Bloomberg BNA

Privacy and Security Law Report®

The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report



BY CÉDRIC BURTON, CHRISTOPHER KUNER, AND ANNA PATERAKI

One year ago (Jan. 25, 2012), the European Commission published its proposal to reform the European Union's (EU) legal framework for data protection. The proposal includes two different legal instruments: a General Data Protection Regulation covering data processing by the private sector and public authorities (the Regulation),[1] and a General Data Protection Directive applicable to law enforcement (the Directive).[2] In ambition, scope, and size, the Regulation is the largest and most complex piece of data protection legislation ever proposed. The proposal was just the first step in a complicated, multiyear process that must still clear many hurdles before it is completed.

On Jan. 8, the main rapporteur for the Regulation in the EU Parliament, German Green Member of the European Parliament (MEP) Jan Philipp Albrecht, issued a draft report (the Albrecht Report or the Report)[3] on the Regulation for the Parliament's Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) that raises many questions about the proposal's future direction, and its implications for the private sector.[4] The Albrecht Report proposes substantive amendments to the Regulation, and its issuance provides a good opportunity to evaluate some of the data protection issues at stake, and to take stock of the progress of the reform proposals thus far (the discussion herein will be limited to the Regulation).

I. Activity Since Publication of the Proposal

The substance of the Regulation has already been described in detail, and we will thus not go into it here.[5]

[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) (11 PVLR 178, 1/30/12), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

[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, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

Cédric Burton (cburton@wsgr.com) and Anna Pateraki (apateraki@wsgr.com) are associates and Christopher Kuner (ckuner@wsgr.com) is senior of counsel with Wilson Sonsini Goodrich & Rosati PC. All are with the firm's Brussels office.

[3] LIBE draft report 2012/0011 (COD) dated Dec. 17, 2012 (12 PVLR 65, 1/14/13), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf. An erratum to the Albrecht report was issued Jan. 10 and is available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/erratum_/erratum_en.pdf.

[4] The Albrecht Report was officially presented during a Jan. 10 LIBE Committee meeting.

[5] *See* Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," (Feb. 6, 2012) Bloomberg BNA *Privacy & Security Law Report* (11 PVLR 215, 2/6/12).

 ISSN 1538-3423

Following its publication, the sheer size and scope of the proposal seems to have stunned most observers into silence, as they began reviewing it in detail. Many stakeholders in both the private and public sectors then began to issue papers reacting to the proposal.[6]

Once issued, the Regulation entered into the EU ordinary legislative procedure.[7] Most observers believe that the procedure will take at least two years to complete, with others being more pessimistic (one high-level representative of a member state government has stated that it may take up to 10 years!). EU Commission Vice-President Viviane Reding, who is in charge of the data protection reform for the EU Commission, is known to be keen on the procedure being completed in time for the next EU parliamentary elections in June 2014.

The Danish government, which held the six-month presidency of the Council of the European Union (the EU Council) at the time the proposal was announced, began to consider it in a series of meetings with representatives of member state governments (meeting under the auspices of the EU Council's Working Party on Information Exchange and Data Protection, known as ''DAPIX''). The approach of the Danish presidency was methodical, and involved proceeding through the proposal article-by-article.[8] The article-by-article procedure continued in the following EU Council presidency held by Cyprus which in addition decided to follow a horizontal approach focusing on three main issues: (i) delegated and implementing acts; (ii) administrative burdens and compliance costs; and (iii) more flexibility for the public sector.[9]

Because of the length of the proposal, the Danish and Cypriot presidencies resulted in the Council getting through less than half of it by the end of 2012. In addition, many of the tentative conclusions reached in the DAPIX meetings have been made subject to reservations on behalf of various member states, indicating that there is substantial disagreement among them on individual points (one of the most contentious points has been the insistence of Germany that public authorities be exempted from the scope of the Regulation).

