Morrison & Foerster Client Alert

13 November 2013

The Draft EU General Data Protection Regulation: Where We Are Now and Where We Are Going

By Karin Retzer and Joanna Łopatowska

On October 25, 2013, the European Council concluded that the new Data Protection Framework should be adopted in a timely manner in order to strengthen consumer and business trust in Europe's digital economy. The Council did, however, refuse to commit to adoption by early next year.

This conclusion follows on the heels of the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee vote setting out its position on a compromise text of the draft Regulation on October 21, 2013. After some 18 months of intense discussions and lobbying, the compromise text was passed by the LIBE Committee with a 49-3 majority. The compromise text was heavily influenced by the revelations of the surveillance activities of the U.S. National Security Agency (NSA).

Together with the compromise text, the LIBE Committee adopted a "negotiation mandate" to start official talks with the Council, in view of adopting a joint text. This so-called trilogue negotiation procedure will also involve the European Commission.

Adoption of the new Regulation may still be some time away, but the clock is ticking.

Below we set out some of the most important changes for private sector organizations proposed by the LIBE Committee. An unofficial version of the compromise text has been published by Rapporteur Jan Philipp Albrech.

AN OVERVIEW OF THE MAIN CHANGES

Territorial Scope (Article 3): The LIBE Committee's text extends the scope of the Regulation to any organization (including service providers/data processors) collecting personal data of individuals in the EU/EEA when: (i) offering products or services (including free services and products and services available online) to

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
James R. McGuire	(415) 268-7013
Daniel F. Muto	(858) 720-7959
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Sherman W. Kahn	(212) 468-8023
Mark P. Ladner	(212) 468-8035
Peter McLaughlin	(212) 336-4290
Michael B. Miller	(212) 468-8009
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

L. 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
Andrew M. Smith	(202) 887-1558
Nathan David Taylor	(202) 778-1644

EUROPE

Brussels

Joanna Łopatowska	32 2 340 7365
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Caroline Stakim	44 20 7920 4055
David Varney	44 20 7920 4058

ASIA

Beijing

Gabriel Bloch	86 10 5909 3367
Jingxiao Fang	86 10 5909 3382
Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808

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

individuals in the EU/EEA or (ii) monitoring such individuals. As a result, most websites available in the EU/EEA will be covered. How this will be enforced in practice remains unclear.

Most significantly, service providers (data processors) would also be directly subject to the Regulation, which not only goes far beyond the Commission's proposal but is unclear as to when data processors will be covered. Whereas Recital 20 clarifies that the Regulation will cover data controllers that offer goods or services or target EU/EEA residents (and not just any individuals in the EU/EEA), there is no such clarification regarding data processors, which seems to imply a much broader application.

Personal Data (Article 4): The LIBE Committee's compromise text also broadens the definition of "personal data" to cover data that presents the possibility of *identifying or singling out* an individual, directly or indirectly. Device identifiers, IP addresses and location data will be regarded as personal data. Although pseudonymous data is considered to be personal data, they are subject to somewhat less burdensome requirements.

Notice (Article 13a, 14): The LIBE Committee completely transforms the way of providing a privacy notice.

It proposes a two-step process: first, mandatory icons must be shown when collecting data; the icons must appear as follows:

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are collected beyond the minimum necessary for each specific purpose of the	
	No personal data are retained beyond the minimum necessary for each specific purpose of the processing	
	No personal data are processed for purposes other than the purposes for which they were collected	
	No personal data are disseminated to commercial third parties	
	No personal data are sold or rented out	
	No personal data are retained in unencrypted form	

Second, a detailed notice (including security measures, retention period, transfer mechanisms, profiling, disclosure to public authorities, etc.) needs to be provided. But if this requirement were to apply in all offline and online contexts (including on any website or mobile app, in emails, signage, or on paper data collection forms, for example) this will not only be burdensome on businesses, but could also be irritating to individuals who will be bombarded with multiple icons as well as a detailed text. This can lead to a nuisance effect. The icons are somewhat over simplistic, and will still need to be used even if data controllers do not engage in certain processing or process data in other ways not shown in the icons.

Consent (Article 7): The LIBE Committee also imposes additional restrictions on consent. Consent to data processing must be explicit by default (for both sensitive and non-sensitive data) and specific to a very narrow purpose. An individual's consent shall cease to be valid when the original purpose of data collection ceases to exist or where data are used for a secondary purpose. In addition, provision of additional services cannot be made conditional upon providing consent. On the face of these restrictions, providing free online services in return for some marketing would no longer be possible.

