Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 13, NUMBER 11 >>> NOVEMBER 2013

The European Parliament's LIBE Committee Adopts Revised Data Protection Regulation: Changes May Significantly Impact Businesses

By Olivier Proust, of Field Fisher Waterhouse LLP, Brussels.

Introduction

On October 21, 2013, the Committee on Civil Liberties, Justice and Home Affairs ("LIBE") of the European Parliament (the "Parliament") voted in favor of several compromise amendments brought to the European Commission's (the "Commission") proposal for a Data Protection Regulation. The amendments were adopted in less than an hour by an overwhelming majority (49 votes in favor, one opposed and three abstentions), ending in applause (*see report in this issue*).

The LIBE vote follows the Commission's publication, on January 25, 2012, of a proposal for a data protection reform package composed of a Regulation on the protection of personal data (the "Regulation")[1] (*see analysis at WDPR, February 2012, page 4*) and a Directive on the processing of personal data for law enforcement purposes. Intense lobbying followed this publication, resulting in nearly 4,000 amendments being tabled (*see WDPR, May 2013, page 22*). Jan Philipp Albrecht, the designated rapporteur for the draft Regulation, was tasked with the heavy duty to review these amendments and propose a compromise version of the text that would serve as a basis for the negotiations between the Parliament and the Council of Ministers of the European Union (the "Council").

The legislative procedure is not yet over, but the swift adoption of the compromise amendments certainly paves the way for the adoption of a stronger data protection framework in the European Union.

The context in which this text was debated in Parliament is also unprecedented. Following the recent revelations by Edward Snowden regarding the alleged interception of electronic communications of EU citizens by the U.S. National Security Agency (the "NSA"), discussions about the Regulation have taken a more political turn (*see WDPR, July 2013, page 18*). Seldom before has privacy been the focus of so much attention in the European Union.

In the weeks to come, discussions about the Regulation will take on a new dimension as the three main EU institutions (the Commission, the Parliament and the Council) enter into a trilogue in order to reach a consensus over the text. The adoption of the compromise amendments gives us a better indication of the key provisions that will shape these negotiations.

The LIBE Committee's swift adoption of the compromise amendments certainly paves the way for the adoption of a stronger data protection framework in the European Union.

This Special Report briefly explains why the vote in the LIBE Committee is an important milestone in the adoption process. It also analyzes some of the key compromise amendments that were adopted by the LIBE Committee. Finally, it discusses the next steps.

Why Is the Vote of the LIBE Committee Important?

The vote by the LIBE Committee is not the final act in the legislative procedure, and there are still several steps along the way before the Regulation comes into force. Nonetheless, this vote is important for three main reasons.

First of all, the data protection reform package is the most ambitious piece of EU legislation in the field of privacy to be introduced since the adoption of the 1995 Data Protection Directive (95/46/EC). Among other things, it aims at better harmonizing privacy legislation within the European Union, reinforcing the rights of individuals, strengthening the enforcement powers of the data protection authorities and modernizing the legal framework to better address the technological challenges of the 21st century.

Second, the sheer length and complexity of the Commission's initial proposal, followed by the exceptionally high number of proposed amendments, led many commentators to predict that it would take years of endless negotiation before this text would ever get adopted. Who would have imagined that the LIBE Committee would succeed in less than a year to consolidate nearly 4,000 amendments into just 104 compromise amendments? This is certainly a remarkable achievement. The vote also sends a strong signal to businesses, governments and stakeholders that the Parliament considers this to be a major piece of legislation.

Third (and this may be the most important element here), the context in which the data protection reform package was examined is unprecedented. Following the revelations by Snowden about the NSA's alleged interception of electronic communications in the European Union, privacy has suddenly and unexpectedly become a priority issue for EU leaders and decision-makers. For example, the LIBE Committee is currently conducting hearings in the Parliament in relation to the electronic mass surveillance of EU citizens.[2] The "PRISM scandal" has almost certainly influenced the manner in which the LIBE Committee adopted its compromise amendments.

