Bloomberg BNA

Privacy and Security Law Report®

The Proposed EU Data Protection Regulation Three Years Later: The Council Position

By Cédric Burton, Laura De Boel, Christopher Kuner and Anna Pateraki

It has been over three years since the European Commission proposed its reform to the European Union legal data protection framework .[1] On June 15, the ministers of justice of all 28 EU member states, sitting as the Council of the EU (Council), reached a crucial agreement for the future EU data protection legal framework.[2] Much work still needs to be completed, but this is a major step forward in the adoption of the EU General Data Protection Regulation (Draft Regulation or Regulation).[3]

The Draft Regulation introduces important changes to EU data protection law that will have a significant impact on companies doing business in the EU.

The Draft Regulation was originally based on a proposal issued by the European Commission (Commis-

Cédric Burton (cburton@wsgr.com) is of counsel, Christopher Kuner (ckuner@wsgr.com) is senior privacy counsel and Laura De Boel (ldeboel@wsgr.com) and Anna Pateraki (apateraki@wsgr.com) are senior associates in the Brussels office of Wilson Sonsini Goodrich & Rosati.

All authors devote 100 percent of their time to European Union and global data protection law and help clients manage risks related to the enforcement of privacy and data protection laws globally. The authors are grateful to Anna Ciesielska, legal intern in the firm's Brussels office, for her excellent research assistance.

[1] The proposed reform package consisted of a 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 (Draft Regulation), COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, and a 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 (the Draft Directive) COM (2012) 10 final, *available at* http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0010; this article will only deal with the Regulation.

[2] *See* Council's press release of June 15, 2015, *available at* http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/ (14 PVLR 1124, 6/22/15).

[3] To keep up to date with the legislative developments concerning the Draft Regulation, *see* the Wilson Sonsini Goodrich & Rosati EU Data Protection Regulation Observatory at https://www.wsgr.com/eudataregulation/index.htm.

sion) in 2012,[4] and the European Parliament (Parliament) approved its own version in 2014.[5] Now that the Council has also adopted its own version (known as a ‘‘General Approach’’),[6] the EU institutions are ready to enter the final stage of the legislative process. Known as the ‘‘Trilogue,’’ this is a negotiation between representatives of the Council, the Commission and the Parliament, in which the three institutions will attempt to reach an agreement on the final text of the Draft Regulation.

The Draft Regulation introduces important changes to EU data protection law that will have a significant impact on companies doing business in the EU. While the timing of final approval is still uncertain, the fact that the Council has reached a General Approach significantly increases the chances that the final text of the Draft Regulation will be adopted in the foreseeable future. This article analyzes the current status of the Draft Regulation, with a focus on the Council's General Approach adopted June 15.

The Council's General Approach and How It Relates to the Commission's Proposal and the Parliament's Amendments

The Council's General Approach is a massive document of 201 pages (dated June 11) that includes hundreds of amendments covering all articles of the Draft Regulation.[7] The following analysis covers some of the main topics of interest to the private sector and explains how the Council's amendments deviate from the Commission's proposal and the Parliament's amendments.

I. General Remarks

Since the Draft Regulation was proposed by the Commission in January 2012 to replace the EU Data Protection Directive 95/46/EC (Directive),[8] both the Parliament and the Council have been working intensively on their own amendments. The Parliament issued its first draft report on the proposal in early 2013.[9] This text was heavily debated in Parliament and triggered massive comments from stakeholders. After lengthy debates in different committees, the Parliament adopted its amendments to the Commission's proposal March 12, 2014.[10]

In parallel to the negotiations in the Parliament, the Council has been meeting since 2012 to discuss its own amendments to the Commission's proposal. The work of the Council has been spread over the presidency of various member states, including the Danish Presidency (first half of 2012), the Cypriot Presidency (second half of 2012), the Irish Presidency (first half of 2013), the Lithuanian Presidency (second half of 2013), the Greek Presidency (first half of 2014), the Italian Presidency (second half of 2014) and the Latvian Presidency (first half of 2015). During this period, the Council had reached non-binding political agreements at the Justice and Home Affairs (JHA) minister level on certain topics (know as ‘‘Partial General Approach’’).[11] After lengthy debates, the Council finally reached a General Approach[12] covering amendments in relation to all

[4] 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). For a detailed analysis of the Commission's 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), *available at* https://www.wsgr.com/eudataregulation/pdf/kuner-020612.pdf.