Legal Basis (Article 6): Despite some welcome amendments, such as extending the definition of "legitimate interest" to cover the processing of business contact details, direct marketing relating to the organization's own or similar products, postal marketing, and sharing of data with EU/EEA affiliates, the LIBE Committee has significantly limited the use of the legitimate interest legal basis for processing data. The legitimate interest basis may be used where the company's interests meet the "reasonable expectations" of the individual, based on his/her relationship with the data controller.

In contrast with an earlier draft of the Regulation proposed by the European Commission, the legitimate interest legal basis can no longer be used as a means to transfer data outside the EU/EEA. This means that single data transfers (e.g., for concrete internal investigation purposes) will require burdensome contractual arrangements, Safe Harbor certification, or an adequacy finding.

The Council, on the other hand, has been in favor of maintaining the current understanding of legitimate interest, and also proposes to extend it to prevention and monitoring of fraud, which would cover whistleblowing hotlines and internal investigations.

Profiling (Article 20): The compromise text includes stricter conditions for the use of data for profiling purposes. Notices about profiling must be "highly visible" and individuals must have the right to object to being profiled.

Where profiling results in legal effects or significantly affects an individual's rights, it will only be allowed where the individual's (explicit) consent is obtained; where provided for by law; or where necessary to conclude or perform a contract. There is no further clarification on the meaning of "significantly affects" but for an exception stating that profiling based on pseudonymous data is not presumed to result in significant effects. This could bring more flexibility to analytics companies. However, where such profiling is based on aggregated pseudonymous data originating from different sources, and if it were possible for the data controller to link data to a specific individual, such profiling would be possible only with explicit consent. As many profiling activities do involve data from multiple sources, it is difficult to foresee the practical significance of this provision.

Compliance Obligations (Article 22): There is less red tape in some areas and more of a risk-based approach to compliance in the compromise text. This means there are no prescriptive internal documentation requirements. Instead, internal practices must take into account the risks of processing data, the nature of the data processed, and the use of

current technology. The strict 24-hour deadline for security breach notification has been removed. Instead, breaches would need to be reported without "undue delay." There is no need to consult the data protection authority (DPA) in cases of risky processing if a data protection officer (DPO) has been appointed. However, burdensome obligations for data controllers remain and this could increase compliance costs for companies and not necessarily directly benefit individuals. For example, the LIBE Committee requires impact assessments for all data controllers and data processors in a broad range of situations (including where personal data of more than 5,000 individuals are processed within a 12-month period) and a bi-annual review of compliance policies.

Data Protection Officer (Article 35): Appointment of a DPO is mandatory for any organization processing personal data of more than 5,000 individuals within a 12-month period. Multinationals may appoint a "main responsible" DPO, provided the DPO is easily available from each location/establishment. There is a minimum term of appointment of 4 years for employees and 2 years for external contractors. As the DPO is protected against dismissal, organizations will have to carefully consider who to appoint. On the positive side, if a DPO is appointed, consulting the DPA in case of risky processing would no longer be required; the matter could be referred to the DPO. The Council favors optional appointment as a general compliance choice, but this would not provide relief from administrative requirements.

Employee Data (Article 82): Under the compromise text, Member States retain the right to adopt employee data protection laws, however, minimum common standards would need to be adopted across the EU/EEA. For example, consent to data processing in the employment context is invalid if it has not been freely given. This provision would cover processing of employee data in most situations. The DPAs have continuously argued that because an employee is in a subordinate position, he or she cannot freely consent (see the EU Article 29 Working Party's Opinion on the processing of personal data in the employment context). Processing must be linked to purpose for data collection and must remain within the employment context. Use of employee data for secondary purposes would be prohibited. It is unclear whether employers could obtain employee consent for such processing (which would be difficult) or whether such processing would generally be prohibited under any circumstances. Importantly, investigations would be permitted only where related to employees' criminal behavior, which significantly limits the possibility of performing employee monitoring for any other purposes. Finally, blacklisting of employees based on political or trade union membership is prohibited. Although no significant limitations are placed on sharing of employee data with other EU affiliates, cross-border restrictions will still apply.

Data Processors (Article 26): The text proposed by the LIBE Committee maintains prescriptive requirements for data processing contracts. The only positive change is that there is no need to list all sub-processors in the contract; details can be limited to "determining the conditions for enlisting another processor" with prior permission of the data controller. This provision allows for more flexibility in outsourcing contracts and, in particular, in the cloud computing context. On the negative side, the LIBE Committee kept joint liability for data processors (and data controllers) if they act contrary to or outside the processing agreement or become the determining party for the processing. Burdensome contractual requirements and joint liability for data processors make outsourcing very difficult in practice.

