Bloomberg BNA

Privacy and Security Law Report®

The Proposed EU Data Protection Regulation Two Years Later



By Christopher Kuner, Cédric Burton and Anna Pateraki

I. Introduction

Two years after the European Commission proposed its reform to the European Union legal framework for data protection, it is time to take stock of where things stand. The package consisted of two parts, a proposal for a General Data Protection Regulation (Regulation) covering the private sector and public administrations,[1] and a proposed directive for the processing of personal data in the law enforcement context;[2] this article will only deal with the Regulation.

Since the European Commission proposal was first published in January 2012,[3] the Regulation has been the subject of intense discussion and lobbying on both sides of the Atlantic. It had been hoped that the legislative process would be completed by now, but there is still a lack of agreement between the three EU institutions that are involved in it (the European Commission, European Parliament and Council of the EU), and the outcome of the process remains unclear. A complicating factor is that elections to the European Parliament are planned for May 2014, and the five-year term of the European Commission will also expire Oct. 31, 2014, making it necessary for a new commission to be selected by November 2014.[4] Thus, European politics has, and will continue to have, a significant effect on the work on the reform proposal being finalized in the com-

[1] 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), COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (11 PVLR 178, 1/30/12).

Christopher Kuner is senior of counsel at Wilson Sonsini Goodrich & Rosati in Brussels. He may be reached at ckuner@wsgr.com.

Cédric Burton is a senior associate at Wilson Sonsini Goodrich & Rosati in Brussels. He may be reached at cburton@wsgr.com.

Anna Pateraki is an associate in the firm's Brussels office and may be reached at apateraki@wsgr.com.

The authors are grateful to Bastiaan Suurmond, legal intern in the firm's Brussels office, for his excellent research assistance.

[2] Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM (2012) 10 final (Jan. 25, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF (11 PVLR 200, 1/30/12).

[3] For an analysis of the initial commission proposal, *see* Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, 11 Bloomberg BNA Privacy & Sec. L. Rep. 215 (Feb. 6, 2012) (11 PVLR 215, 2/6/12).

[4] For an analysis of the impact of the upcoming parliamentary elections and the appointment of a new commission, *see* Cédric Burton & Anna Pateraki, *Status of the Proposed EU Data Protection Regulation: Where Do We Stand?*, 12 Bloomberg BNA Privacy & Sec. L. Rep. 1470, 1473–74 (Sept. 2, 2013) (12 PVLR 1470, 9/2/13).

 ISSN 1538-3423

ing months. Adding to the complexity of the political process are the revelations about access to data by intelligence agencies that have been the subject of intense interest in the past months.

In this article we analyze the current status of the proposed Regulation, focusing in particular on the compromise amendments adopted by the European Parliament in October 2013, and on the progress made in the Council of the EU. In addition, we provide some background about the upcoming parliamentary elections and the appointment of a new commission, and outline possible next steps for the proposal. While the European Parliament has voted on amendments to the Regulation and has adopted a compromise text, the Council of the EU has not yet adopted any definitive text, and we will thus not cite to any text of the council.

II. The European Parliament: The LIBE Committee's Compromise Amendments

In the last two years, the European Parliament has discussed the Regulation at length, and a number of parliamentary committees have proposed amendments.[5] For the purpose of this article, we will focus only on the latest consolidated amendments adopted Oct. 21, 2013, by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), the lead committee with regard to the data protection reform.[6]

After Jan Philipp Albrecht, German Green member of the European Parliament (MEP) and the lead rapporteur of the LIBE Committee, issued his draft report on the proposed Regulation (Albrecht Report) in January of 2013,[7] all MEPs were invited to submit amendments. As a result, almost 4,000 amendments were tabled, forcing the LIBE Committee to postpone its vote twice. In October 2013, the LIBE Committee held its long-awaited vote and proposed compromise amendments to the commission proposal. While many of the compromise amendments are similar to those presented in the Albrecht Report, the text also makes some changes.

