen or is in the possession of an unauthorised third party
- Measures taken by the provider to address the Breach
- Measures recommended by the Provider to mitigate possible adverse effects

Related Tech, Information Technology, ThinkHouse

Jocelyn S Paulley

Partner - London

Email

jocelyn.paulley@gowlingwlg.com

Phone

+44 (0)20 3636 7889

vCard

Jocelyn S Paulley