[5] *See* the European Parliament legislative resolution of 12 Mar. 2014 on the 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, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (13 PVLR 444, 3/17/14). For a detailed analysis of the Parliament's amendments, *see* Christopher Kuner, Cédric Burton and Anna Pateraki, *The Proposed EU Data Protection Regulation Two Years Later*, Bloomberg BNA Privacy & Sec. L. Rep. (Jan. 6, 2014), *available at* https://www.wsgr.com/eudataregulation/pdf/kuner-010614.pdf (13 PVLR 8, 1/6/14).

[6] *See* Latvian Presidency, General Data Protection Regulation, preparation of a General Approach, June 11, 2015, document no. 9565/15, *available at* http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

[7] *Id.* This text was approved as a General Approach June 15.

[8] Directive 95/46/EC of the European Parliament and the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, p. 31, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

[9] *See* the Draft Report of the Parliament's Committee on Civil Liberties, Justice, and Home Affairs (LIBE Committee), which is the lead committee with regard to the data protection reform, *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.

[10] European Parliament legislative resolution of 12 Mar. 2014 on the 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, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN

[11] In detail, the Partial General Approaches covered topics such as international data transfers (June 2014), obligations of controllers and processors (October 2014), public sector and specific processing situations (December 2014) and main principles of the processing and the one-stop shop (March 2015).

[12] It is important to explain what is meant by a General Approach. The Council's informal ‘‘General Approach’’ is different from the Council's formal ‘‘position at first reading’’ (pre-Lisbon known as Council's ‘‘Common Position’’), which formally concludes the first reading of the ordinary legislative procedure and is binding. A General Approach is a political agreement on the text by which the Council indicates its informal position. The adoption of a General Approach by the Council forms a basis for informal negotiations (‘‘Trilogue’’) vis-à-vis the Parliament, with the help of the Commission. To respect the ordinary legislative procedure, once the agreement on a joint text will be informally reached between the Parliament and the Council, the joint text will then have to be formally adopted by the Council (‘‘first reading procedure’’). As a final step, the informal joint text will need to be formally adopted also by the Parliament (‘‘second reading procedure’’), after which the Draft Regulation will be finally adopted. For more information on the ordinary legislative procedure, *see* http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers.

topics and articles of the Draft Regulation June 15, under the Latvian Presidency. On July 1, the Luxembourg Presidency will take the lead from the Latvian Presidency for the second half of 2015.

II. Key Elements of the Council's General Approach

A. Modification or Addition of Key Concepts

The Council's text amends some of the key concepts of EU data protection law and introduces new concepts:

- **Concept of personal data.** The Parliament proposed to add to the Commission's text that identifiers such as cookies and Internet protocol addresses constitute personal data, unless they do not relate to an identified or identifiable individual. The Council takes a more flexible approach by adding that identification numbers, location data, online identifiers or other specific factors as such should not be considered as personal data if they do not identify an individual or make an individual identifiable (Recital 24).[13]

- **Pseudonymization, pseudonymous data and encrypted data.** The Parliament introduced new concepts with regard to the definition of personal data that were not included in the Commission's proposal: (1) ''pseudonymous data,'' defined as personal data that ''cannot be attributed to a specific data subject 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. The Parliament's text provided less stringent requirements for the processing of such types of data.

  The Council does not adopt the Parliament's concepts of pseudonymous and encrypted data, but it does add the concept of ''pseudonymization'' to the text. Pseudonymization is defined as ''the processing of personal data in such a way that the data can no longer 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 to an identified or identifiable person'' (Article 4 (3b)). Pseudonymization is considered to be a privacy-enhancing measure and now becomes a quasi-mandatory security measure. The initial intent behind the insertion of the concept of pseudonymization in the Draft Regulation was to provide for some flexibility or lighter obligations for companies, but the Council's version seems to remove this flexibility by providing that, although ''pseudonymization'' reduces the risks of the processing, it is not intended to preclude any other measures of data protection (Recital 23a). This can be considered to be a step backwards compared to the Parliament version.