Some of the major provisions of the compromise amendments approved by the LIBE Committee include the following:

- *Concept of personal data: Cookies and Internet protocol addresses*. The compromise text explicitly states that cookies and IP addresses constitute personal data, unless they do not relate to an identified or identifiable individual (Recital 24), and the reference in the Albrecht Report that IP addresses used by companies would not qualify as personal data has now been deleted.

- *Extraterritorial effect*. Contrary to the commission proposal and the Albrecht Report that applied the Regulation only to non-EU data controllers, the Regulation would now apply to both controllers and processors not established in the EU when: (i) offering services to individuals in the EU, even without payment; or (ii) monitoring such individuals (''monitoring'' seems to involve tracking and the creation of profiles) (Article 3 and Recital 21). The Regulation would thus apply to a variety of online service providers located outside of the EU.

- *Pseudonymous and encrypted data*. The compromise text introduces new concepts with regard to the definition of personal data that were not included in the commission proposal: (1) ''pseudonymous data,'' defined as personal data that ''cannot be attributed to a specific individual without the use of additional information,'' as long as such information is kept separately and secure; and (2) ''encrypted data,'' identified as personal data that are ''rendered unintelligible'' to unauthorized access due to security measures (Article 4 (2a) and (2b)). The compromise amendments clarify that such types of data are considered personal data under the Regulation, but they are subject to less stringent requirements. The concept of pseudonymous data was already contemplated in the Albrecht Report, but the concept of encrypted data is new.

- *Main establishment*. The LIBE Committee suggests harmonizing the concept of ''main establishment'' for both controllers and processors, contrary to the commission proposal that defined different criteria for controllers and processors. Although the definition of main establishment was not changed in the Albrecht Report, the decisive criterion in the compromise text is now the location where the main decisions are taken with regard to the conditions and means of the processing (Article 4(13)). In addition, the compromise text provides three criteria to take into account in deciding where such main decisions are taken: an organization's headquarters; the location which is best placed in terms of management functions and administrative responsibilities to enforce the data protection rules; and the location of effective and real management activities (which are similar to the criteria currently used for designating the lead authority in the context of binding corporate rules (BCRs)).

- *Legal basis for data processing*. Similar to the Albrecht Report, the compromise text imposes additional restrictions in order for consent to be valid. In particular, it requires companies to obtain ''free'' consent (pre-ticked boxes do not suffice), limit consent to specific purposes and not make consent conditional for processing that is not nec-

[5] For an analysis of the progress made by the European Parliament on the Regulation by September 2013, *see id.* at 1471.

[6] LIBE Committee, Compromise Amendments on Articles 1–29 (Oct. 7, 2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf; LIBE Committee, Compromise Amendments on Articles 30–91 (Oct. 17, 2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

[7] LIBE Committee, Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (Jan. 16, 2013), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fEN (12 PVLR 65, 1/14/13). For an analysis of the Albrecht Report, *see* Cédric Burton et al., *The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report*, 12 Bloomberg BNA Privacy & Sec. L. Rep. 99 (Jan. 21, 2013) (12 PVLR 99, 1/21/13).

  PVLR ISSN 1538-3423

essary for the requested services (Article 7 and Recitals 32 and 33). In addition, the compromise text clarifies that: consent requires an affirmative action (e.g., ticking a box); mere use of a service should not constitute consent (Recital 25); and consent cannot be given for the processing of personal data of third persons (Recital 32). Furthermore, the use of a company's legitimate interest as a legal basis is retained, but is further restricted. The Albrecht Report had limited the use of legitimate interest ''in exceptional cases,'' but the compromise text allows companies to rely on their legitimate interest to process data when it meets individuals' ''reasonable expectations'' (Article 6); it is unclear what this would mean in practice, but it could be used to restrict the processing of personal data. In addition, companies would be allowed to rely on their legitimate interest to process pseudonymous data (Recital 38), which was not contemplated in the Albrecht Report.