The proposal has also caused discussions in the member states themselves. Given the current climate of euro-skepticism, any legislative initiative to produce full harmonization of data protection law across all 27 of them (soon to be 28, with Croatia joining later in 2013) was never going to be easy. In some member states, the proposal has led to national *angst* about stronger national data protection standards being watered down through the adoption of mandatory EU standards.

Other committees in the EU Parliament besides the LIBE Committee have also issued draft opinions on the Regulation, including the Employment and Social Affairs Committee; the Industry, Research and Energy Committee; the Internal Market and Consumer Protection Committee; and the Legal Affairs Committee.[10] However, the Albrecht Report is particularly significant since MEP Albrecht of the LIBE Committee has been selected as the lead rapporteur for the EU Parliament. The Regulation has been subject to a huge amount of lobbying, much of which has been carried out by U.S.-based companies and also by the U.S. government, and has led to tensions between the EU Commission and the U.S. government.

II. The Albrecht Report

The Albrecht Report is a massive document of 215 pages that includes 350 draft amendments. The following analysis covers some of the main topics of particular interest to the private sector, and compares the amendments to the relevant provisions of the Regulation.[11] It is important to remember that many other amendments to the Regulation will be made by the EU Parliament over the coming months, so that the current amendments in the Albrecht Report are by no means the Parliament's last word.

A. General Remarks

The Albrecht Report generally supports the objectives of the EU Commission's proposed reform, and its attempt to establish a ''coherent, harmonious and robust framework with a high level of protection of all data processing activities in the EU.''[12] In particular, the Report strongly supports the Commission's proposal to chose a regulation (rather than a directive) as the legal basis for the data protection framework, the objective being to reduce the current fragmented approach to data protection in the EU.

The Report further supports the Commission's ambition of ''reducing the administrative burden, strengthening individuals' rights, further advancing the internal market dimension and ensuring better enforcement of data protection rules, and strengthening the global dimension.''[13] The discussions during the LIBE meetings have also emphasized that the Regulation and the Directive are deeply linked, meaning that there will be no agreement on the Regulation without one on the Directive. The EU Commission reacted positively to the Albrecht Report.[14] At this stage, the EU Council (via the current Irish Council Presidency) has committed to

[6] Most stakeholders' papers are collected at the WSGR EU Data Protection Regulation Observatory, see http://www.wsgr.com/eudataregulation/stakeholders-position-papers.htm.

[7] Regarding the ordinary legislative procedure, see http://www.europarl.europa.eu/aboutparliament/en/0080a6d3d8/Ordinary-legislative-procedure.html.

[8] The Danish presidency reviewed Articles 1 to 10 as well as Articles 80(a) and 83 of the Regulation and proposed amendments. For more information see the presidency's report, *available at* http://www.statewatch.org/news/2012/jun/eu-council-revised-dp-position-11326-12.pdf.

[9] The Cyprus presidency reviewed up to Article 40 of the Regulation. For the results of the horizontal approach see the presidency's report, *available at* http://register.consilium.europa.eu/pdf/en/12/st16/st16525.en12.pdf.

[10] For a full list of the involved parliamentary committees and their various opinions and working documents on the Regulation, see the WSGR EU Data Protection Regulation Observatory at http://www.wsgr.com/eudataregulation/process-updates.htm.

[11] *Id.*

[12] *See* Albrecht Report, explanatory statement, p. 209.

[13] *See* Albrecht Report, explanatory statement, pp. 211–15.

[14] *See* EU Commission's memo, ''Commission welcomes European Parliament rapporteurs' support for strong EU data protection rules,'' Jan. 8, 2013, *available at* http://ec.europa.eu/commission_2010-2014/reding/pdf/m13_4_en.pdf.

  PVLR ISSN 1538-3423

make the Regulation a major priority, and to work in cooperation with the EU Parliament.[15]

B. Key Elements of the Albrecht Report

1. Broader Application of EU Data Protection Law

The criteria for the application of EU data protection law have been broadened. As stated in the Report, companies that collect data of EU individuals with the aim of offering goods or services (even without any payment) or monitor such individuals (not just their behavior) would be subject to EU data protection law.[16] It is unclear what the differences between monitoring individual behavior and monitoring an individual are, but arguably the latter has a broader scope.