Analysis of the Key Compromise Amendments Adopted by the LIBE Committee

Overall, the adopted compromise amendments do not alter significantly the Commission's initial proposal. The structure, spirit and content of the text remain largely untouched. Nevertheless, when analyzed in more detail, some significant changes were introduced to the text, which may have an important impact on businesses.

A Regulation, Not a Directive

"One continent, one law". This has been the constant leitmotif used by EU Commissioner Viviane Reding in the last year and a half. Since the beginning of the legislative procedure, the Commission has made it very clear that the purpose of this reform is to build a strong, harmonized legal framework for privacy in the European Union, and that the only way to achieve this is by adopting a Regulation, which is directly applicable in each EU Member State.

The Parliament agrees that the new data protection framework for the private and public sectors should be a Regulation, and no longer a Directive. Even if, technically, it is possible for the Council to revert back to a Directive, the chances that this will happen at this point are quite slim. Following the Snowden revelations, there is a stronger consensus among EU Member States to adopt a robust legal text for the protection of personal data in the European Union.

Territorial Scope

The territorial scope of the Regulation is based on two criteria: the "establishment" criterion and the "data subject" criterion. The Parliament maintains this distinction, but makes certain important changes in the wording.

Criterion Based on the 'Establishment'

Initially, the Commission proposed that the Regulation should apply to the processing of personal data that takes place in the context of the activities of an establishment of a controller or a processor in the European Union.

The Parliament has broadened the extraterritorial scope of the Regulation by considering that it must apply "whether the processing takes place in the Union or not" (Article 3-1). Thus, this provision would oblige EU organizations to comply with the Regulation even if they are processing personal data outside the European Union and, in particular, to grant the same privacy rights to data subjects who are not EU residents.

Criterion Based on the 'Data Subject'

The Commission also proposed that the Regulation should apply to the processing of personal data of data subjects in the Union by a controller or processor not established in the European Union, but where the processing concerns either 1) the offering of goods or services to those data subjects or 2) the monitoring of the

   ISSN 1473-3579

data subjects' behavior (Article 3-2). The logic behind this provision is that non-EU companies, when offering goods or services to EU consumers, should abide by the EU rules on personal data protection.[3]

Under the Commission's proposal, this criterion was initially meant to apply only to controllers. The Parliament has extended the scope of this provision to processors, which means that service providers that process data in the European Union on behalf of controllers established outside the Union must also comply with the Regulation.

The Parliament also removed the word "residing" from the text, which means that the second criterion applies to *all* data subjects, irrespective of whether or not they are EU residents. In practice, this could mean that the Regulation would also apply to individuals who are simply transiting via the European Union or spending their vacations there.

In amending the Commission's "one-stop shop" proposal, the Parliament has robbed the proposed rule of its very essence, which was to simplify and streamline the proceedings among DPAs in the European Union.

Under the Parliament's draft, the second criterion now applies to the offering of goods or services "irrespective of whether a payment is required". Gifts, free contests or promotional offerings without payment would all fall within the scope of the Regulation as long as the collection of personal data is involved.

Lastly, the application of the second criterion is no longer conditioned on the monitoring of an individual's "behavior". Initially, this provision was meant to cover the tracking of individuals on the Internet. Under the Parliament's draft, the term "behavior" was deleted, which automatically extends the scope of the second criterion to any type of profiling activity, regardless of the origin of the data (*e.g.*, profiling based on publicly available information).

