JULY 2013

EUROPE HARMONIZES HOW OPERATORS MUST NOTIFY PERSONAL DATA BREACHES

On June 26, the European Commission published Regulation 611/2013 ("Regulation") which harmonizes across the 28 EU Member States the practical operation of notifying personal data breaches.[1] This clarifies a requirement contained in the E-Privacy Directive since 2009 (Directive 2002/58/EC as amended by Directive 2009/136/EC).

WHAT IS A PERSONAL DATA BREACH?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Personal data is any information relating to an identified or identifiable natural person, and it includes information such as personal e-mails, calling data, and IP addresses.

WHO MUST NOTIFY?

The E-Privacy Directive imposes an obligation to notify data breaches only on providers of electronic communication services, i.e., telecoms operators and internet service providers. However, the Regulation sets the tone for the manner in which data breaches must be notified when such requirement is extended to all businesses (see below).

TO WHOM SHOULD NOTIFICATIONS BE ADDRESSED?

Three types of addressees could be contemplated:

- First, notifications must be addressed to the competent national authority. Usually, this will be either the data protection authority or the telecommunications regulator.

1 *See* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:EN:PDF

- Second, the individual/service subscriber must also be informed, unless data has been securely encrypted such that it is rendered unintelligible to any person who is not authorized to access it. The Commission is expected to publish a list of appropriate encryption measures in the near future.

- Finally, if the provider does not have a direct contractual link with the individual concerned, it is not obliged to issue the above notifications but must notify the provider having such a link.

WHAT INFORMATION SHOULD BE NOTIFIED?

The information to be included in the notification is specified in the Annex to the Regulation, which provides separate specifications for notifications to national authorities and individuals. Generally, they both include information such as (i) the provider's identity and relevant contact details, (ii) the timing and circumstances of the breach, (iii) the nature and content of the data, (iv) remedies contemplated, (v) likely consequences of the breach, and (vi) technical/organizational measures taken to address the breach.

For national authorities, additional information is required, such as (i) the number of individuals involved, (ii) information on the individual notifications performed, and (iii) data breaches and notifications effected in other Member States. Individuals should be informed of measures that they can take to mitigate possible adverse effects.

WHEN MUST A NOTIFICATION BE MADE?

In respect of a national authority notification, an initial notification must, in all cases, be made within 24 hours of the detection of the personal data breach. The notification of some information may be postponed up to three days from the initial notification, if not immediately available. In cases where it has not been possible to collect all requested information within the set time frame, the provider must submit instead a reasoned justification for such failure.

In respect of a notification to an individual, only personal data breaches that are "likely to adversely affect" the personal data or privacy of an individual must be notified. The factors to be taken into account in making this determination include:

- **The type of data:** in particular, financial data, data of a sensitive personal nature, location data, internet log files, web browsing histories, e-mail data, and itemized call lists;

- **The likely consequences of the breach:** in particular, identity theft or fraud, physical harm, psychological distress, humiliation, or damage to reputation; and

- **The circumstances of the breach:** in particular, theft or where, to the provider's knowledge, data is in the possession of an unauthorized third party.

The notification to an individual is to be made "without undue delay" after detection. Unlike the national authority notification, there is thus no specified time limit. In exceptional circumstances, where notification to the individual would put at risk the investigation into the breach, the provider may delay notification with the permission of the national authority.

HOW MUST A NOTIFICATION BE MADE?

The Regulation provides that national authorities are to provide an online form by which providers may communicate the breach. In relation to individuals, there is no standard form, but the communication must be (i) clear and easy to understand, (ii) prompt and secure, and (iii) independent of information concerning other topics.

WHAT ARE THE SANCTIONS FOR FAILURE TO PROPERLY NOTIFY?

Under the E-Privacy Directive, Member States are obliged to lay down rules on penalties, including criminal sanctions if deemed appropriate, for failure to comply with the notification obligation. Thus, the precise nature of the sanction will vary between the various Member States. As an example, in the UK, the relevant authority is empowered to impose a monetary penalty.

IMPLICATIONS AND CONCLUSION

The Regulation comes into force across the EU on the August 25 and will have immediate direct effect. By that date, providers of electronic communications services should thus put in place internal measures so that, when a personal data breach is detected, the information is channeled sufficiently quickly within the company to be notified within the 24 hours time frame. Such measures could include:

- Developing internal protocols for reporting to legal departments (e.g., through the company's intranet);
- Adopting pan-European standards and procedures for responding to and notifying personal data breaches, whether implemented at the national level or through a one-stop shop principle;
- Introducing personal data breach notifications in the relevant employees' compliance program; and
- Including contract terms in all subcontracting agreements with third parties, with reporting obligations to the relevant person or department within the company.

There is no doubt that the practice established through this Regulation will influence the application of the general EU data protection regulation2 when it is adopted, since this latter foresees the introduction of similar data breach notification requirements for all businesses.

2 See "The EU Launches Initiative to Revamp EU Privacy Rules," *available at* http://www.jonesday.com/eu__launches__initiative/

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Alexandre Verheyden
Brussels
+32.2.645.15.09
averheyden@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

ADDITIONAL CONTACTS

FRANCE

Emmanuelle Rivez-Domont
Paris
+33.1.56.59.39.39
earivez@jonesday.com

GERMANY

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

ITALY

Stefano Macchi di Cellere
Milan
+39.02.7645.4001
smacchi@jonesday.com

SPAIN

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

UNITED KINGDOM

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Elizabeth A. Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

UNITED STATES

Kevin D. Lyles
Columbus
+1.614.281.3821
kdlyles@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com