Some of the exemptions for small and medium-sized enterprises (SMEs) contained in the Commission proposal have been modified, to increase the reach of the Regulation. In particular, reference to the threshold of 250 employees has been replaced by a criterion based on the number of data subjects involved in the processing activities, and as soon as data from 500 data subjects are processed per year, the exceptions would not apply. Since most, if not all, email systems, employee databases, customer databases, *etc.* will contain data of at least 500 individuals, virtually any companies processing personal data, in particular those that are active on the internet, would be subject to the entire set of obligations included in the Regulation. According to the Report, the rationale of this change is to cover areas like cloud computing where small companies ''can process large amounts of data through online services.''[17]

2. Weakening of the One-Stop-Shop Approach

The Regulation as proposed by the EU Commission sought to advance the internal market by providing that a single data protection authority (DPA) or ''lead DPA'' (the one of the data controller's or data processor's main establishment) be responsible for ensuring compliance with EU data protection law throughout the EU. However, the Report weakens the one-stop-shop approach by stating that each DPA should be competent to supervise all data processing operations on the territory of its member state or where the data of its residents are processed. Under the Albrecht Report, the lead DPA[18] would only serve as a single contact point to ensure cooperation among DPAs for cross-border issues (*i.e.*, when a data controller or data processor is established in more than one member state or where personal data of the residents in several member states are processed; the latter criterion was not contained in the Regulation). In other words, instead of having a single DPA competent for data protection law throughout Europe, the lead DPA would in effect become a central contact point for companies, but these companies would still have to deal indirectly with other European DPAs. This amendment was likely proposed to assuage some data protection authorities who are reluctant to lose jurisdiction over data processing concerning their nationals.

In addition, despite lobbying efforts and other parliamentary committee opinions proposing amendments to the main establishment concept, which is crucial for the functioning of the lead DPA, the current version of the Albrecht Report does not include any amendments related to this specific issue.[19]

3. Modification or Addition of Key Concepts and Obligations

The Albrecht Report modifies a number of key definitions and introduces some new concepts, in particular the following:

- **Personal data**. The Report broadens the concepts of personal data by providing that data subjects now include natural persons who can be identified or ''singled out'' directly or indirectly, ''alone or in combination with associated data.''[20] According to the Report, internet protocol (IP) addresses, cookies, and other unique identifiers will in most cases be considered to be personal data, since they leave traces and can be used to single out natural persons, unless it can be shown that they do not allow for the singling out of a natural person.[21]
- **Pseudonyms and anonymous data**. The Report creates a new category of pseudonymous data. According to the Report, a pseudonym is a ''unique identifier which is specific to one given context and which does not permit the direct identification of a natural person, but allows the singling out of a data subject.''[22] Lighter data protection obligations would apply to the processing of pseudonyms.[23] The Report also introduces a definition of anonymous data as ''any data that cannot be related, directly or indirectly, alone or in combination with associated data, to a natural person or where establishing such a relation would require a disproportionate amount of time, expense, and effort, taking into account the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed.''[24] Anonymous data will not be subject to the Regulation.[25]
- **Roles of the parties**. The definitions of controller and processor included in the Regulation stay unchanged. However, the Report introduces the concept of ''producer'' of a data filing system (*i.e.*, the entity that creates automated data processing or filing systems to be used by data controllers or data

[15] *See* the Irish Minister for Justice, Equality and Defense publishes Agenda for Justice and Home Affairs Informal, *available at* http://www.eu2013.ie/news/news-items/20130111jhaagenda/.

[16] According to the Albrecht Report, the ''Regulation should cover not only the monitoring of the behavior of Union residents by data controllers outside of the Union, such as through internet tracking, but all collection and processing of personal data about Union residents.'' Justification to Amendment 83, p. 63.