  However, if companies pseudonymize personal data, they may see their obligations reduced indirectly. For instance, the outcome of a data protection impact assessment will be more positive for the processing of pseudonymized data than for the processing of fully identifiable data. Companies that process pseudonymized data could therefore argue that they need to implement less strict measures to demonstrate compliance with the Regulation (Recital 66a). Furthermore, if proper pseudonymization techniques are used, companies will not be able to identify individuals anymore and should thus benefit from the exemption to comply with an individual's request to exercise his/her rights when the company is not in a position to identify the individual concerned (Article 10—see below).

- **Genetic and biometric data.** The Commission's proposal introduced a definition for a specific category of sensitive data, namely genetic data. This concept was further developed by the Parliament. The Council now defines genetic data as ''all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question'' (Article 4 (10)). The Parliament's definition did not require that such data provide unique information about the physiology or health of an individual and was thus arguably broader than the Council's definition. The Council's text confirms that genetic data are sensitive data. The Council's text allows member states to adopt specific conditions for the processing of genetic or health data (Article 9 (5)). This might lead to a situation where the processing of genetic data will be subject to different regulations under member state law and therefore lead to fragmentation.

  Biometric data remains a defined concept in the text of the Council, covering ''any personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data'' (Article 4 (11)). Although biometric data are not considered to be a type of sensitive data according to the Council, the processing of such data may trigger some specific obligations such as the requirement to conduct data protection impact assessments (Article 33 (2)(b)).

- **Data relating to criminal convictions and offenses.** While the Commission's proposal restricted the processing of data relating to criminal ''convictions,'' the text of the Council also captures criminal ''offences'' (Article 9a). This implies that the processing of data relating to a suspicion of a criminal offense may also be prohibited under the Regulation, which could be highly impractical (e.g., in the case of whistle-blowing hotlines, or the prevention of illegal activities within a corporate group).

[13] All references to articles and recitals relate to the Council's General Approach (text of June 11, 2015).

Non-EU data processors wouldn't be directly subject to the Regulation under the Council's text. Yet, a variety of non-EU based technology companies targeting data subjects in the EU, with or without payment, would be captured by the Draft Regulation.

B. Extraterritorial Effect

- The Commission's proposal gives extraterritorial effect to the Regulation by extending its scope of application to non-EU controllers that offer goods or services to individuals in the EU, or that monitor their behavior. The Parliament's amendments added non-EU processors to the scope of application. The Council limits the extraterritorial scope of the application of the Draft Regulation to non-EU controllers and clarifies that the offering of goods and services does not require a payment from the individuals (Article 3 (2)). Consequently, non-EU processors are not directly subject to the Regulation under the Council's text. Yet, a variety of non-EU based technology companies targeting data subjects in the EU, with or without payment, would be captured by the Draft Regulation. Non-EU controllers, which are subject to EU data protection law, must appoint in writing a representative in the EU (Article 25).

C. Legal Basis for Data Processing

- **Individuals' consent.** The Commission's proposal limits the use of consent as a legal basis for data processing, in particular where there is a significant imbalance between the individual and the controller. In addition, the Commission's proposal requires consent to be ''explicit.'' The Parliament adds further requirements for consent to be valid. The Council removes the requirement that consent must always be explicit (Article 4 (8)). Under the Council's text, consent must only be unambiguous (Article 7 (1)), with a few exceptions for which it must be explicit: sensitive data (Article 7 (1a)) and data transfers (Article 44 (1) (a)). The Council also provides examples of consent that would be acceptable, such as the data subject's conduct in a particular context, or through the data subject's browser setting (Recital 25). This may make it possible to use implied consent in the online context, although the Council also clarifies that silence or inactivity does not constitute consent. Finally, the Council clarifies that when there are various purposes, consent should be given for all purposes (Recital 25) and should include some unbundling requirements for it to be valid (Recital 34).