- *Privacy policies*. The compromise amendments require companies to complement privacy policies with icons that would describe in a graphical way a number of elements, such as how personal data are collected, retained and shared with third parties and how encryption is used (Article 13a). In addition, the compromise text clarifies that privacy policies should be as clear and transparent as possible, and should not contain hidden or disadvantageous clauses (Recital 32).

- *Right to be forgotten*. The right to be forgotten, which was included in the commission proposal and was highly controversial, has now been renamed and merged with the right to erasure in the compromise amendments (Article 17). Some concerns have been taken into account, but others remain, such as obliging companies that have made data public without legal justification to erase the data, including data held by third parties (Recital 54). In addition, individuals can request third parties to erase any links to or copies of data or otherwise request restriction of the processing based on a court order or if the particular type of storage technology no longer allows for erasure (Article 17).

- *Profiling*. Similar to the Albrecht Report, the compromise text restricts profiling activities when they lead to measures producing legal effects or when they significantly affect the interests, rights and freedoms of individuals. In these situations, profiling is allowed only if it is based on individuals' consent, if provided by EU member state law or if conducted in the context of the performance of a contract (and if adequate safeguards are implemented). Profiling that is based solely on sensitive data is prohibited (Article 20). Contrary to the Albrecht Report, the compromise text provides some flexibility in cases where profiling is based on pseudonymous data, provided that it is impossible for the data controller to attribute the data to a specific individual based on a single source of pseudonymous data or on aggregated pseudonymous data (Recital 58a). This could in theory introduce some flexibility for companies conducting online data analytics.

- *Joint controllers*. The Albrecht Report had required joint controllers to allocate roles and responsibilities among themselves by means of a ''written arrangement'' and to describe such allocation in their privacy policies. These requirements have been now replaced by the obligations that such arrangements duly reflect the roles and relationships vis-à-vis individuals, and that the ''essence'' of such arrangements be made available for individuals. Where the allocation of liability between joint controllers is unclear, the Albrecht Report had limited their joint liability to cases related to individuals exercising their rights, but the compromise text is more vague and seems to assume joint liability in all cases (Article 24).

- *Compliance and data protection officers (DPOs)*. The compromise text mandates a biannual review and update of compliance policies and procedures (Article 22), which was not contemplated in the commission proposal or the Albrecht Report. In addition, the compromise text requires companies to designate a DPO when the processing affects more than 5,000 individuals in a consecutive 12-month period (Article 35). This contrasts with the Albrecht Report, which had imposed the obligation to appoint a DPO when the processing relates to more than 500 individuals per year, and the commission proposal, which had imposed the same obligation when the processing is carried out by a company employing 250 persons or more.

- *Breach notification*. The 24– or 72-hour deadline to notify data breaches to data protection authorities (DPAs) contained respectively in the initial commission proposal and in the Albrecht Report has been withdrawn, and the draft now requires companies to notify ''without undue delay'' (Article 31).

- *European Data Protection Seal*. The text introduces the ''European Data Protection Seal,'' a standardized data protection mark to be issued by DPAs to certify a controller's or processor's compliance with the Regulation (Recital 77 and Article 39). The seal would limit administrative liability to cases of intentional or negligent noncompliance (Article 79). Further, like BCRs or standard contractual clauses, the seal would exempt data controllers from having to obtain authorization before transferring data to third countries (Article 42).