[17] *See* justification to amendment 223 of the Albrecht Report.

[18] In cases of disagreements regarding the lead authority, the European Data Protection Board would determine which supervisory authority is the lead.

[19] Compare amendments of the ''main establishment'' concept, Article 4(13) and Recital 27 of the Regulation, as proposed by the Industry, Research and Energy Committee and the Legal Affairs Committee, *available at* http://www.wsgr.com/eudataregulation/process-updates.htm.

[20] *See* amendment 84 of the Albrecht Report.

[21] For example, the Report states that IP addresses used by companies can in theory not be considered to be personal data, see Albrecht Report, amendment 15, Recital 24, p. 16.

[22] *See* amendment 85 of the Albrecht Report.

[23] *See* justification to amendment 85 of the Albrecht Report.

[24] *See* amendment 14 of the Albrecht Report.

[25] *Id.*

processors). The producer will have to comply with privacy by design and privacy by default principles. While the exact scope of this definition remains to be seen, it would likely cover software and hardware developers. In addition, the Report reinforces the obligations applicable to joint controllers and requires a clear allocation of roles and responsibilities among them that must be described in their privacy notices.

- **Data breach notification**. The deadline within which data breaches must be notified to the DPA is extended from 24 hours to 72 hours, but DPAs would be required to keep a public register of the types of breaches notified. Furthermore, to prevent notification fatigue, data subjects should only be notified where a breach is likely to adversely affect the protection of their personal data or privacy (*e.g.*, in cases of identity theft or fraud, financial loss, physical harm, significant humiliation, or damage to reputation). In addition to the elements described in the Regulation, the notification to data subjects should contain information regarding their rights, including possibilities of redress.

4. Legal Basis for Data Processing

Considerable changes have been made to the legal bases available for the processing of personal data. In particular, the consent requirements have been tightened, and the balancing of interests as a legal basis has been largely restricted, as follows:

- **Consent**. The Report considers consent as the cornerstone of EU data protection law and as the best way for individuals to control data processing activities. As indicated by MEP Albrecht during a Jan. 9 press conference, the Report supports the idea of ''if you want my data, ask for consent.''[26] Accordingly, the importance of consent is even increased compared to the EU Commission proposal. Consent must be freely given, specific, informed and explicit, consequently impeding data controllers from relying on implicit consent and on pre-ticked boxes.[27] In addition, the processing of data for the execution of a contract may not be made conditional on consent for uses of personal data that are not necessary for the execution of the contract or to provide the service. This means, for example, that consent will not be a valid legal basis where the company ''is in a dominant market position with respect to the products or services offered to the data subject, or where a unilateral and nonessential change in terms of service gives a data subject no option other than to accept the change or abandon an online resource in which they have invested significant time.''[28] This would have a significant impact on how companies actually obtain individuals' consent and potentially disturb existing business models.
- **Balancing of interests**. In addition to the limitations regarding the use of consent, the Report restricts other legal bases for the processing of personal data. In particular, processing data for the purpose of the legitimate interest pursued by the data controller that is not overridden by the interest of the data subject (''balancing of interests test'') should be only used ''in exceptional circumstances.''[29] Therefore, companies relying on this legal basis will have to comply with additional requirements, such as providing information about why their legitimate interest should prevail. The Report also specifies situations where the legitimate interests of the controller should and should not prevail. For example, the legitimate interest of the controller would override that of the data subject's where the controller can rely on the right to freedom of expression, or processes data for the direct marketing of its own similar products or services to existing customers.[30] On the other hand, the legitimate interest of the controller would not prevail if the processing involved sensitive data, location data, and biometric data, or included profiling and large scale data combinations.[31] Finally, companies will not be able to rely on the balancing of interests to process personal data for a purpose different than that of data collection. This will restrict the abilities of companies to rely on this legal basis, in particular for data analytics purposes.