'One-Stop Shop' Rule

The "one-stop shop" rule was initially proposed by the Commission as a way to simplify the rules of applicable law and to streamline the dealings with EU data protection authorities ("DPAs"). Where the controller or processor is established in more than one EU Member State, the Commission proposed to designate the supervisory authority of the main establishment as the one in charge of supervising all the processing activities of that organization within the European Union (Article 54a). This provision is one of the central pillars of the Commission's proposal, and has recently been the focal point of discussion among Member States.[4]

In an attempt to find a compromise solution, the Parliament has introduced a cooperation mechanism that would require the DPA of the main establishment that is acting as the "lead authority" responsible for supervising an organization's processing activities in the European Union, to take appropriate measures "only after consulting all other competent supervisory authorities" in an attempt to reach a consensus. The lead DPA would remain the sole authority empowered to decide on measures intended to produce legal effects (*e.g.*, enforcement actions), but it would have to "take the utmost account of the opinions of the authorities involved". The European Data Protection Supervisor ("EDPS") would have non-binding powers to step in, upon request by a DPA, in situations where it is unclear which authority should be acting as the lead authority.

The new wording proposed by the Parliament is intended to ensure a more balanced exercise of powers between the DPAs. In so doing, however, the Parliament has robbed the one-stop shop rule of its very essence, which was to simplify and streamline the proceedings among DPAs in the European Union.

The Parliament removed the 24 hour deadline for notification of data breaches from its revised draft, leaving controllers with an obligation to notify the regulator "without undue delay".

Instead, this rule is now based on a complex cooperation mechanism between DPAs, drafted in unclear terms, thus creating uncertainty on how this mechanism would work in practice. How would a "consensus" translate in legal terms? What would happen if the lead DPA did not abide by the opinions of its counterparts? What if the competent authorities disagreed on which supervisory authority should act as the lead authority, despite the EDPS's opinion on this matter?

Therefore, much effort still needs to be made to come up with an efficient mechanism that simplifies the proceedings among DPAs while guaranteeing that data subjects can exercise their rights without any burden.

International Data Transfers

Under the Commission's proposal, transfers of personal data outside the European Economic Area ("EEA") are prohibited, unless one of the following conditions applies: 1) the data are transferred to a third country or territory with adequate protection; or 2) the controller or processor adduces appropriate safeguards with respect to the processing of personal data (*e.g.*, binding corporate rules ("BCRs") or contractual clauses); or 3) a legal derogation applies (Article 40 and following). Each of these conditions is reviewed in more detail below.

Transfers with an Adequacy Decision

All adequacy decisions pronounced by the Commission shall remain in force for five years after the entry into force of the Regulation, unless they are amended, re-

placed or repealed by the Commission before the end of this period (Article 48-8). This means that prior decisions of the Commission approving the adequate level of protection of third countries (such as Argentina, Canada, Israel, New Zealand, or Switzerland) would be repealed and the Commission may have to re-assess the adequacy level of those countries.

It is unclear how this provision would impact the Safe Harbor framework, in particular, whether the Commission and the U.S. Federal Trade Commission ("FTC") would have to renegotiate the Safe Harbor framework from scratch, potentially leaving thousands of U.S. organizations without a legal basis for transferring EU data to the United States.

Transfers by Way of Appropriate Safeguards

The Commission initially proposed four possible legally binding instruments that provide adequate safeguards to the data being transferred, namely: 1) BCRs; 2) standard data protection clauses adopted by the Commission; 3) standard data protection clauses adopted by a DPA; and 4) contractual clauses between the controller or processor and the recipient of data that have been approved by a DPA.

On the one hand, the Parliament has made some interesting proposals that can be viewed as an improvement. For example, organizations would be able to rely on a "European data protection seal" granted by a DPA, certifying that the processing of personal data is performed in compliance with the Regulation (although it remains unclear in this case how the DPA would consider that the organization adduces appropriate safeguards for data transfers). Most data transfers (*i.e.*, those that are based on BCRs, a valid European data protection seal or standard contractual clauses adopted by a DPA) would no longer require any specific authorization (Article 42-3). The DPA's prior approval would be needed only for transfers that are based on contractual clauses between the controller/processor and the recipient of data. Transfers that have already been approved by a DPA would remain valid for two years after the entry into force of the Regulation (Article 42-5), but it is not clear whether companies would still be compelled to obtain the DPA's approval for those transfers.