- *International data transfers*. The compromise amendments provide that commission adequacy decisions (such as the one on the U.S.-EU Safe Harbor Program) would remain in force for five years after the Regulation went into effect, unless they were amended, replaced or repealed by the commission (Article 41(8)), contrary to the Albrecht Report that provided for a two-year period regarding the same issue. As provided in the Albrecht Report, the compromise text also contains a sunset clause for data transfer authorizations based on Article 26(2) of the current Directive 95/46/EC, meaning, for example, that authorizations for BCRs or standard contractual clauses would have to be reissued by DPAs within two years of the entry into force of the Regulation (Article 42(5)). Another notable change is the removal of

the reference to BCRs for processors (Article 43(1)(a)), which was included in both the commission proposal and the Albrecht Report. While this would not prohibit DPAs from approving BCRs for processors, DPAs might no longer be obligated to accept them. Finally, the compromise text has removed the reference to standard contractual clauses approved by the European Commission from the list of the appropriate safeguards for data transfers, suggesting that only standard contractual clauses adopted through the consistency mechanism would be recognized (Art. 42(2)).

- *Law enforcement requests.* Both the Albrecht Report and the compromise amendments inserted a provision that would require controllers and processors to notify DPAs about requests to disclose personal data to courts or regulatory authorities in countries outside of the EU, and to obtain formal approval from DPAs before turning over European data for law enforcement purposes (Article 43a). Driven by the law enforcement revelations made recently in the press, the compromise text also provides that ''any legislation which provides for extra-territorial access to personal data processed in the Union without authorization under Union or Member State law should be considered as an indication of a lack of adequacy'' (Recital 82). While the issue of conflicting obligations needs to be addressed, in its current form the amendment seems too complex for its own good and raises a number of problems, such as that data controllers faced with conflicting legal obligations would face sanctions in multiple jurisdictions, and that the DPAs' power to review judicial decisions, as contained in the LIBE Committee proposals, might raise constitutional questions. For example, it is not clear how the requirement for DPA approval would interact with obligations to transfer personal data under treaties (such as mutual legal assistance agreements) or other international instruments. Because the suggested amendments are controversial, they are likely to be debated during the upcoming negotiations between the three EU institutions.
- *One-stop shop mechanism*. In addition, the compromise text amends the one-stop shop mechanism. The rationale for the one-stop shop approach is to have one DPA, such as the DPA of the company's main establishment, competent for all of its data processing activities in the EU. Contrary to the Albrecht Report that considered the lead DPA to be a mere contact and coordination point, and to the initial commission proposal that provided for a comprehensive one-stop shop approach, the compromise text now takes an intermediary position and creates a system where the lead DPA would be the sole authority empowered to take legal decisions with regard to a company, but would have complex cooperation obligations with other relevant DPAs (Article 54a). Furthermore, individuals could lodge a complaint before the DPA of their home jurisdiction, and the lead DPA would be required to coordinate its work with that DPA.
- *Consistency mechanism.* The compromise text builds on the approach taken in the Albrecht Report, where the European Data Protection Board (i.e., a body consisting of the heads of the DPAs of all member states and the European Data Protection Supervisor (EDPB)) would act as an appeal mechanism in case of disagreement between DPAs, and could take decisions that would be legally binding upon DPAs. However, the compromise text goes further and creates a system where ''matters of general application'' (e.g., adoption of standard contractual clauses, approval of BCRs) and ''individual cases'' (i.e., measures adopted by the lead DPA where the one-stop shop is triggered) are treated differently. While matters of general application would trigger an opinion of the EDPB taken by a simple majority, all measures that would be adopted by the lead DPA would be subject to a complex two-step process, including veto rights of other DPAs. In particular, if other DPAs have serious objections to a draft measure submitted by the lead DPA, the measure cannot be adopted, but should be submitted to the EDPB, the opinion of which is supposed to be given the ''utmost account'' by the lead DPA. If the lead DPA does not follow the opinion of the EDPB, the EDPB can adopt a measure by a two-thirds majority that will be binding upon the DPAs involved (Article 57–58a). The roles of the lead DPA and the EDPB in the consistency mechanism have proved to be points of continuing political disagreement (see below).
- *Sanctions and fines.* The fines have been significantly increased compared to the initial commission proposal and the Albrecht Report (i.e., fines of up to 1 million euros ($1.4 million) or up to 2 percent of a company's annual worldwide turnover), and can now amount to 100 million euros ($138 million) or up to 5 percent of a company's annual worldwide turnover, whichever is greater (Article 79).
- *Employment context.* Contrary to the limited amendments contained in the Albrecht Report that gave leeway to member states to regulate the employment sector, the compromise text now adds specific restrictions that must be respected in all member states. This includes limitations on profiling performed on employees, the exclusion of consent as a legal basis for the processing if it is not freely given and a number of minimum standards such as: prohibiting any data processing without employees' knowledge; respecting a number of requirements before collecting employee data based on suspicion of ''crime or serious dereliction of duty'' (including having concrete suspicion, respecting proportionality and defining data deletion periods); prohibiting the use of covert closed-circuit TV (CCTV) measures at all times, and limiting the use of open CCTV measures so that they are not used in areas such as bathrooms, changing rooms, etc.; setting out rules for the processing of medical examinations and aptitude tests by the employer, including prohibiting the use of employee data for the purpose of genetic testing and analyses; regulating the monitoring of information technology systems (such as telephone, e-mail and Internet) at the workplace; where the private use of IT systems is allowed, limiting the monitoring of IT traffic data solely for security, operational and