5. Rights of Individuals

One of the main objectives of the Report is to strengthen individuals' rights. Interestingly, the Report tends to reinforce existing rights, but also tries to simplify the legal framework for individuals by merging some of them:

- **Right of access and right to data portability**. The right of access has been broadened, and includes new elements such as the right to obtain information regarding profiling in clear and plain language, and the right to obtain confirmation as to whether public authorities have requested personal data, together with information about whether or not the company had complied with such request and an overview of the disclosed data. The right to data portability is now considered to be an extension of the right of access, while by contrast the EU Commission proposal considered these rights separately; the legal consequences of this change are unclear. The rationale proposed by the Albrecht Report for linking these rights is that if a data subject wants to exercise its right of access, the data should be provided in a useful format that allows individuals to migrate them to other platforms or services.
- **Right to be forgotten and to erasure**. The controversial right to be forgotten is viewed in the Report as an extension of the right to erasure and rectification. Again, the legal implications of this merger are unclear, but at least this has the merit of trying to simplify the rights of individuals. The Report restricts the scope of that right by providing that it is ''neither legitimate [nor] realistic'' in situations where the individual has agreed to make his/her personal data public.[32] Therefore, if the initial publication of the data by the data controller was conducted with the data subject's consent or based on another lawful legal basis, controllers would no longer have to take reasonable steps to contact third parties and request them to erase copies of data. However, in cases where data are transferred or published without a proper legal basis, the original data controller is obliged to inform such third parties and ensure the erasure of the data. The Report maintains freedom of expression as a potential exception to the right to be forgotten, underlying the importance of balancing these two rights against each other for ''any measures for erasure of published personal data.''[33]

[26] Albrecht press conference, Jan. 9, 2013, video *available at* http://www.europarl.europa.eu/ep-live/de/other-events/video?event=20130109-1000-SPECIAL-UNKN.

[27] *See* amendments 17 and 19 of the Albrecht Report.

[28] *See* amendment 20 of the Albrecht Report.

[29] *See* amendment 22 of the Albrecht Report.

[30] *See* amendment 101 of the Albrecht Report.

[31] *See* amendment 102 of the Albrecht Report.

[32] *See* Albrecht Report, explanatory statement, p. 212.

[33] *See* amendment 148 of the Albrecht Report.

  PVLR ISSN 1538-3423

- **Right to object**. The right to object is broadened and strengthened. For example, when the legal basis for the processing is the legitimate interest of the controller or in case of profiling, individuals will always be able to object to the processing free of charge. (The Albrecht Report no longer allows the continued processing of data in case of a compelling legitimate ground.)
- **Increased notice obligations**. The Report encourages the use of multilayered privacy notices together with the use of symbols. However, compared to the EU Commission proposal, the Report imposes increased notice obligations on companies in the following circumstances:
  - If a company relies on the balancing of interests for the processing, it will have to provide information on what its legitimate interest is and to explain why it relies on this legal basis.
  - A company must provide notice when personal data are disclosed to a public authority (*e.g.*, to a law enforcement agency).
  - Specific information must be provided when personal data are transferred outside of the EU on the basis of appropriate safeguards (*e.g.*, a copy of the appropriate safeguards used as the basis of the transfer must be available).
  - Information must be provided on the existence of the profiling activities, the logic behind the processing, and how to object to profiling.
  - The notice must include a list of all data recipients (and not only the categories of data recipients).
  - The notice must include information on the rights and mechanisms to oppose the processing of personal data in clear and plain language.

Joint data controllers will also be subject to increased notice obligations as they will have to describe the allocation of roles and responsibilities among them. Due to the complexity of the current data processing activities, it may be difficult to convey this information clearly to individuals.

- **Effective redress**. The possibilities for individuals and associations to seek effective redress are further strengthened. For example, the right to lodge a complaint before DPAs, to go before the courts, and to seek redress for nonpecuniary loss will be extended to any associations acting in the public interest, and will not be limited to associations specialized in data protection.