On the other hand, some of the amendments adopted by the Parliament are confusing. For example, the model clauses that were adopted by the Commission would remain in force for five years after the entry into force of the Regulation (Article 41-8). After this period, it is unclear whether they would continue to constitute a valid appropriate safeguard. Indeed, the Parliament's draft has removed model clauses from the list of appropriate safeguards under Article 42, but continues to refer to them as a valid safeguard for data transfers under Recitals 83 and 84. Furthermore, processors are now excluded from the scope of BCRs (Article 43), which both diminishes the efforts of the EU Article 29 Data Protection Working Party to create a specific Binding Safe Processor Rules ("BSPR") framework (*see analysis at WDPR, July 2013, page 7*), and also casts doubt on the validity of the BSPRs that have already been approved so far.

Legal Derogations

The list of legal derogations authorizing the transfer of personal data is similar to the current provision under the Data Protection Directive. However, the condition based on the legitimate interests of the controller or processor that was proposed by the Commission has been deleted under the Parliament's draft (Article 44).

Transfers or Disclosures Not Authorized by EU Law

In response to the PRISM scandal,[5] the Parliament has introduced a new provision requiring controllers and processors to notify and obtain prior authorization of a DPA to transfer or disclose personal data to a judicial or administrative authority in a third country which has requested access to the data (Article 43a). This amendment also requires the DPA to assess the validity of the request under the provisions of the Regulation, and controllers or processors must inform the data subjects in the European Union about the possible disclosure of their data to a foreign judicial or administrative authority and the decision of the DPA authorizing such disclosure.

This new provision resembles the blocking statutes that already exist in some European countries (*e.g.*, France and Switzerland), which prohibit the disclosure of business-related documents or information to foreign judicial and administrative authorities without a formal request handed over to the local authorities. If this rule is generalized across the European Union, this would mean that EU companies could potentially find themselves in violation of foreign laws, for example, when they are requested to transfer EU data to their U.S.-based headquarters company for the purpose of complying with U.S. pre-trial discovery rules. Recital 90 of the Regulation states in unambiguous terms that, when the controller or processor is confronted with conflicting compliance requirements between the jurisdictions of the European Union and those of a third country, "the Commission should ensure that EU law takes precedence at all times". This does not tell companies what would happen if a DPA refused the disclosure of data to a foreign authority.

Consent

Under the Commission's proposal, consent is defined as "any freely given specific, informed and explicit indication of his or her [the data subject's] wishes by the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed" (Article 4-8). If the data subject's consent is given in the context of a written declaration which also concerns another matter, the requirement to give consent must be clearly distinguished from this other matter (Article 7). The controller also has the burden of proving that consent was properly obtained from the data subject, which means that, in practice, written consent will almost always need to be obtained.

The Parliament's draft further clarifies the meaning of consent and the conditions of its validity. In particular, consent must be "purpose-limited", meaning that consent is valid for only as long as the purpose of the pro-

   ISSN 1473-3579

cessing continues to exist or that the data are necessary for carrying out that purpose (Article 7-4). In particular, the execution of a contract or the provision of a service should not be made conditional on the data subject's consent to the processing of data that is not necessary for the execution of that contract or provision of a service. Finally, consent is valid only if the data subject is able to refuse or withdraw consent without detriment. For example, the use of default options which the data subject is required to modify to object to the processing (*e.g.*, pre-ticked boxes) is explicitly mentioned as *not* expressing free consent (Recital 33). Withdrawing consent should be easy and the data subject must be informed if withdrawal of consent may result in the termination of a service provided or of the relationship with the controller (Article 7-3).

Profiling

Under the Commission's proposal, data profiling is defined as "a measure which produces legal effects concerning a natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyze or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior" (Article 20). Profiling is permitted only if it is 1) necessary for the entrance into, or performance of, a contract; 2) authorized by a Member State law; or 3) based on the individual's consent. Profiling cannot be based solely on the use of sensitive data (*i.e.*, race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity).

