

Update

New Rules on European Data Protection announced

A view from Andrew Horrocks and Charlotte Worlock

Key features of the proposed Regulation:

- Creates a single European data protection law
- Applies to businesses – including those based outside the EU – handling personal data of EU residents
- Imposes a general obligation to provide notification of a serious breach of personal data to national supervisory authority, where feasible, within 24 hours
- Introduces principles of transparency and privacy by design
- Where consent is required for data processing, it must be explicit
- Introduces right to be forgotten and right to data portability
- Requires large businesses to appoint a Data Protection Officer
- Provides for a private right of action, and administrative sanctions of up to €1 million for individuals, and up to 2 per cent of annual worldwide turnover for companies

Summary

A proposed new European Regulation on data protection was announced by the EU Justice Commissioner, Viviane Reding, at a press conference held today (January 25, 2012). This update provides an overview of the proposals.

The proposed Regulation is called the “Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (“the Regulation”). Ms. Reding stated that the Regulation is intended to provide a single data protection law for the whole European Union, and

create a “strong, clear and uniform legal framework at EU level [which] will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation.”

The proposed Regulation is intended, she said, to safeguard privacy and reduce the administrative burden to businesses, which currently must comply with different rules in each of the 27 EU Member States, leading to a reduction of around €2.3 billion each year in administrative costs. The draft rules will now be put before the European Parliament for consultation and approval by the Member States, and the Regulation is

expected to come into force in two or three years time.

While enforcement of the new rules might seem some way off, businesses should be aware that the proposed Regulation is intended to have broad application, and contains various onerous obligations which, if implemented, will require most companies to employ additional measures to ensure compliance. As such, we recommend businesses work with their legal representatives to evaluate their obligations under the proposed Regulation now, and prioritise their data protection and privacy obligations as soon as possible. The new Regulation is intended to apply to entities based both inside and outside the EU, including social networks, and therefore all businesses must be proactive in ensuring compliance, or risk heavy fines and prosecution.

Finally, we anticipate that the proposed Regulation will bring increased opportunities to the insurance industry, which must innovate or adapt existing products in order to address the needs of those clients which are bound by the forthcoming EU rules.

Scope

The proposed Regulation is intended to apply to all businesses engaged in the “processing” (i.e. collection, storage, dissemination and use) of personal data belonging to EU residents. “Personal data” is broadly defined, and can include a name, a photograph, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.

The Regulation does not apply to data processing “by a person without any gainful interest in the course of its own exclusively personal or household activity, unless personal data of other natural persons is made accessible to an indefinite number of individuals.” However, it appears that this exception could include an individual who posts personal data belonging to others on a social network, such as Facebook, and it will be interesting to see how this plays out in practice.

Non-EU-based businesses which process personal data belonging to EU residents will fall within the scope of the proposed Regulation if the company offers goods and services to EU residents, or monitors the online behaviour of EU residents. Where a large company is not physically established in the EU, the draft Regulation will require the foreign entity to establish an EU representative in one of the Member States where the data subjects reside, who would be required to comply with the Regulation. Small to medium sized businesses may not be required to appoint a representative, although their activities will still be subject to the Regulation.

Mandatory Breach Notification Requirement

Notification to Supervisory Authority

Most significantly, the proposed Regulation introduces a general obligation to provide notification in the event of a personal data breach. All companies will be required to notify any breach of EU residents’ personal data to the relevant national supervisory authority “without undue delay” and, where feasible, no later than 24 hours after they have become aware of the breach. If notification to the supervisory authority is made more than 24 hours after discovery of the breach, it must be accompanied by a reasoned justification.

Notification must: (a) include a description of the breach, including the categories and amount of data subjects and data involved; (b) provide contact information for the Data Protection Officer (see below); (c) recommend measures to mitigate any possible adverse effects of the breach; (d) describe the consequences of the breach; and, (e) describe any measures proposed or taken by the controller to address the breach.

Notification to Data Subject(s)

When a breach is likely to adversely affect the protection of the personal data or privacy of a data subject(s), notification is to be provided to the data subject(s) following notification to the supervisory authority. Notification to a data subject must occur “without undue delay” and shall include a description of the nature of the breach, as well as (b) and (c) (above).

However, if the breached data is encrypted, there is no requirement to notify the data subject (although notification must still be given to the supervisory authority). This follows the general US approach, and enables companies to avoid some of the highest costs arising from a breach.

Penalties

The Regulation provides national supervisory authorities with the power to impose penalties for intentional or negligent failure to notify of up to €1 million or – if an enterprise – up to two per cent of their worldwide annual turnover. Such penalties bring data protection legislation in line with EU competition law, which also provides for maximum penalties of a percentage of an organisation’s annual worldwide turnover. The draft rules also provide individuals with the right to seek judicial remedy against a company which fails to comply with its obligations under the Regulation.

Requirements for Businesses

Transparency

The proposed Regulation requires that personal data be processed “lawfully, fairly and in a transparent manner in relation to the data subject” and “collected for specified, explicit and legitimate purposes”. Companies will be required to carry out privacy impact assessments before processing any data that is likely to present specific risks to individuals, and to be transparent as to what data they hold and how it is used. The draft rules also require that joint data processors sign an agreement allocating responsibility between them; absent such an agreement, both processors will be jointly liable for all processing.

Explicit Consent

The draft Regulation requires that where consent to processing is required, such consent must be “freely given specific, informed and explicit”. The draft Regulation also provides that a data subject has the right to withdraw their consent at any time, and the consent of a person under 13 is only valid when given or authorised by the child’s parent or custodian.

Consent to data processing must be meaningful, which removes the right for a brand to assume consent if a consumer is silent or inactive. In addition, businesses are barred from considering legitimate interests of third parties in instances other than security-related processing; this has the effect of barring the data industry from collecting and providing information to credit bureaus.