  PVLR ISSN 1538-3423

billing purposes (unless there is a concrete suspicion of illegal activity in the employment context); and prohibiting the use of employees' sensitive data for blacklisting employees. In addition, the compromise amendments aim to facilitate the transmission of employee data within a group of undertakings and to service providers providing legal and tax advice; however, they clarify that the Regulation's data transfer restrictions will continue to apply for the transfer of employee data to third countries (Article 82).

III. The Council of the European Union

The EU legislative procedure requires agreement on the final text between the European Parliament and the Council of the EU (i.e., the 28 EU member states). The work of the council is led by the presidency, which rotates among member states every six months; as of Jan. 1, 2014, the presidency is held by Greece, Italy will take over as of July 1, 2014, and Latvia as of Jan. 1, 2015.

In addition to the vote on the compromise text in October 2013, the LIBE Committee voted to give the Parliament a mandate to negotiate the text with the Council of the EU. However, the council has not yet adopted a common position on the full version or parts of the text, and there is currently uncertainty as to the direction that the negotiations between council, Parliament and commission may take. Although the European institutions are aiming to adopt a final text before the parliamentary elections in May 2014, the timing and the final content of the Regulation remain hard to predict.

In the first half of 2013, the council has made progress on Chapters I, II, III and IV of the proposal (i.e., general provisions, principles, rights of the data subject and controller and processor), and a consolidated version of those chapters was published in May 2013;[8] however, the discussions on those chapters have not yet been finalized.[9] In the second half of 2013, progress has been made on issues included in Chapters V, VI, VII, VIII and IX of the proposal (i.e., data transfers, duties and competences of supervisory authorities, cooperation and consistency, remedies/sanctions and processing for historical, statistical and scientific research purposes) by holding a variety of formal and informal meetings within the council's Working Party on Information Exchange and Data Protection (DAPIX) and at a higher political level. However, the delegations of EU Member States in the council did not manage to adopt a common position on the text, and there are currently no definitive amendments to these chapters.

Some of the main points of continuing political disagreement within the council include:

- *One-stop shop mechanism*. The commission proposal aims to reduce administrative burdens of pan-European data controllers by allowing them to deal with a single DPA. The council's DAPIX group has discussed the one-stop shop mechanism during at least eight meetings in 2013. As the Lithuanian presidency noted to the council in October: ''the vast majority of delegations have voiced various and detailed criticisms on this principle.''[10] The main concern about the one-stop shop mechanism, as proposed by the European Commission, appears to relate to the lack of proximity of citizens to an effective remedy.[11] The delegations of member states have proposed improvements to the mechanism, however without yet reaching a political agreement. Such proposed improvements include: imposing limitations on the competences of the lead DPA; implementing a clear process for the cooperation between the local DPAs and the lead DPA; and improving the proximity of individuals to effective judicial review.