The Parliament's draft clarifies the right of any individual to "object" to profiling and the right to be informed about this right in a highly visible manner (Article 20). The Parliament explicitly prohibits any profiling activities that are based on sensitive data and that either have the effect of discriminating against individuals or result in measures that have a discriminatory effect towards individuals. Data controllers must take action effectively against such discrimination by implementing protection measures that are designed to prevent possible discrimination resulting from profiling (Article 20-3).

Furthermore, profiling that produces legal effects for a data subject, or significantly affects the interests, rights or freedoms of the data subject concerned, cannot be based solely or predominantly on automated processing, and must include a human intervention, including an explanation of the decision reached after such an assessment is made (Article 20-5).

Profiling that is based solely on the processing of pseudonymous data would benefit from less prescriptive provisions; in particular, a presumption would apply that such profiling does not significantly affect the interests, rights and freedoms of individuals (Recital 58a). Pseudonymous data is defined as "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution" (Article 4-2a).

Right to Be Forgotten

Under the Commission's proposal, the right to be forgotten and to erasure is defined as the right for any individual "to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data" if 1) the data are no longer necessary for the purposes of the processing; or 2) the data subject withdraws consent; or 3) the data subject objects to the processing; or 4) the processing does not comply with the Regulation (Article 17). If the data was made public, the controller has an obligation to take reasonable steps to inform third parties that they must erase any links to, or copy or replication of, that personal data.

Under the Parliament's draft, the "right to be forgotten" has been renamed the "right to erasure", probably in response to the outcry from technology companies that consider the right to be forgotten to be technically impossible to implement.

Furthermore, the Parliament makes a subtle distinction between public and non-public data.

As a general rule, controllers must erase any personal data upon request by a data subject and obtain from third parties the erasure of any links to, or copy or replication of, that data when one of the above-mentioned conditions applies (Article 17-1). The Parliament has broadened the scope of this provision to situations where a court or regulatory authority in the European Union has ruled as final and absolute that the data concerned must be erased. This means that, in theory, a DPA could force an organization to erase the data it withholds about a data subject. Where the data was made public without justification (meaning without a legal basis), the controller must then take all reasonable steps to have the data erased, including by third parties (Article 17-2).

Privacy Impact Assessment

Under the Commission's proposal, controllers or processors are required to carry out a privacy impact assessment ("PIA") where the processing operations present specific risks, such as profiling, processing of sensitive data, video surveillance, or processing of data on minors, genetic and biometric data (Article 33).

Under the Parliament's draft, PIAs are redefined as part of a "lifecycle data protection management". The scope of processing activities considered to present a risk has been substantially broadened, and now includes, for example, the processing of personal data relating to more than 5,000 data subjects, the processing of location data, the processing of data on employees in large scale filing systems and processing where a data breach would likely adversely affect the protection of personal data or the privacy rights of individuals (Article 32a).

Therefore, PIAs appear to have become the norm, not the exception.

The maximum level of fines is significantly higher under the Parliament's draft than under the Commission's proposal, which is clearly aimed at giving DPAs more clout to enforce the Regulation.

Data Protection Officer

The Commission proposed to render the appointment of a data protection officer ("DPO") compulsory where: 1) the processing is carried out by a public authority body; or 2) the processing is carried out by an enterprise employing more than 250 persons; or 3) the core activities of the controller or processor concern the regular or systematic monitoring of the data subjects (Article 35).

Under the Parliament's version, the criterion based on the number of employees has been replaced by a new criterion where the processing "relates to more than 5,000 data subjects in any consecutive 12-month period" (Article 35-b). This provision does not apply where the data has been archived (Recital 75).

It is also worth noting that this provision now applies to any "legal person", whereas the Commission referred to "enterprises" employing at least 250 persons. In other words, all types of legal entities (*e.g.*, associations, non-governmental organizations or other types of organizations), not only companies, would be subject to this provision.