6. Profiling

The legal regime applicable to profiling is tightened, and stricter rules will apply. Profiling will be allowed only in limited situations, in particular: (i) with the individuals' consent (which has to be freely given, specific, informed, and explicit); (ii) when profiling is explicitly permitted by legislation; or (iii) when profiling is ''necessary'' for entering into or the performance of a contract, subject to certain restrictions.[34] In addition, reference is now made to ''electronic information and communications services'' in the definition of profiling. While these definitions seem to derive from the EU e-Commerce Directive[35] and the Telecom package,[36] none of them match the existing definitions contained therein, which can only lead to confusion. Profiling that involves sensitive data or children is prohibited. Finally, notice obligations and the rights of individuals have been strengthened as described above.

7. Accountability, DPO, and Related Data Protection Principles

The Report welcomes the EU Commission's proposal to shift the regulatory focus from notifying data processing to the DPAs to practical measures inspired by the accountability principle and implemented by company data protection officers (DPOs). Consequently, obligations resulting from the accountability principle have been maintained, reinforced, and to some extent simplified:

- **Documentation requirement**. The documentation requirement and notice obligation are now seen as two sides of the same coin. Compared to the Regulation, this would arguably ease some of the burdens on companies by requiring them to only prepare one set of documentation on their data processing activities that would allow them to comply with both the documentation and notice requirements. However, it should be noted that, as described above, the notice obligations have been considerably increased, so the burden may not be decreased for most companies.
- **Data Protection Officer**. The role of DPOs is strengthened and inspired to a large extent by the current German legal framework. One of the major changes concerns the criterion for the designation of a DPO. The Report provides that mandatory designation of a DPO is no longer based on the size of the enterprise (*i.e.*, 250 employees or more), but rather on the relevance of the data processing (*i.e.*, a DPO will have to be appointed as soon as a data controller or processor processes data about more than 500 individuals per year). Thus, in practice, most if not all companies processing personal data on the internet will have to appoint a DPO, which will be problematic for start-ups and SMEs that may lack the necessary resources. The Report also requires companies with a core activity consisting in processing sensitive data or conducting profiling activities to appoint a DPO. The minimum period of appointment for DPOs is extended from two to four years, and DPOs will have to be direct subordinates of the head of the company's management. In addition, DPOs will be bound by strict confidentiality requirements and subject to an obligation to report suspected violations to DPAs.
- **Data protection by default, data protection by design, and data protection impact assessments**. These principles already included in the EU Commission proposal are welcomed by the Report as core innovations of the reform. The Report also provides for new obligations, such as imposing data protection by design and data protection by default on producers. Further, the Report increases the number of instances in which a data protection impact assessment is required (*e.g.*, where personal data are made accessible to a large number of persons or if high volumes of personal data about a person are pro-

[34] *See* amendments 38, 158, and 160 of the Albrecht Report.

[35] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (''Directive on electronic commerce'').

[36] The EU Telecom package consists of the following Directives: Framework Directive, Authorization Directive, Access Directive, Universal Service Directive, and e-Privacy Directive. For more information see http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm.

cessed or combined with other data), and suggests that the DPO be consulted where a data protection impact assessment indicates that processing operations involve high risks.

8. International Data Transfers

While the Commission proposal introduced a bit more flexibility and some improvements regarding data transfers, the Albrecht Report takes a strict approach that will increase the burden on the private sector:

- **Adequacy determination**. One of the innovations of the Regulation was to allow for the possibility of recognizing specific sectors in third countries as providing an adequate level of data protection. This option is rejected by the Report, as ''this would increase legal uncertainty and undermine the Union's goal of a harmonized and coherent international data protection framework.''[37] Of particular concern is the provision that would make all current EU Commission and DPA adequacy decisions (*e.g.*, the EU-U.S. Safe Harbor Framework) expire two years after the entry into force of the Regulation, which introduces considerable legal uncertainty. New adequacy decisions would probably have to be adopted via delegated acts by the EU Commission, which would not only require the approval of the European Data Protection Board (EDPB), but would also allow the EU Parliament and the EU Council to block an adequacy procedure, thus presenting a danger to global data flows and the current data economy. Finally, the criteria for assessing the adequacy of third countries are strengthened, and the EU Commission is given an obligation to monitor the effectiveness of its adequacy findings.