Cross-Border Transfers (Article 41-42): In reaction to the NSA surveillance activities, the LIBE Committee has on numerous occasions called for tightening of the rules on international data transfers and more scrutiny of existing data transfer mechanisms, including, in particular, the Safe Harbor Framework. This has resulted in significant limitations on cross-border data transfers in the compromise text.

Under the compromise text proposal, the Safe Harbor Framework and the Commission's Model Clauses will expire 5 years after the Regulation enters into effect, or earlier if so decided by Commission. DPA data transfer approvals based on Binding Corporate Rules and other transfer contracts will automatically expire within 2 years after entry into force of the Regulation (unless earlier amended, replaced, or repealed by the DPA). The legitimate interest basis for cross-border transfers has been removed, which will have significant implications. The Commission will also have the authority to blacklist countries or sectors if local laws allowed for governmental access to personal data without EU/EEA authorization. This is a very explicit example of how the NSA operations have influenced the tightening of the rules by the LIBE Committee.

Regulatory Disclosure (Article 43a): The LIBE Committee proposes that DPA approval be required for any transfer in response to a foreign (i.e., non-EU/EEA) regulatory or court request for personal data, unless international treaties allow for such disclosure. This means that any foreign company holding EU/EEA personal data will need to ask for DPA approval before allowing access to such data by foreign law enforcement agencies. This is clearly a move against the NSA or similar practices to request access to data from online companies in possession of massive EU/EEA data. This provision certainly requires greater clarity. The way it reads at present creates a risk that transfers to Safe Harbor recipients may effectively be blocked as such data are vulnerable to U.S. governmental disclosure. The LIBE Committee adds that, in cases of jurisdictional conflict, EU law should always take precedence.

This puts foreign companies between a rock and a hard place. Companies responding to regulatory requests before obtaining DPA approval will risk non-compliance with the Regulation. On the other hand, such companies will risk non-compliance with foreign laws – due to the lengthy DPA approval process they will not be able to comply with tight deadlines. By adding this provision, the LIBE Committee has effectively re-inserted the Commission's original proposal that was later removed from the proposal after intensive lobbying.

The "One Stop Shop" (Article 56): "One stop shop" means that the DPA in the jurisdiction where a company has its "main establishment" will be responsible for oversight of that company's data processing activities, irrespective of where the processing takes place. This approach was set out in the Commission's proposal.

The LIBE Committee appears to agree with the concept in principle but interprets it differently. It favors what it calls a "lead DPA" system for enforcement. The lead DPA – in the jurisdiction where a company has its main establishment – would be the only authority to make legal decisions but would have to cooperate with DPAs in the other jurisdictions where processing is carried out. This dilutes the Commission's original idea of ensuring more consistency in enforcement by allowing both companies and consumers to have a single point of contact.

The Council, the Member State representation, supports the Commission's proposed one stop shop mechanism but has not reached an agreement on the details. For example, some countries (e.g., Austria, Belgium and France) prefer that decisions are made through a formal co-decision procedure including the lead DPA and other DPAs. Other countries (e.g., Ireland, Luxembourg and Portugal) favor decision-making powers assigned to the lead DPA with other DPAs in an advisory role.

Sanctions (Article 79): The further tightening of sanctions is a good example of the approach pursued by the LIBE Committee. Under the compromise text, any violation of data processing requirements would be subject to sanctions instead of a tiered, violation-specific approach. These sanctions include fines of up to 5% of annual worldwide turnover (increased from the Commission's proposal of 2%) or EUR 100 million, whichever is greater. Alternatively (supposedly for

less serious violations), DPAs will order regular data protection audits or issue a written warning for a first instance of unintentional noncompliance. Imposition of one of these sanctions is mandatory. However, the LIBE Committee does set out a list of mitigating factors, including the seriousness of the violation; whether the violation is repetitive in nature; any intended or actual financial gains; and cooperation with enforcement authorities.

WHAT HAPPENED

The Commission published its General Data Protection Regulation ("Regulation") to revise the EU's existing data protection framework back in January 2012 (see our client alert *A New Chapter in European Data Protection: Commissioner Reding Publishes Long-Awaited Draft Data Protection Regulation*). The Regulation, once adopted, will apply to all EU Member States and replace the existing Data Protection Directive, adopted in 1995.

Following publication of the Regulation, the Commission sent the text to the European Parliament, composed of directly elected members representing EU citizens, and to the Council, representing the EU Member State governments. Both institutions will review the text and may propose amendments (see our client alert *The Review of the EU Data Protection Framework: A quick guide to EU lawmaking*) and eventually pass a final text into law in a co-decision procedure.