- **Legitimate interest legal basis.** The Council follows an approach broadly similar to the Commission and the Parliament regarding this legal basis. However, it clarifies that a legitimate interest exists ''when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller'' (Recital 38). The Council also specifies situations where companies should be able to rely on their legitimate interest to process personal data: intra-group communication of data for internal administrative purposes (without prejudice to data transfer restrictions) (Recital 38a); ensuring network and information security; fraud prevention; certain marketing activities (Recital 39); and communicating possible criminal acts or threats to public security to a competent authority (subject to an obligation of secrecy) (Recital 40).

- **Purpose limitation principle.** The purpose limitation principle as articulated in the Council's text is similar to that in the Directive, the Commission's proposal and the Parliament's text. The Council does add a set of criteria to determine whether or not the purpose of further data processing is compatible with the purpose for which the data were initially collected (Article 6 (3a)), which should be useful in practice. The Council also adds a new paragraph that would allow further processing by the same controller for incompatible purposes on the ground of legitimate interests of that controller or a third party, if these interests overrode the interests of the data subjects (Article 6 (4)). This seems to be designed to enable the use of big data applications. It is however very unlikely that this provision will be retained in the final version of the Regulation, as during the June 15 vote, 11 countries in the Council expressed reservations[14] and the Council's Legal Service stated that it considers this provision to be incompatible with Article 8(2) of the Charter of Fundamental Rights of the EU. The Article 29 Working Party (WP29) has also raised concerns regarding this point.[15]

D. Rights of Individuals

- **Notice obligations.** The Commission's proposal contains stricter requirements for privacy policies compared to the existing Directive. The Parliament adds a requirement to complement privacy policies with icons to inform data subjects in a graphical way, and a prohibition to include hidden or disadvantageous clauses in a privacy policy. The Council refers to the possibility to use visualization (Recital 46), but it generally remains closer to the Commission's text and requires many more elements to be included in a privacy policy than are required under the existing Directive, such as references to legitimate interest where relevant, data transfers, the right to withdraw consent and the right to data portability (Article 14).

[14] Belgium, France, Poland, Malta, Italy, Hungary, Austrian, Estonia, Bulgaria, Cyprus and Lithuania.

[15] WP29 issued a statement that it is ''very much concerned'' about this aspect of the Council's proposal. *See* the WP29's press release from March 17 on Chapter II of the draft regulation at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20150317__wp29_press_release_on_on_chapter_ii_of_the_draft_regulation_for_the_march_jha_council.pdf.

- **Right to erasure and to be forgotten.** The right for individuals "to be forgotten," which was explicitly provided in the Commission's proposal and affirmed by the Court of Justice of the EU in its 2014 *Costeja* decision,[16] is renamed and merged by the Parliament with the right to erasure. The Council follows a similar approach. Data controllers must erase personal data without undue delay where: (1) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (2) individuals withdraw their consent for the data processing; (3) individuals object to the processing of personal data; (4) the data were unlawfully processed; and (5) a law requires the controller to erase the data (Article 17). The Council text lists a number of exceptions to this right that are substantially similar to those in the Commission's proposal.

The Council's proposal is more business-friendly than the Parliament's text, which required controllers to actually have the third-party data recipient erase the data.

As concerns data that have been made public by the controller, the Council provides that the controller should take reasonable steps to notify the request for erasure to the controller who received the data (Article 17 and Recital 54). What constitutes "reasonable" steps will depend on the available technology and the cost of implementation. The Council's proposal is more business-friendly than the Parliament's text, which required controllers to actually have the third-party data recipient erase the data.

- **Right to restriction of processing.** Compared to the Parliament, the Council introduces a new right in the Draft Regulation: the right to restriction of processing (Article 17a).[17] This right can actually be somewhat compared to the right to blocking, which is currently included in the Directive, but very rarely applied or enforced in practice.