At the Justice and Home Affairs Council meeting of Dec. 6, 2013, Hubert Legal, the head of the council's Legal Service, stated that in its current form the one-stop shop was a ''very bad outcome'' for data subjects, as it would create a one-stop shop for companies but would require complicated interaction between the DPAs that would interfere with individuals exercising their rights, and would thus be incompatible with the case law of the European Court of Human Rights.[12] He added that instead a new EU authority should be set up for one-stop shop purposes, but this proposal was received with criticism. Indeed, the commission and the council have all but ruled out the creation of a new pan-European data protection agency. During the press conference following the meeting, Vice-President of the European Commission Viviane Reding concluded that ''[t]oday . . . we have moved backwards.''[13]

- *Consistency mechanism*. The consistency mechanism is a concept that would require DPAs to cooperate with regard to certain matters and escalate issues to the EDPB. The role of the lead DPA (where the one-stop shop mechanism is triggered) in the consistency mechanism has been proved difficult to regulate, as some member states oppose the concentration of enforcement powers on the part of the lead DPA. In addition, the role and legal status of the EDPB in the consistency mechanism is controversial. Although under the commission proposal the EDPB does not have legal personality and its opinions are not legally binding

[8] EU Council, Addendum to Note, Key Issues of Chapters I-IV (May 31, 2013), *available at* http://register.consilium.europa.eu/pdf/en/13/st10/st10227-ad01.en13.pdf (12 PVLR 1019, 6/10/13).

[9] For a comparison of Chapters I-IV of the Regulation, as proposed by the European Commission (initial proposal), the European Parliament (Albrecht Report) and the council (as of May 2013), *see* Wilson, Sonsini, Goodrich & Rosati LLP, *Comparison of Chapters I–IV of the General Data Protection Regulation as Proposed by the European Commission, the European Parliament and the Council of the EU* (July 2013), *available at* http://www.wsgr.com/eudataregulation/pdf/chapters-i-iv-comparison.pdf.

[10] EU Council, Presidency Note to the Council, One-Stop Shop Mechanism (Oct. 3, 2013), *available at* http://register.consilium.europa.eu/pdf/en/13/st14/st14260.en13.pdf.

[11] *See* Background, Justice and Home Affairs Council, Dec. 5–6, 2013 Meeting in Brussels (Dec. 3, 2013), *available at* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/139884.pdf.

[12] EU Council, *3279th Council Meeting (Justice)—Legislative Deliberations* (Dec. 6, 2013), http://video.consilium.europa.eu/webcast.aspx?ticket=775-979-13755 (12 PVLR 2048, 12/9/13).

[13] Viviane Reding, European Comm'n Vice-President, Press Conference at the Justice and Home Affairs Council (Dec. 6, 2013), *available at* http://europa.eu/rapid/press-release_SPEECH-13-1029_en.htm.

(similar to the Article 29 Working Party today), some member states seek to make the EDPB an appeal mechanism for DPAs' decisions, while others have shown reluctance to give more power to it.

Although the council has made progress on many fronts, there has been substantial slowdown because of political disagreement on key parts of the Regulation such as the one-stop shop. The criticisms raised by Legal may not rule out the possibility of a one-stop shop completely, but must be taken seriously and require further analysis. In addition, there remain different blocs of member states in the council that have contradictory views on the Regulation, with some wanting to reach agreement on it soon (e.g., France, Italy and Spain), others opposing it completely (e.g., Denmark, Sweden and the U.K.), and a third group being in the middle. The position taken by Germany will be crucial to see if the council can reach agreement.

