MORRISON | FOERSTER

Morrison & Foerster Client Alert.

January 25, 2012

A New Chapter in European Data Protection: Commissioner Reding Publishes Long-Awaited Draft Data Protection Regulation

By Karin Retzer and Joanna Łopatowska

On January 25, 2012, Vice-President of the European Commission for Justice, Viviane Reding, officially presented the Proposal for a 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 (General Data Protection Regulation)[1] (the "Regulation"). The long-awaited legislative proposal sets out new standards and requirements for the protection of personal data in the European Economic Area ("EEA").[2] Once adopted, the Regulation will replace the existing Data Protection Directive 95/46/EC and will directly apply not only to organizations established in the EU/EEA, but also to other organizations that collect and process EU/EEA residents' personal data. The aim of the Regulation is to update the EU's 15-year-old data protection framework, and to harmonize privacy laws across the Member States.

Upon its publication, the Regulation will be sent to the Council of the European Union (an institution representing each of the national governments) and the European Parliament (composed of representatives elected by EU citizens). These two institutions must agree on a final text before the Regulation can be adopted as law; changes to the text are therefore very likely.

Although Regulations, unlike the Directives, are directly applicable to organizations and individuals, meaning there is no lengthy implementation period, it is unlikely that the final law will be adopted before the summer of 2014. The draft also provides for a transition period of two years before the Regulation becomes operational (Article 90). Thus, organizations still have some time to

[1] Available at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[2] The European Economic Area ("EEA") is comprised of the EU Member States, as well as Iceland, Liechtenstein, and Norway. The 27 Member States of the European Union (EU) currently are: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom (collectively, the "Member States"). While the Regulation will not have the same immediate direct effect in the EEA countries as in the EU countries, the EEA countries will need to issue legislation essentially the same as the Regulation.

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Anna Ferrari (650) 813-5681
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

prepare for and work to influence the likely changes.

The Regulation sets out changes to the rules applicable to almost every area of data processing. Regrettably, the "promised" lessening of administrative burdens seems quite illusionary. Organizations will not only face additional administrative and operational obligations, but will be challenged with often disproportionate standards of compliance not necessarily contributing to the protection of an individual's privacy. Liability for violations will be increased, as will the likelihood of active enforcement. Below we outline some of the key areas in which the companies operating in the EU/EEA will likely be impacted.

THE MOST IMPORTANT CHANGES

1. Scope of Application

The Regulation attempts to clarify one of the most challenging aspects of data protection: the scope of territorial application of the EU privacy laws. The Regulation will apply to any processing of personal data by a controller or processor established in the EU/EEA, as is currently the case under the Data Protection Directive. However, for controllers and processors established outside the EU/EEA, there is a fundamental change because the location of the equipment used to process data is no longer the determining factor. Instead, the Regulation would apply to any processing of EU/EEA residents' personal data when the processing relates to: (i) the offering of goods or services to such individuals, and (ii) the monitoring of individuals' behavior. (Art. 3.) This means that almost every website available in the EU/EEA will be covered by the Regulation. This was one of the key aims of the Commission.

As in the Data Protection Directive, "personal data" is broadly defined to cover any information relating to an identifiable individual. The Regulation now provides that such identification can be through all means "reasonably likely to be used" by the controller or other parties, in particular through references such as ID number, location information, online identification, or other factors. This means that most online information will be regarded as personal data, even if the data are not used to identify specific individuals.

The proposal also introduces new definitions of health data, genetic data, and biometric data. Health data are particularly broadly defined to cover any information relating to the physical or mental health of an individual or to the provision of health services to individuals. (Art. 4.)

2. New Compliance Requirements

Definition and Requirements for Consent

Consent is defined as any freely given, specific, informed and explicit indication of an individual's wishes, and can be expressed in the form of a statement or as clear affirmative action that signifies an individual's agreement to the processing of his/her personal data. This signifies that implied or tacit consent could be valid. According to the press statement, "assumed" consent is insufficient. Consent is not valid where there is a "significant imbalance in the form of dependence between the position of the individual and the controller". However, unlike earlier drafts, there is no explicit prohibition on consent in the employment relationship. (Art. 7.)