- **Exceptions to individuals' rights.** Where a controller is not in a position to identify the data subject, the right of access, rectification, erasure and to be forgotten, the right to restriction of processing, the notification obligation regarding rectification, erasure or restriction and the right to data portability do not apply, unless the individual provides additional information enabling his or her identification for exercising his or her rights (Article 10). Controllers are thus not obliged to engage in new or additional data processing to comply with individuals' rights. However, controllers should not refuse to accept additional information provided by an individual in order to support the exercise of his or her rights. In addition, the controller will bear the burden of proof to demonstrate that it is not in a position to identify the individual concerned (Article 12 (1a)). This last provision will be difficult to apply in practice, as it requires controllers to prove a negative.

E. Profiling

The restrictions on profiling introduced by the Commission's proposal are generally followed by the Parliament and the Council. The three institutions seem to agree that profiling activities that lead to measures producing legal effects or significantly affecting the interests, rights and freedoms of individuals[18] are only allowed if they are based on (1) the individual's consent; (2) a member state's law; or (3) a contract with the data subject (and if adequate safeguards are implemented). The Parliament added some flexibility for profiling based on pseudonymous data (where it is impossible for the data controller to attribute the data to a specific individual), which allowed for some leeway concerning online data analytics, but this is not foreseen in the Council's text (Article 20 and Recital 58). However, the Council text clarifies what is processing "significantly affecting the interests, rights and freedoms of individuals" by giving a few examples: "automatic refusal of an on-line credit application or e-recruiting practices without any human intervention" (Recital 58). The Council prohibits profiling activities based on sensitive data unless individuals' explicit consent is obtained, while the Parliament simply prohibits this type of processing activities.

F. Accountability, Data Protection Officer, Data Protection Impact Assessment and Related Principles

- **Risk-based approach.** One of the main novelties of the Council's text is that it introduces a risk-based approach into the Regulation. While the exact implications and concrete applications of the risk-based approach remain uncertain, this arguably provides for flexibility in the new EU data protection legal framework. At a high level, the risk-based approach consists in adjusting some of the data protection obligations to the risks presented by a data processing activity. To conduct that assessment, the nature, scope, context and purpose of the processing should be taken into account, as

[16] CJEU Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* (May 13, 2014), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131 (13 PVLR 857, 5/19/14).

[17] Methods to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system or making the selected data unavailable to users or temporarily removing published data from a website. In automated filing systems the restriction of the processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted (Recital 54a).

[18] Such processing also includes "profiling" consisting in any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyze or predict aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements as long as it produces legal effects concerning him or her or significantly affects him or her (Recital 58).

well as the likelihood and severity of the risks for the rights and freedoms of individuals posed by the processing. A two-level risk approach is used (i.e., ''risk'' or ''high risk''). High risk is defined as a ''particular risk of prejudice to the rights and freedoms of individuals'' (Recital 60b). The obligations that are relevant for high-risk processing include: (1) when to conduct a data protection impact assessment (Article 33); (2) when to notify data breaches (Article 31, 32); and (3) when to launch a prior consultation with DPAs (Article 34). The risk-based approach also appears in various other articles of the Regulation, including in the provisions on privacy by design and by default, appointment of a representative in the EU by a non-EU controller, documentation requirements, data protection officer (DPO) and security requirements.

- **Data protection impact assessments and DPA consultation.** The Commission's proposal obliged controllers and processors to carry out a data protection impact assessment before conducting high-risk data processing operations. The Parliament added a requirement to first perform a risk analysis after which, in certain situations, controllers and processors would have to conduct a data protection impact assessment. The Council does not maintain the risk analysis obligation but further develops the requirement to carry out a data protection impact assessment for processing that presents a high risk. However, the Council limits this obligation only to controllers. In addition, the Council requires conducting a data protection impact assessment for profiling activities, the processing of sensitive data, biometric data and data relating to criminal convictions or offenses. The Council proposes that data protection authorities (DPAs) establish a list of types of processing operations that are and/or are not subject to the requirement for a data protection impact assessment (Article 33 (2a) and (2b)). In the event the data protection impact assessment indicates that the risk of the processing is high, and the controller does not (or cannot) take measures to mitigate the risk, the controller should consult a DPA prior to the processing (Article 34 (2)), which will have to reply in writing within a maximum period of six weeks. These provisions are rather confusing, and it is unclear in which situations exactly a data protection impact assessment and consultation with the DPA would be required.[19]