Privacy by Design

The draft Regulation also provides that only the minimum of personal data necessary should be processed, and requires businesses to ensure that personal data is not by default accessible to “an indefinite number of individuals”.

Data Protection Officer

Any company employing more than 250 staff is required to appoint a Data Protection Officer, to ensure compliance with the Regulation’s obligations.

Cross-border transfers

Once one national supervisory authority approves a company’s “binding corporate rules” (BCRs) governing internal and extra-EU transfers of personal data of any entity in a group of companies, no further approvals from other national supervisory authorities are required, with some exceptions.

Rights for data subjects

With regard to the status of privacy and data protection as fundamental rights in the EU, the draft Regulation proposes several new rights for data subjects in connection with the use of their personal data - especially in relation to

personal data made available when the data subject was under 13. Nonetheless, as Ms. Reding pointed out during her press conference today, none of the rights under the Regulation is an absolute right, and there are exceptions.

Right to be Forgotten

Upon request, any company could be required to erase an EU resident’s personal information, including public internet links to copies of personal data kept by social networks and search engines. In her press conference today, Ms. Reding specifically cited the example of an individual seeking removal of a photograph published on Facebook. In general, according to the draft Regulation, the right to be forgotten should be enforced when there are no legitimate grounds for the information to be kept. It remains to be seen how straightforward it will be to enforce the requirements on companies such as Google.

However, a company is not required to erase personal data where it is necessary to protect freedom of expression, or the need to collect information for scientific, statistical or historical research.

Right to Data Portability

The draft Regulation introduces the right to transfer data from one service provider (such as a social network) to another, which the Commission hopes will improve competition.

Right to Object

The draft rules propose that data subjects be given the right to object to the processing of their data for direct marketing purposes. This right must be explicitly and intelligibly offered.

Enforcement

Supervisory Authorities

The draft Regulation requires each Member State to set up a supervisory authority to monitor and ensure consistent application of the Regulation, including conducting investigations and hearing complaints. The supervisory authorities will each have the same powers and their rulings will be binding across all other Member States, so that organisations will only have to deal with a single national data protection authority in the EU country where they have their main office. The supervisory authorities will act as a “one-stop shop” to ensure enforcement of the Regulation, and have the power to administer sanctions for non-compliance of up to €1 million or two per cent of an organisation’s worldwide annual turnover.

European Data Protection Board

The draft Regulation establishes a European Data Protection Board, which replaces the Article 29 Working Party, and oversees regulatory enforcement of the

Regulation. The Board is composed of a head of one supervisory authority of each Member State and the European Data Protection Supervisor. The Commission also has the right to participate in all of its activities and meetings.

European Commission

The proposed rules provide the Commission with extra powers, including the power to adopt delegated acts – which have supremacy over national laws – and the right to determine when a third country/territory or international organisation has an adequate level of protection in place for personal data, and the Commission may prohibit the transfer of personal data to such areas if it deems such a level of protection is not in place.

Rights of Action

Under the draft Regulation, data subjects have the right to lodge a complaint with a supervisory authority in the event of a controller's non-compliance with any provision of the Regulation. Consumer organisations and similar associations also have the right to file complaints on behalf of a data subject or, in case of a personal data breach, on their own behalf.

Furthermore, the draft Regulation provides individuals with the right to seek a judicial remedy against decisions of a supervisory authority concerning them. Individuals also have the right to a judicial remedy if they consider that their rights under the Regulation have been infringed as a result of the processing of their personal data in non-compliance with the Regulation.

Conclusion

The Ponemon Institute recently published its 2010 Annual Study: UK Cost of a Data Breach, which estimated that the average cost of a data breach for a UK business in 2010 was £1.9 million or £71 per record, an increase of 13 per cent on 2009, and 18 per cent on 2008. Given the heavy penalties and numerous possible sanctions available under the proposed new Regulation, these costs are only likely to increase. As such, businesses must start reviewing their own data protection and IT security policies in line with the proposed EU rules now, and should give serious consideration to implementing encryption software in order to guard against the increased costs of providing notification to individual data subjects.

Furthermore, it is clear that traditional liability insurance products cannot provide the scope of coverage required by those companies covered by the proposed Regulation. Accordingly, insurers are developing and offering specialist standalone data breach products, designed to address the unique exposures faced by those companies which fall within the scope of the new Regulation. Such products, which are already available but much more commonplace in the U.S., can provide first party coverage for notification costs, forensic investigations and credit monitoring, along with a list of approved suppliers and privacy counsel, as well as third party cover for civil claims arising from breach incidents.

We recommend that businesses and insurers move swiftly to prepare for the proposed Regulation. Please do not hesitate to contact the authors or your usual Clyde & Co contact if you would like to discuss any aspect of the proposals.

Further information

If you would like further information on any issue raised in this update please contact:

Andrew Horrocks

E: andrew.horrocks@clydeco.com

Lisa Payne-Lawrey

E: lisa.payne-lawrey@clydeco.com

Manoj Vaghela

E: manoj.vaghela@clydeco.com

Charlotte Worlock

E: charlotte.worlock@clydeco.com

Clyde & Co LLP
The St Botolph Building
138 Houndsditch
London EC3A 7AR

T: +44 (0)20 7876 5000

F: +44 (0)20 7876 5111

Further advice should be taken before relying on the contents of this summary.

Clyde & Co LLP accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary.

No part of this summary may be used, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, reading or otherwise without the prior permission of Clyde & Co LLP.

Clyde & Co LLP is a limited liability partnership registered in England and Wales. Authorised and regulated by the Solicitors Regulation Authority.

© Clyde & Co LLP 2012