Also, unlike in previous drafts which imposed a consent requirement for all uses of personal data for direct marketing purposes, the Regulation does not include such a requirement. Therefore, it will be possible to rely on other legal bases such as legitimate interest.

The Regulation provides that parental consent will not be required to use personal data of minors over the age of 13, but this is limited to offering e-services. Controllers would need to make reasonable efforts to obtain "verifiable" consent, taking into account the available technology. In other areas, parental consent will be required for anyone under 18. (Art. 8.)

More Rights for Individuals

From the very beginning of the review of the data protection framework, Commissioner Reding stressed her intention to significantly strengthen the rights of individuals, including providing them with more information about how their personal data would be used. This translates into increased transparency obligations in the Regulation. Notice formats may be standardized across Europe and will need to be easily understandable and accessible, and include a much broader scope of information than under current laws, e.g., information about the data retention period and intended data transfers. (Art. 11.)

The Regulation also introduces a one-month deadline for responding to access requests, and gives individuals the right to obtain information about retention periods. However, where several individuals exercise access rights collectively, the deadline to respond may be prolonged for an extra month. (Art. 12.)

The proposal introduces an explicit "right to be forgotten" – the exercise of this right, highly problematic in an online environment, resulted in a great deal of debate in the course of 2011. The compromise proposed by the Commission requires a controller who has made the data publicly available to take all reasonable steps, including technical measures, to inform third parties using such data that an individual requests the controller to erase any links to the personal data and to refrain from copying or replicating the personal data. (Art. 17.)

Transfer Restrictions

The Regulation sets out that the Commissioner may issue black lists and white lists of "adequate" countries. Local data protection authorities may approve transfer contracts that the Commission may declare "generally valid", including contracts to be used by EU/EEA-based processors. These types of contracts may in fact largely resemble existing Standard Contractual Clauses. Other contractual clauses, deviating from the standard, are subject to prior authorization by the authorities. The Regulation also formally recognizes binding corporate rules as an adequate mechanism for the transfer of data outside the EEA, and sets out requirements and an approval procedure. The legitimate interest basis has been added to the list of exemptions to the requirements for data transfers to countries outside the EEA (or international organizations).

Regrettably, the Regulation does not sufficiently clarify the controller's obligations under foreign authorities' requests for disclosure (e-discovery). There only is a rather ambiguous Recital (No. 90) indicating that disclosure may be possible if justified by important grounds of public interest. However, any such conditions must be later specified by the Commission in an implementing act. Commissioner Reding in her speech did not provide any guidance but rather stressed this issue needs to be explored further.

3. Increased Liabilities

Joint and Several Liability for Joint Data Controllers and Service Providers

Under the draft Regulation, joint controllers are required to have a written agreement and must determine their respective obligations relating to data protection in such an agreement. Joint controllers, as well as processors, are jointly and

severally liable for the total amount of damages. (Art. 77.) This provision in particular may be problematic for organizations offering services to other organizations or public entities.

Substantial Statutory Obligations for Service Providers

Under the Regulation, controllers would be obliged to carefully select and supervise service providers, and put in place a detailed contract, including purpose limitations, confidentiality and security requirements, restrictions on sub-processing, return of personal data upon termination, and audit rights.

Currently only a few Member States impose statutory liabilities on processors. This new provision will drastically alter the legal risks for service providers in the processing of EU/EEA personal data, and include additional statutory obligations on processors, in particular the requirement to implement appropriate state-of-the-art security standards. Processors must also immediately notify controllers about any data security breaches. Processors may not process personal data outside of the specific documented terms. Providers who act outside of such terms will be considered controllers, and thus subject to increased liability. (Art. 26.)

Data Breach Notification

The Regulation introduces broad data breach notification requirements for any personal data security breach similar to those set out in the amended ePrivacy Directive for electronic communications service providers. There is no limitation to specific data sets, but any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to, personal data transmitted, stored or otherwise processed" needs to be notified to the national supervisory authorities. These authorities must be notified without undue delay within 24 hours of the controller becoming aware of the breach. Reasoned justification must be provided in cases of delays. Despite strong criticism that the deadline is unworkable in practice, the Commission has not changed its initial proposal. Individuals must be notified without undue delay, but only after the controller has notified the relevant authority. Individuals would not need to be informed where the controller can demonstrate that it applied appropriate measures (e.g., encryption) to protect the data. (Art. 31-32.)