- **Internal documentation.** The Commission's proposal replaced the current requirement to register data processing activities with the national DPA with a requirement to put in place internal privacy documentation. The Parliament proposed to add a mandatory biannual review and update of such compliance policies and procedures. The Council does not adopt this amendment and takes a more lenient approach towards compliance documentation. For instance, it mandates the implementation of measures that demonstrate compliance taking into account the risk-based approach. The Council also provides that approved codes of conduct and certification mechanisms may be used as elements to demonstrate compliance (Article 22).

- **Data protection officer.** The Commission's proposal mandated the appointment of a DPO for companies employing 250 persons or more. The Parliament's text imposed this requirement to companies that carry out data processing activities that affect more than 5,000 individuals in a consecutive 12-month period. The Council abolishes the mandatory requirement to appoint a DPO, makes it optional and leaves it to the member states to impose this obligation via national law (Article 35). This is a step backward as companies could face different legal thresholds and requirements for the appointment of DPOs in the EU, which could lead to fragmentation and undermine the status of DPOs.

- **Codes of conduct.** The Commission's proposal envisaged the possibility for associations and other bodies representing controllers or processors to draw up codes of conduct for compliance with the Regulation. The Parliament and the Council have taken over this option with some variations. The Council includes a possibility for DPAs to approve codes of conducts that do not relate to processing activities in several member states (Article 38 (2a)). However, codes of conduct relating to processing activities in several member states should be submitted to 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, or EDPB) via the consistency mechanism (Article 38 (2b)), and, in the case of a positive EDPB opinion, to the Commission for approval. Accredited bodies will monitor compliance with codes of conduct (Article 38a). The accreditation would be two-fold: The DPA drafts the criteria for accreditation and then submits it to the EDPB under the consistency mechanism (Article 38a (3)). Codes of conduct are definitely an interesting development as they would provide a co-regulatory regime in the EU. One of the key additions of the Council is that codes of conduct are considered a valid mechanism for data transfers (Article 38 (1ab)).

- **Certification, seals and marks.** The Council elaborates on the possibility, introduced by the Commission, to establish data protection certification mechanisms. These mechanisms are intended to demonstrate compliance with the Regulation, while codes of conduct contribute to the proper application of the Regulation. Independent certification bodies will certify companies and monitor proper compliance with the certification. Certifications are issued for a maximum period of three years with a possibility of renewal (Article 39 (4)). Certification bodies must be accredited by either the DPA or the National Accreditation Body (Article 39a). As for codes of conduct, certification, seals and marks are now recognized as a valid mechanism for data transfers (Article 39 (1a)).

[19] The text is unclear and contradictory, as Article 34 (2) requires consulting the DPA when the processing would result in a high risk ''*in the absence of measures*'' to be taken by the controller to mitigate the risk, while Recital 74 provides that the controller should consult the DPA when the processing would result in a high risk ''*despite the envisaged safeguards, security measures and mechanisms*'' to mitigate the risk.

The Council's text provides for a 72-hour deadline after having become aware of a breach for notifying DPAs, where feasible, and notification to the affected individuals without undue delay.

G. Data Security

- **Security requirements.** Data controllers and processors have an obligation to implement appropriate technical and organizational measures, such as pseudonymization of personal data, to ensure a level of security appropriate to the security risks presented by the data processing. Such measures must take into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals (Article 30).

- **Breach notification.** The Commission's proposal introduced an obligation to notify DPAs and individuals of data security breaches. The Commission's 24-hour deadline for notifying DPAs was replaced by the Parliament with a duty to notify ''without undue delay.'' The Council's text provides for a 72-hour deadline after having become aware of a breach, where feasible, and notification to the affected individuals without undue delay. The Council limits notification to both DPAs and individuals to breaches that are likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage (Article 31). The Council's text also provides for a number of exceptions for notification to individuals, such as the use of encryption or the implementation of mitigating measures, (Article 32 (3)), which considerably reduces the number of instances where breach notification to individuals will be required.

