MORRISON | FOERSTER

Morrison & Foerster Client Alert.

December 6, 2011

The Review of the EU Data Protection Framework: A quick guide to EU lawmaking

By Karin G. Retzer and Joanna Łopatowska

It has been more than two years since the review of the EU data protection framework officially started. Despite several announcements from the European Commission ("Commission") and growing expectations from the business sector, the publication of the draft law has been continuously delayed. The European Commission has said it plans to publish its proposal by the end of January 2012.[1] Timing has become a key factor in the review. But there is still a long way to go before any proposal becomes law. The process of adopting EU laws is lengthy, complex, and sometimes unclear for businesses established outside the EU.

Below we outline the main stages that govern EU lawmaking procedures to help organizations prepare for when changes to EU data protection laws are likely to become effective.

We also summarize some of the implications of changes considered by the Commission's data protection service. The draft regulation, if adopted "as is," would broaden the geographic scope of EU data protection law and entitle individuals to file complaints at their place of residence, irrespective of the location of the organization holding the data. While leaving many of the principles intact, the regulation would substantially increase liabilities, particularly for service providers, and allow for collective redress. The draft also proposes broad security breach notification requirements for all data types and across sectors.

WHO ARE THE PLAYERS?

There is no single body acting as a legislature in the EU. Instead, the power to adopt laws is spread out among three institutions:

- **The European Commission**: a body made of 27 Commissioners (politicians appointed by each EU country) and supporting staff that has the expertise and legal and technical knowledge to prepare draft laws;

[1] A likely date could be January 25, which is a Wednesday, the day the Commission generally formally adopts its decisions and three days before the sixth annual EU data protection day on January 28, 2012. If all goes according to schedule, the choice of date would be a symbolic mark of the importance of the review.

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

- **The European Parliament**: a directly-elected body composed of 751 members ("MEPs") elected once every five years by voters across the EU;
- **The Council of the European Union**: the main decision-making body representing the governments of EU Member States and composed of 27 national ministers. Unlike national governments, it does not have a fixed composition, but depending on the laws to be adopted the composition changes. For example, to adopt the data protection law, Ministers responsible for data protection in their national jurisdiction (most commonly internal affairs or justice) meet.

THE PROCESS, STEP BY STEP

In the EU, the Commission has the power to initiate legislation. Thus, the Commission must first prepare, formally adopt, and publish a draft law. Before that happens, it takes months, and sometimes years, to consult various private groups and public institutions, prepare the draft, and assess its potential economic, social, and environmental impact. The Commission is currently still in this first stage of reviewing the EU's data protection law.

Once the Commission has finalized its proposal, it sends the draft law to the Parliament and to the Council, which review the proposal in parallel and suggest amendments.

According to the procedure established in the treaties governing the EU, to adopt data protection laws the Council and the Parliament must reach an agreement on the final wording of the text. Unlike national parliaments, the European Parliament does not have self-standing legislative powers; *i.e.,* it cannot pass laws alone, but must act in co-operation with the Council. In this procedure, called the "ordinary legislative procedure" both institutions share equal powers to adopt the law. This means that they must work out a robust compromise. Achieving this may take many months.

There is no time limit to adopt the law. The road to reaching a compromise may, but does not have to, include three stages:

1. In the first stage, the Parliament, voting by a simple majority, proposes to the Council a revised text with amendments.

    a. If the Council approves the Parliament's position, then the law is adopted.

    b. If not (which is usually the case), the Council must propose its own position, adopt an amended text in the form of a so-called 'common position' and pass it back to the Parliament with detailed explanations.

If the Parliament agrees with the Council's proposal, the law is adopted. According to the official Parliament statistics from the previous legislature (2004-2009), 72% of agreements were reached in the first stage, with the average length of the procedure being about 15 months. The longest procedure took almost 48 months (or 4 years).

2. If the Council and the Parliament cannot agree upon amendments, the procedure goes into the second reading. The Parliament and the Council can again propose amendments.

    a. If the Parliament approves the Council's proposal in full, or does not express an opinion, the law is adopted.

    b. The Parliament may modify the Council's proposal and pass it back for Council's consideration.

    c. If the Parliament rejects the Council's text, the procedure fails and the institutions must move on to the third stage. This may also happen if the Commission rejects the amendments. In such a case, the Council does have the power to act unanimously to pass the law if it so chooses.

Despite the official deadline to reach a compromise within four months, the Parliament's statistics indicate that 23% of agreements were reached in the second reading and the average procedure took about 31 months; the longest procedure took 108 months (or 9 years).