4. Registration with Authorities Replaced by Accountability

Registration Replaced by Accountability

The Regulation to some extent replaces the requirement to register with national data protection authorities with a requirement to establish specific and detailed internal documentation. (Art. 28.) But the much-proclaimed easing of administrative burden does not correspond with the provisions of the Regulation. Controllers will be required to carry out onerous impact assessments prior to processing activities involving particular risks, such as profiling; processing sensitive, genetic and biometric data; or creating large databases of children's data. (Art. 33.)

The individuals concerned, and representatives such as works council, will need to be consulted.

This goes hand in hand with comprehensive requirements to demonstrate compliance, for example through internal policies. Codes of conduct, certification mechanisms, and data protection seals are given greater weight under the Regulation, and those obligations may become more significant.

Prior Consultation with Authorities

Where there are particular risks involved in data processing, controllers would still be required to consult with authorities. Such "consultation" may be relevant where processing involves: (i) analytics or ratings based on work performance, credit history, location information, health information, personal preferences, or behavioral or sensitive data; (ii) CCTV and video surveillance information; (iii) or large quantities of data on children, biometric or genetic data. (Art. 34.) In practice this may cover many types of processing operations and seems to suggest that those controllers will still be obligated to notify the data protection authorities.

Data Protection Officer Mandatory for all Larger Organizations

The Regulation would require all private sector organizations with more than 250 employees or those undertaking "risky" monitoring of individuals, as well as all public sector organizations, to appoint a data protection officer ("DPO"). Group companies may appoint a single data protection officer. The DPO may be an employee or contractor, and must serve a minimum of two years. Appointment of the DPO needs to be reported to the authorities and his/her contact details should be made publicly available. (Art. 35-37.)

5. Strengthened Enforcement

Stronger and Harmonized Powers of National Supervisory Authorities

The Regulation substantially strengthens the powers of national supervisory authorities, and also provides for a mechanism to ensure that only the data protection authority in the country of the controller's central operations is in charge.

The Regulation would introduce mandatory mutual assistance between these data protection authorities and a new "consistency" mechanism to ensure uniform application and enforcement of the Regulation. The Regulation replaces the existing EU-level consortium of national data protection authorities, the Article 29 Working Party ("WP29"), with a new European Data Protection Board. But as the composition of the Board will be the same as the WP29, this change is rather symbolic.

Right of Action and Right to File Claims or Complaints

Under the Regulation, individuals are explicitly entitled to file a complaint either in the country where they reside or in the country where the controller or processor is located. Importantly, consumer, privacy, and similar associations would be able to lodge complaints with the supervisory authorities and seek judicial redress. These changes will greatly facilitate judicial recourse for the individuals, but may also lead to an increase in litigation, a consequence that companies should take into account when implementing compliance measures.

Tougher Administrative Sanctions for Violations

The Regulation also sets out much-debated administrative sanctions, including fines of up to 2% of annual worldwide turnover. The imposition of fines is mandatory, without any discretion by the supervisory authorities – "the supervisory authority shall impose a fine". However, this is softened by a provision setting out that in case of a first and unintentional noncompliance with the Regulation, no sanction shall be imposed, but only a written warning be issued, where, e.g., a company with "fewer than 250 employees is processing data only as an activity ancillary to its main activities." (Art. 78.)

THE WAY FORWARD

The publication of the draft Regulation comes more than two years after the review of the data protection framework started. Before it presented this official proposal, the European Commission's Directorate-General for Justice had to consult with the other Commission Directorate-Generals and services. It appears that the final draft has been slightly amended to accommodate concerns raised by other Commission Directorate-Generals and services. It is very likely to undergo more changes after review by the Council and the Parliament. The coming months will definitely bring interesting discussions as a balance between advocating amendments that may promote business and economic innovation and safeguarding people's right to privacy at all costs is sought.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.