H. Roles and Responsibilities of Parties

- **Joint controllers.** The Commission's proposal required joint controllers to determine their respective responsibilities under the Draft Regulation by means of an arrangement between them. The Parliament specified that such arrangement should duly reflect the roles and relationships vis-à-vis individuals and that the essence of such arrangements be made available to individuals. The Council substantially takes over the Parliament's amendment, but adds an obligation for joint controllers to determine how they will comply with the notice obligation. The Council also adds that the arrangement should designate which of the joint controllers acts as single point of contact for data subjects to exercise their rights. If the data subject has been properly informed of which joint controller is responsible, the data subject should exercise his/her rights with that controller (Article 24). Absent such information, it can exercise its rights with any of the data controllers. Another key aspect of the Council's text is that it removes the joint and several liability between joint controllers provided by the Parliament's text.

- **Processing and sub-processing.** The Council adds a number of obligations on processors. In particular, the data processing agreement between the controller and the processor must include an obligation for the processor to allow for and contribute to audits conducted by the controller, an obligation to inform the controller of a legal requirement that may impede it to comply with the controller's instructions and a commitment to respect the controller's conditions for enlisting subprocessors. Notably, processors are prohibited from outsourcing sub-processing to third parties except with the general or specific authorization of the controller. If the controller gives a general authorization, the processor must inform the controller of its intent to use a sub-processor, and the controller must have the opportunity to object to the sub-processing. In addition, the contract between the processor and the sub-processor must include similar obligations as those between the controller and the processor. Finally, the initial processor must stay liable vis-à-vis the controller for the performance of the sub-processor's obligations (Article 26). These requirements on subprocessing are similar to the sub-processing requirements provided in the European Commission's 2010 Controller-to-Processor Standard Contractual Clauses, or under binding corporate rules (BCRs), for sub-processing that involves an international transfer of personal data. These strict sub-processing rules, which are difficult to comply with in practice, would thus become mandatory for sub-processing activities within the EU as well. Interestingly, the Council's text allows for the creation of model contracts for data processing agreements (Article 26 (2ab)).

I. International Data Transfers

- **Adequacy decisions.** The Council adds a number of criteria that the Commission must take into account when assessing the level of protection of a country or sector, including the rules for onward transfers, the existence of effective and enforceable rights for individuals and the existence of an independent authority that is responsible for ensuring and enforcing compliance with data protection rules (Article 41 2(a) and 2(b)). In addition, the Council text requires that the Commission take into account the third country's general and sectoral law, including laws relating to public security, defense and national security, as well as public order and criminal law (Recital 81).

- **Withdrawal of sunset clause for adequacy decisions and authorizations.** The Council's text allows for an easier transition from the existing Directive to the Regulation as concerns Commission adequacy decisions and authorizations for international data transfers. The Parliament had included a sunset clause of five years for the Commission to renew its adequacy decisions after the Regulation comes into force. This sunset clause has disappeared in the Council's text. The Commission is responsible for monitoring the functioning of such decisions and may, where necessary, repeal, amend or suspend such decision without retroactive effect. The Parliament had also added a sunset clause for data transfer authorizations based on Article 26(2) of the current Directive, 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. This is also withdrawn from the Council's text (Article 41 (4a) and Article 42 (5b)).

- **Safe Harbor.** The Council's text does not explicitly deal with the EU-U.S. Safe Harbor Framework. The Safe Harbor would remain valid until amended or replaced. However, the text does indirectly intend to regulate self-regulatory frameworks, such as the Safe Harbor (given that Safe Harbor is based on a sectoral adequacy decision), by adding (stricter) criteria that the European Commission should take into account when assessing whether a country (or a sector within a country) provides an adequate level of data protection in the future (Recital 81).