Organizations must also appoint a DPO where the core activities of the controller or the processor consist of processing sensitive data, location data or data on children or employees in a large scale filing system (Article 35-d). This catch-all phrase broadens the scope of the requirement significantly. In practice, any organization that processes location data (*e.g.*, telecommunications service providers, mobile app providers or companies using location tracking devices in their vehicles), data on minors (defined as any person below the age of 18) or data on employees in a large scale filing system would be obliged to appoint a DPO, regardless of the size of the organization or the number of data subjects involved in the processing.

Data Breach Notification

Under the Commission's proposal, controllers are required to notify the DPA in case of a breach "without undue delay and, where feasible, not later than 24 hours after having become aware of it" (Article 31-1).

The Parliament removed the 24 hour deadline from its revised draft, leaving controllers with an obligation to notify the regulator "without undue delay". On this issue, the Parliament was sympathetic to the arguments of the business sector, according to which a 24 hour deadline is unrealistic and unreasonable in practice.

The requirement is also less stringent for data processors, which must alert and inform the controller "without undue delay" after the establishment of a personal data breach, as opposed to doing so "immediately" (Article 31-2).

While this new wording will certainly be welcomed by the business sector, the current draft Regulation is now in conflict with the data breach notification requirements applicable to telecom companies and Internet service providers which, under the e-Privacy Directive and its technical implementing measures for data breaches, must notify data breaches within 24 hours.[6]

Enforcement and Sanctions

The Commission made a bold move under its proposal to harmonize the enforcement powers of the DPAs and to give a stronger deterrent effect to the administrative fines that they can impose in case of a violation of the Regulation. Under the Commission's proposal, administrative fines range between 250,000 euros (U.S.$334,902) or 0.5 percent of the annual worldwide turnover and 1 million euros (U.S.$1.3 million) or 2 percent of annual worldwide turnover, depending on the type and gravity of the violation that are listed in the text (Article 79).

Under the Parliament's draft, the categories of violations are no longer described. Instead, the Regulation now states that the DPA shall impose one of three possible sanctions on "anyone who does not comply with the obligations laid down in this Regulation" (Article 79-2):

- a warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits; or
- a fine of up to 100 million euros (U.S.$134 million) or up to 5 percent of the annual worldwide turnover in case of an enterprise, whichever is greater.

The maximum level of fines is significantly higher than under the Commission's proposal, which is clearly aimed at giving DPAs more clout to enforce the Regulation. But under the Parliament's draft, fines are not the only type of sanction that DPAs can impose. Depending on the facts, organizations may get away with a simple warning or a regular audit, although it is unclear regarding the latter who would conduct the audit (*e.g.*, the DPA or possibly an independent certified organization) and how long this audit would last. It is worth noting that organizations that possessed a valid European data protection seal would be fined only in case of intentional or negligent non-compliance (Article 79-2b).

DPAs would also be required to assess each situation based on various factors (*e.g.*, gravity of the violation, intentional or negligent character of the infringement, degree of responsibility, repetitive nature of the infringement, degree of cooperation with the DPA, types of personal data affected, level of damage, *etc.*).

The Parliament has also introduced a new provision requiring supervisory authorities to cooperate with one another with a view to guaranteeing a harmonized level

   ISSN 1473-3579

of sanctions within the European Union. This provision is consistent with the cooperation and consistency mechanism introduced under Chapter 7.

Next Steps in the Legislative Process

The vote by the LIBE Committee is an important step forward in the legislative process, but it does not constitute the final phase of the adoption procedure. After the end of the vote by the LIBE Committee, the Parliament decided to postpone the vote in the plenary session until April 2014 so as not to delay further the legislative procedure. This sends a strong signal that "the ball is now in the court of Member State governments to agree a position and start negotiations."[7]

The vote of the LIBE Committee also gives the Parliament a mandate to start negotiating the text officially with the Council (composed of the Justice Ministers of each Member State).

The LIBE Committee vote has created a new momentum, and the adoption of the Regulation in 2014 seems possible.