- **Appropriate safeguards**. The Report modifies the general approach of the Regulation regarding data transfers by way of using appropriate safeguards (*e.g.*, Binding Corporate Rules (BCRs) and standard contractual clauses). The Report provides for a general prohibition of data transfers that applies unless adequate safeguards are implemented, while the Regulation took the opposite approach and authorized transfers only if certain conditions were met. The Report has also slightly increased the requirements for approval of BCRs, and thus arguably goes beyond existing DPAs' practices.

- **Access requests from non-EU authorities**. The Report provides for a specific legal regime regarding data transfers to non-EU public authorities, and requires companies to obtain the prior approval of DPAs when seeking to disclose data in response to a court or other legal order issued in a third country. This clause could apply to situations involving law enforcement access to data stored in the cloud, or to requests related to e-discovery orders by U.S. courts. The amendment would require that both the relevant DPA and the data subjects be informed about such requests, which may violate foreign requirements in some cases.

- **Failure to recognize accountability as a basis for international data transfers**. It is notable that despite strong lobbying efforts to introduce an accountability approach for data transfers, the Albrecht Report does not mention this.

[37] *See* justification to amendment 241 of the Albrecht Report.

9. Coordination Among DPAs, the Consistency Mechanism, and Delegated and Implementing Acts

Generally speaking, the Report gives more power to the DPAs, either directly or through the EDPB, the role of which is significantly increased:

- **Data protection authorities**. The Report requires member states to comply with certain minimum requirements regarding the staffing and resourcing of DPAs, and welcomes the Commission's proposal to empower them to impose strong fines on companies violating EU data protection rules.

- **Consistency mechanism**. The consistency mechanism has been heavily modified. The Report creates an alternative consistency mechanism based on the lead DPA principle discussed above. The new draft would require the lead DPA to ensure coordination among the various DPAs involved and to consult with them before adopting a measure. If a DPA disagrees with the draft measure proposed by the lead DPA, the EDPB will have the right to intervene and to issue an opinion. If the lead DPA does not intend to follow this opinion, it will be required to provide a reasoned opinion to the EDPB. The EDPB may then adopt a final decision, by a qualified majority, which is legally binding upon the lead DPA. This decision can be subject to judicial review and can be suspended or challenged by the EU Commission or before the EU Court of Justice.

- **Delegated and implementing acts**. The Regulation included a large number of Commission delegated and implementing acts, the number of which has been considerably reduced by the Albrecht Report. Depending on the topic, references to delegated and implementing acts are now either directly covered by the Regulation (thus creating more detailed and prescriptive provisions), or have been replaced by obligations of the EDPB to further specify the criteria and requirements of particular provisions; the EU Commission has recently demonstrated its openness to such an approach.[38] When references to delegated and implementing acts have been retained, the Report requires in some cases that the Commission adopt them before the Regulation enters into force, so as to ensure legal certainty (*e.g.*, for data breach notifications, data protection impact assessments, and the right to be forgotten and to erasure).

10. Sanctions and Fines

The sanctions regime is to a large extent similar to the Commission's initial proposal. The tiered fine system has been retained, but the Report provides that the highest level of fine applies when the violation is not explicitly mentioned in one of the lower categories of fines. Consequently, this increases the number of instances in which the highest level of fines would apply. Nevertheless, the Report introduces some proportionality and flexibility regarding the actual level of sanctions. In particular, under the Report, the DPAs and the EDPB would have more flexibility to determine the amount of the applicable fine by taking into account various criteria in their assessment (little flexibility was given in that respect under the Regulation). Such criteria include an assessment of whether accountability

[38] *See* Commissioner Vivian Reding (Speech/12/897), ''The overhaul of EU rules on data protection: making the single market work for business,'' *available at* http://europa.eu/rapid/press-release_SPEECH-12-897_en.htm?locale=en.