WHAT TO EXPECT

The LIBE Committee's compromise text sets out its formal position which is ready for the trialogue negotiations. The Council of Ministers meeting scheduled for December 5-6, 2013, which will gather ministers in charge of justice and home affairs, will be an indicator of the Member States willingness to move ahead quickly. But no firm commitments have been made so far: EU leaders only have committed to have the new Data Protection Framework adopted by 2015, but they have not specified whether the target date should be at the beginning or rather at the end of 2015.

Important changes will occur during 2014 in the EU. First, in May 2014, elections will be held in all Member States to elect the new European Parliament. Following the elections, a new Commission will be appointed and this may take several months.

The composition of the new Parliament is unclear, as is that of the new Commission. It is unlikely that Commission Vice-President Viviane Reding will remain the Commissioner in charge of data protection, and it is unclear whether Jan Philipp Albrecht (and other members of the LIBE Committee negotiating team) will be reelected. The LIBE Committee, however, will continue to the lead on the data protection framework negotiations.

The trialogue is a closed process, but Albrecht has pledged to provide regular updates on the developments. There are no formal rules regarding timing or methods. It is still possible to try to influence the process through targeted lobbying by talking to governments and their Permanent Representations in Brussels or by approaching some of the more business-friendly members of Parliament's negotiating team. Parliament has scheduled a first full plenary reading of the Regulation for March 2014.

HOW TO INFLUENCE THE PROCESS

There is still some way to go before the final Regulation is adopted. This lengthy process means there is ample opportunity to influence the various parties involved in the negotiations, as well as to pull together industry alliances to increase the impact of such lobbying.

The Council, with its generally more business-friendly position, is likely to be the most effective target for businesses. Although Parliament has been clear on its strict, human rights-oriented position, established lobbying channels and a commitment to keep the negotiation process more or less transparent mean that lobbying Parliament is an easier and potentially effective route to take.

Efforts to lobby the Commission will probably be less effective; it is likely that Vice-President Viviane Reding will want to tightly monitor and control the process and, in any event, it is not the Commission that has the final say on the Regulation, but the Council and Parliament together. Reding has also warned that "excessive lobbying can be counter-productive."

In the trialogue negotiations, the Council will be led by a representative of the government holding the EU Presidency – currently Lithuania, then Greece from January 1, 2014, and Italy from July 1, 2014. While Lithuania has kept the data protection reform relatively high on the EU agenda, Greece's announcement on its Presidency priorities for the first half of 2014 did not include the Regulation.

For all parties, the most effective approach is to identify the areas of the compromise text that will be harmful to all businesses and propose alternative workable provisions. It may also be worth highlighting some of the contradictions in the text, for example, provisions strengthening enforcement of data protection laws but other provisions abolishing database registration fees which many national DPAs rely upon for their annual income. Concerns about contradictions have already been raised by the UK Information Commissioner's Office.

Targeting Member State governments represented in the Council in order to influence the negotiations is most effectively done by lobbying the responsible ministries or the head of state offices in Member States. In addition, each Member State has an ambassador to the EU and some countries have dedicated staff responsible for broad policy areas. The larger, more influential Member States (e.g., France, Germany, the Netherlands, Spain andthe UK) and the country that holds the Council Presidency will be the prime targets. It is understood from the recent Council summit that the UK and Sweden oppose any swift adoption of the Regulation and have raised many concerns about its provisions.

LOOKING AHEAD

The LIBE Committee's compromise text sets out the European Parliament's informal view on the future Regulation and is a step closer towards its adoption. However, the significance of the text should not be overestimated. Before the Regulation becomes law, many steps must still be taken. Political compromises to be reached are difficult to predict, although the compromise text provides a starting point for influencing both the Council and the Parliament.

The final text will very likely differ from the current compromise text, which remains far from perfect. But in any case, the future Regulation will significantly impact how companies collect, use and share personal data both within the EU/EEA and globally. It is becoming clearer that the main principles of the Regulation will remain, including the strengthened enforcement provisions and more limitations on rather than facilitations for data transfers. Even if the Regulation is adopted by or in 2015, companies will still have approximately two years to come into compliance. However, companies should already be considering the potential impact of the Regulation on how they intend to process personal data going forward, what changes will likely be required in their data protection policies, what resources will need to be allocated to data protection compliance, and how to prioritize areas where the impact of the Regulation could be the most significant.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. 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 10 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 treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or 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. Prior results do not guarantee a similar outcome.