IV. Possible Next Steps and Outlook

In the two years since the proposal was issued, substantial progress has been made in reaching a final agreement, but many problems remain. While the Parliament has made significant progress by adopting a compromise text, many of the amendments are controversial and are likely to be contested in the so-called ''trialogue'' procedure, a process of negotiation between the European Parliament, the council and the commission, that begins once the council has reached internal agreement. However, it remains unclear whether the council will be able to agree on a text because of political disagreement among member states and inter-institutional legal objections against key concepts of the Regulation such as the one-stop shop mechanism.

In addition, political factors will continue to complicate the reaching of an agreement between the three EU institutions. It can be expected that the European Parliament will hold a plenary vote on the LIBE-approved version of the Regulation in the spring of 2014, in order to create a legacy that could be the subject of negotiations later on in the year. Any texts agreed on by the existing Parliament before it leaves office will not be legally binding on the new Parliament and commission, but will leave a ''line in the sand'' that will be difficult for the commission and council to ignore in the subsequent negotiations.

The new MEPs elected in May 2014 are expected to be a more ''Eurosceptic'' group than the existing Parliament, raising the question of whether they will want to reach agreement on such a wide-ranging project as the Regulation. Furthermore, the selection of a new president of the European Commission and College of Commissioners is a process that is likely to be highly political. It is also not clear whether the new commissioner in charge of data protection will be as interested in the reform proposal as Reding has been. Given that the period from May until November 2014 is likely to be taken up with selecting and electing the commission, choosing new heads of committees and political groups in the European Parliament and similar political tasks, it seems that the earliest that agreement could be reached on the Regulation would be the end of 2014 or early 2015.[14]

The recent Edward Snowden revelations have been a wake-up call at a political level and have increased pressure for final adoption of the Regulation.[15] They have also led to strong reactions from MEPs, who have sought to toughen provisions in the Regulation dealing with transborder data flows, and who have organized numerous hearings on mass surveillance issues.[16] The commission and the council have also been active in relation to trans-Atlantic data protection matters, such as by examining the efficacy of the U.S.-EU Safe Harbor Framework.[17] In response to all these events, the European Commission proposed several steps in November 2013 with a view to restoring trust in EU-U.S. data flows.[18]

Much work has been done on the proposal, and it is clear that the EU cannot continue indefinitely under the existing Data Protection Directive 95/46/EC, so that it is hard to imagine that some sort of agreement on the Regulation will not be reached in the coming months. At the same time, final agreement is complicated by political factors that go beyond data protection, such as the current wave of ''Euroscepticism'' and resistance at a national level against EU-led regulatory harmonization. The next year will be crucial to determining whether the EU and its political institutions are able to cope with the mammoth task of producing a new, future-proof data protection framework covering half a billion European citizens.

---

[14] For an analysis of the impact of the upcoming parliamentary elections and the appointment of a new commission, *see* Burton & Pateraki, *supra* note 4.

[15] *See* Christopher Kuner, *Legal Reform Is Needed on Both Sides of the Atlantic, Not Just in Europe*, IAPP Privacy Perspectives Blog, (Dec. 2, 2013), https://www.privacyassociation.org/privacy_perspectives/post/legal_reform_is_needed_not_only_in_europe; Christopher Kuner, *Parallel Privacy Universes and PRISM*, IAPP Privacy Perspectives Blog (July 30, 2013), https://www.privacyassociation.org/privacy_perspectives/post/parallel_privacy_universes_and_prism.

[16] By the time this article was being finalized, the LIBE Committee had held 15 hearings on ''Electronic Mass Surveillance.'' For more information *see* LIBE Committee, *Events*, http://www.europarl.europa.eu/committees/en/libe/events.html#menuzone (last visited Dec. 31, 2013).

[17] Press Release, European Comm'n, European Comm'n Calls on the U.S. to Restore Trust in EU-U.S. Data Flows (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_IP-13-1166_en.htm (12 PVLR 2012, 12/9/13).

[18] Memorandum from European Comm'n, Restoring Trust in EU-US data flows—Frequently Asked Questions (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

  PVLR ISSN 1538-3423