Inter-institutional discussions between the Parliament, the Council and the Commission (*i.e.*, trilogue) are expected to begin as soon as the Council agrees on its own negotiating position for the text. It is unclear when this will happen, given the conflicting positions between Member States on some of the proposals, as illustrated by the Council's meeting of October 7, 2013, where the Justice Ministers discussed the "one-stop shop" mechanism (*see WDPR, October 2013, page 18*). The next meeting of the Justice Ministers on the data protection reform package is scheduled to take place on December 5-6, 2013, at which point it should become clearer which amendments will be maintained and within what time frame the text is likely to be adopted.

The LIBE Committee vote has created a new momentum, and the adoption of the Regulation in 2014 seems possible, despite recent comments made by certain Heads of State suggesting that the adoption of the text could be postponed until 2015.[8]

The EU Member States seem to be generally in favor of a stronger data protection framework, especially after the Snowden revelations, and the Commission will certainly continue to push hard for the adoption of this text before spring 2014. If the Regulation is not adopted by then, the European Parliament elections will create an important reshuffling of the cards, with new political leaders entering the scene, and the risk that the draft Regulation might be abandoned, put aside, or redrafted from scratch.

What seems more likely, however, is that the main provisions on which the Parliament and the Council agree will be adopted in the next plenary session, and the more controversial provisions will be left for after the elections.

Conclusion

The Parliament has made a remarkable effort to review the Commission's proposal in a timely manner. The Parliament has also made an effort to maintain a balance between the fundamental rights of individuals and the accountability obligations of organizations. While many of the amendments may be viewed as an improvement, the draft Regulation nevertheless remains a long and structurally complex piece of legislation, which still needs to be improved, simplified and clarified in certain parts.

Once adopted, the Regulation will come into force after a two-year grace period, leaving time for organizations to make the necessary changes for compliance. The current political attention to privacy issues in the European Union sends a clear signal to organizations that they should not wait until the text comes into force to begin complying with its provisions.

NOTES

[1] The Commission's proposal is available at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[2] See Council of the European Union, Summary of the 7th hearing of the LIBE inquiry on electronic mass surveillance of EU citizens, held in Brussels on October 14, 2013, available at http://register.consilium.europa.eu/servlet/driver?page=Result&ssf=DATE_DOCUMENT+DESC&srm=25&md=400&typ=Simple&cmsid=638&ff_SOUS_COTE_MATIERE=&lang=EN&fc=REGAISEN&ff_COTE_DOCUMENT=15106/13&ff_TITRE=&ff_FT_TEXT=&dd_DATE_REUNION=&single_comparator=&single_date=&from_date=&to_date=.

[3] See European Commission's memo entitled "LIBE Committee vote backs new EU data protection rules", published on October 22, 2013, available at http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

[4] See Note from the Presidency to the Council of the European Union on the "one-stop shop" mechanism, published on October 3, 2013, available at http://register.consilium.europa.eu/servlet/driver?page=Result&ssf=DATE_DOCUMENT+DESC&srm=25&md=400&typ=Simple&cmsid=638&ff_SOUS_COTE_MATIERE=&lang=EN&fc=REGAISEN&ff_COTE_DOCUMENT=14260/13&ff_TITRE=&ff_FT_TEXT=&dd_DATE_REUNION=&single_comparator=&single_date=&from_date=&to_date=.

[5] See EU Parliament's press release: "Civil liberties MEPs pave the way for stronger data protection in the EU", published on October 21, 2013, available at: http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706/html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU.

[6] See Olivier Proust, "European Commission Adopts Technical Implementing Measures for Data Breaches", available at http://privacylawblog.ffw.com/category/data-security.

[7] See EU Parliament's press release: "Civil liberties MEPs pave the way for stronger data protection in the EU", published on October 21, 2013, available at: http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706/html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU.

[8] See "Data protection talks delayed at EU summit talk", Euractiv, October 25, 2013, available at http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pac-news-531306#!.

The compromise amendments adopted by the LIBE Committee are available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf and http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

Olivier Proust is Of Counsel at Field Fisher Waterhouse LLP, Brussels. He may be contacted at olivier.proust@ffw.com.

  WDPR ISSN 1473-3579