3. If an agreement cannot be reached, the institutions convene the Conciliation Committee. It is made up of 27 representatives of the Member States, an equal number of MEPs, and the relevant Commissioner. The Committee revises the two positions and draws up a joint text.

    a. If within six weeks there is no agreement on a common text, then the law has failed.

    b. If the Committee approves the text, the Council and Parliament must in addition formally approve it. If either fails to do so, the law is not adopted.

The Parliament statistics indicate that only 5% of agreements went through the conciliation procedure, and the average procedure took about 43 months; the longest procedure took 159 months (or 13 years).

The EU data protection review is likely to impact on many different areas within the EU and, as such, will involve many discussions over many months before the EU institutions agree on a common text. It is not yet possible to predict whether agreement will be reached in the first reading or whether the procedure will develop into further stages.

WORK BEHIND THE SCENES

The final position of the Parliament is adopted during a plenary session gathering all 751 members of Parliament or "MEPs." The Parliament holds twelve full plenary sessions per year in Strasbourg and six "mini-plenary" sessions in Brussels. Not all of these politicians are equally engaged in the process of adopting the laws. This would be extremely impractical, given the number of MEPs and the amount of legislation the EU produces. Instead, one MEP is tasked with preparing the Parliament's position. To prepare this, the MEP, called the 'Rapporteur,' works within a smaller grouping of MEPs in a Committee. For the review of the EU's data protection law, this will most likely be the Committee on Civil Liberties, Justice and Home Affairs.

The Rapporteur will collaborate with other MEPs from other relevant committees (such as Legal Affairs, Industry, Research and Energy, and Internal Markets, for example) who prepare opinions that complement the main report prepared by the Rapporteur. The Rapporteur will also meet with representatives of the Council to ensure that the work that takes place simultaneously in both institutions can be aligned. At this stage, it is a common practice for interested organizations to meet the Rapporteur and other engaged MEPs and present their arguments and ideas for amendments.

Once ready, the draft report is subject to amendments by all other MEPs and must be then approved by the main Committee and voted on by all MEPs at a plenary session. Even at this stage, interested organizations can present their views and influence the draft.

OTHER STAKEHOLDERS

Other stakeholders are also involved in this process, such as:

1. The **European Data Protection Supervisor**, an independent supervisory authority devoted to protecting personal data and privacy and promoting best practices in the EU institutions and bodies.

2. **Article 29 Data Protection Working Party** (WP 29), a network composed of representatives of the data protection authorities of each Member State, the European Data Protection Supervisor, and the European Commission.

These bodies have no role in adopting the EU laws, but they are consulted and play a very active role in interpreting and influencing EU laws on data protection.

DIRECTIVE OR REGULATION: WHAT DIFFERENCE DOES IT MAKE?

In recent months there has been a lot of speculation about the form a new law would take: a directive or a regulation. The first comprehensive EU measure introduced on data protection was a directive (EU Data Protection Directive 95/46/EC). It is now quite clear that the Commission will publish two legislative proposals: a general regulation on data protection and a directive on the processing of personal data by competent authorities for the purposes of criminal justice.

The difference between a regulation or a directive and why one is used rather than another may not always be clear.

- **Regulations** are measures addressed to all Member States and are directly applicable in all Member States. This means they do not require any additional implementation in national legislation. Regulations apply in all Member States in the same wording and scope as they are adopted by the EU institutions. Put another way, once a regulation is passed, it is the law across all of the EU Member States exactly as it is written.

- **Directives** set out specific objectives that must be reached, and Member States need to adopt national implementation legislation. Member States are left with the choice of form and method of implementation. In principle, directives are not directly applicable to organizations. Often language used in the directives is more general and vague in order to allow Member States to adapt the legislation to their particular national context. To date, most legislation adopted in the area of data protection has been via directives; therefore national laws which give effect to the directives often vary and are inconsistent.

Directives usually include a set timeframe by which Member States must have implemented the required measures at the national level. Regulations do not require such deadlines, as they are directly applicable and come into force on the date specified in the regulation or, if no date is specified, on the twentieth day following publication in the Official Journal. Whether a regulation or directive is used will depend on the law's objectives.

A regulation allows a comprehensive approach to be introduced across EU Member States to address issues of fragmentation in the way data protection rules have been implemented. In addition, a regulation is viewed as an appropriate response to new perceived risks that have come about as a result of developments in technology.

CHANGES INCLUDED IN THE DRAFT REGULATION

The proposals included in the draft regulation that is currently being finalized by the European Commission would substantially strengthen the EU's powers to combat data protection breaches, similar to those it exercises in competition matters.