   ISSN 1538-3423

measures were implemented, and whether the company actively cooperated with DPAs to remedy the infringement and mitigate possible adverse effects.

III. Next Steps and Outlook

Members of the LIBE Committee will now review the Report and suggest amendments or modifications with a view to finalizing it. Work from other parliamentary committees will also be taken into account in an attempt to reach the broader possible agreement within the EU Parliament. The next steps are as follows:

- The LIBE Committee deadline for other political groups to table amendments on the Albrecht Report is Feb. 27.
- The advisory committees have until March to submit their final comments.
- Final vote on the Albrecht Report in the LIBE Committee is tentatively scheduled for April 24–25.
- The Report will then likely be presented to the entire EU Parliament for vote in plenary probably by mid-2013.

In parallel, the DAPIX group will meet under the Irish Council Presidency to try to reach a political agreement and propose amendments to the Regulation; several meetings are planned over the coming weeks.[39] Substantial disagreements between the member states still need to be resolved before the EU Council can reach a common position, and timing of this is uncertain.

Many of the proposals contained in the Albrecht Report are not surprising given the Parliament's orientation towards protecting individual rights, but they will be viewed with concern by companies that would have to implement them. The position of the EU Parliament has been substantially strengthened under the Lisbon Treaty, so that its final report will carry a great deal of weight. While the Albrecht Report will serve as the basis for the discussions in Parliament and gives a good indication of its likely position, there is no doubt that it will be modified in the coming weeks, in particular before the full Parliament adopts its own final position in 2013.

Once the EU Parliament and the EU Council have reached their final positions, then they will still have to negotiate between themselves (with the participation of the EU Commission) to reach a final agreement; if this cannot be reached, then there will be a so-called ''second reading'' between the various institutions that will result in further negotiations. Thus, the procedure is likely to continue at least into 2014.

Developments since the Commission proposal was issued in January 2012 demonstrate several important points to be kept in mind about the EU data protection reform:

- The reform is a marathon, not a sprint. The process will likely take at least two more years to complete, if not longer, and there will be further important steps along the way. This means that those who want to make their voices heard should think strategically about how best to provide input.
- The reform is being driven at least as much by internal European politics as by the substantive issues, and as the process moves towards its conclusion, the political dynamics will become increasingly important. The EU is currently in the midst of an identity crisis, and the data protection reform is one of the first large-scale initiatives to harmonize fundamental rights law since adoption of the Lisbon Treaty in 2009; the jury is still out as to whether the new legal framework under the treaty will result in final product of high quality.
- There is sensitivity in Brussels about lobbying by U.S. organizations (including by the U.S. government). The ''full court press'' lobbying style that may be appropriate in Washington can be counterproductive in Brussels.
- Arguments about economic efficiency resonate less in Brussels than they do in Washington. The current economic crisis should make the need to spur economic growth a major factor in structuring the data protection reform, and all three institutions involved in it (the EU Commission, EU Council, and the EU Parliament) often clothe their proposals in doubtful arguments about how they would help the EU economy. But fundamental rights considerations and internal EU politics are proving to be more powerful factors in the reform than the reality of what rules would promote economic growth.

For the first time in a generation, all actors involved in the data protection reform agree on the need for a more coherent and effective legal framework for data protection in the EU, and such a framework is in reach. But the necessary reforms risk being overwhelmed in a maelstrom of political maneuvering and internal struggles between the EU institutions. The coming months will be crucial in determining the further direction of the EU's data protection reform.

[39] *See* http://www.eu2013.ie/news/news-items/20130111jhaagenda/.