The draft Regulation would expand the applicability of EU data protection law to any processing of data relating to EU/EEA residents where the processing is "directed" at such individuals or a service to monitor their behavior.

Some of the major changes introduced in the regulation relate to enforcement. The regulation provides for additional sanctions, including granting national data protection authorities with the power to impose fines of up to 5% of a

company's annual turn-over. New offences are introduced and the rights of individuals and consumer and similar associations to file complaints are expanded. It introduces mandatory mutual assistance between Member State authorities and a new "consistency" mechanism to ensure uniform application and enforcement of the Regulation. The Regulation replaces the existing consortium of data protection authorities, the Article 29 Working Party, with a new European Data Protection Board, the secretariat of which would be run by the European Data Protection Supervisor.

The regulation also introduces joint and several liability for controllers and processors, as well as for joint data controllers. Joint controllers are expected to address their respective compliance obligations though appropriate contracts.

A detailed contract is required with all service provides who may only act upon written instruction from customers, and data processors are subject to additional statutory obligations. The Regulation also clarifies that service providers that act outside the strict mandate of the controller will be considered data controllers.

Importantly, the draft regulation provides consumer, privacy, and similar associations with rights to lodge complaints with the DPAs and seek judicial redress, and substantially strengthens the powers of national DPAs.

The regulation also includes a definition of consent, which must be a freely given, informed, and explicit indication of the data subject's wishes. This implies that opt-out consents will not be sufficient to authorize data processing. In addition, consent is no longer a legal basis for data processing in the employment context. Consent from children, that is any minor below the age of 18, is not valid without parental consent or authorization.

A new breach notification requirement is introduced, under which companies have 24 hours to notify data protection authorities and the affected parties in cases where there is a personal data breach. These requirements are similar to (and equally broad as) those included in the ePrivacy Directive for electronic communications service providers.

Impact assessments, extensive documentation requirements, and the obligation imposed on larger organizations to appoint data protection officers add to compliance burdens. Red tape is not likely to go away as national authorities still need to be "consulted" about many activities.

In relation to international transfers of data, additional criteria are also included for the adoption of adequacy decisions, where data transfers to countries outside the EEA are permitted without a specific legal mechanism. The legitimate interest basis for processing data has been added to the list of exemptions to the requirement for data transfers to countries outside the EEA. Critically, requests from "foreign" courts or authorities may not be recognized unless there is a mutual assistance treaty or international agreement allowing for such recognition.

The much debated "right to be forgotten" is expressly included and strengthens data subjects' access rights and rights to request erasure of data.

The proposal provides for additional accountability and "comprehensive responsibility" for data protection and a requirement to "demonstrate" compliance, for example through internal policies. Codes of conduct, certification mechanisms, and data protection seals are given greater importance.

The proposal, to some extent, would replace the requirement to register with national authorities with a requirement to establish specific and detailed internal documentation and to undertake impact assessments prior to any data processing. Where there are particular risks, the DPAs will still require "consultation," includng: (i) analytics or ratings based on work performance, credit history, location, health, personal preferences, and behavior; (ii) processing of sensitive data; (iii) CCTV; and (iv) large quantities of data on children and biometric or genetic data. All public sector organizations, as well

as larger private sector organizations with more than 250 members of staff or private sector organizations undertaking "risky" monitoring of data subjects, are required to appoint a data protection officer. The officer may be an employee or contractor and must serve a minimum of two years. Appointment of the officer needs to be notified to the authorities, and the public and all individuals should be provided with contact details for the data protection officer.

IS PLANNING FOR THE CHANGES POSSIBLE?

Before the European Commission finalizes and formally announces any draft law, discussions on timing are pure speculation. The timing of the procedure will also be subject to both the Parliament's and the Council's calendars. These calendars are continuously changed, and, as a result, matters under consideration can be prolonged.

It is reasonable to expect that the discussions will take 2-3 years after the Commission publishes its proposal before the final law will be adopted. There is a common expectation that the law should be adopted before the Parliament's term ends in summer 2014. It may then take several months before any new law will enter into force.

What is certain is that the new proposed framework will be debated in detail, involving not only the interests of the Member States, but also balancing the interests of business and the rights of individuals. The EU institutions will most likely be caught between promoting business and economic innovations to boost the EU economy and attract business, and the protection of the people's right to privacy and personal data. All interested parties will be provided an opportunity to put forward their views. All of which suggests, however, rather long discussions and plenty of time to adapt in advance of any law being introduced.

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.