- **Binding corporate rules (BCRs).** The Council specifies that the controller or the processor can adduce appropriate safeguards for data transfers, which includes BCRs. This removes the concern that was created by the Parliament's amendments, which removed the reference to BCRs for processors from the Commission's text but kept the reference to BCRs for controllers. In addition, the Council's text refers to BCRs for a ''group of undertakings or group of enterprises engaged in a joint economic activity'' (Article 43 (1) (a)). This new text also opens the door to BCRs for companies that are not part of the same group but engaged in a joint economic activity. One point to note is that the Council's text now includes the obligation to report to the DPA any legal requirements that may conflict or affect the guarantees provided by the BCRs (Article 43 (2) (l)).

- **Standard contractual clauses.** The Council explicitly provides for the use of clauses adopted by the Commission, contrary to the Parliament's text that seemed to allow only clauses adopted through the consistency mechanism (see below) (Article 42 (2) (b) and (c)).

- **New data transfer mechanisms.** The Council's text introduces two new important grounds for international data transfers: adherence to a code of conduct or to a certification mechanism. Both mechanisms need to consist of binding and enforceable commitments from the controller or processor in the third country to apply the appropriate safeguards and must include a third-party beneficiary right for individuals or its equivalent (Article 42 (2) (d) and (e)).

- **Derogations.** The Council text keeps the derogation from the prohibition on international data transfers for transfers based on the legitimate interest of the data controllers, which was also included in the Commission's proposal. This derogation was deleted from the Parliament's text. The Council, however, adds two conditions. This derogation is only available for transfers that are not large scale or frequent and if the controller's interests are not overridden by the interests or rights and freedom of individuals.

- **Foreign law enforcement requests.** The Parliament's amendment that would require companies 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 in the Parliament's version), is not included in the Council's text. The Parliament's amendment would have been highly problematic for companies facing conflicting legal obligations.

- **Transfer restrictions for reasons of national public interest.** The Council's text introduces a provision according to which member states can ''set limits'' to the transfer of certain types of data based on ''important reasons of public interest.'' If member states enact such laws, they must notify them to the Commission (Article 44 (5a)). However, member states can only use this provision ''in the absence of an adequacy decision,'' thus limiting the impact on countries that have been considered to provide an adequate level of protection and the EU-U.S. Safe Harbor Framework.

J. One-Stop Shop, Cooperation Procedure and the Consistency Mechanism

- **Main establishment.** The concept of ''main establishment'' is important for determining which DPA is competent for a company's data processing activities in the EU (the ''one-stop shop mechanism,'' see below). The Commission's proposal provided different criteria for determining the main establishment of the controller (i.e., place of main decisions) and the processor (i.e., place of central administration). The Parliament suggested harmonizing the concept for both controllers and processors, taking as the decisive criterion (for both controllers and processors) the location where the main decisions are taken with regard to the conditions and means of the processing. The Council proposes that the main establishment for both controllers and processors should be the place of their *central administration in the EU* (Article 4 (13)). The Council provides the following exceptions to this rule:

- *Controllers*: If decisions on the purposes and means of the data processing are taken in another establishment of the controller in the EU, which has the power to have such decisions implemented, then that other establishment will be the main establishment.

- *Processors*: If the processor has no central administration in the EU, the main establishment will be the location in the EU where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the Regulation.

- **One-stop shop.** The Commission proposed that companies doing business in multiple EU member states would only be subject to the jurisdiction of the DPA of the EU member state in which it has its main establishment. The Parliament added to this principle that such a ''lead DPA'' would still need to cooperate with other DPAs and that individuals would be able to lodge a complaint before the DPA of their home jurisdiction. The Council follows an approach similar to the Parliament but weakens the one-stop shop mechanism by, among other things, giving the DPAs of all member states concerned the right to intervene in the decision-making process and by opening the door to complaints, investigations and litigation in every member state. For companies doing business in multiple EU member states, this is a setback compared to the Commission's proposal.

  The situation under the Council's text is complex (Articles 51, 51a, 54a). The general principle is that the lead DPA (i.e., the DPA of the main establishment) is competent for transnational matters. The lead DPA has the power to request mutual assistance from local DPAs and initiate joint operations with them. However, each DPA stays competent to hear local complaints or local violations of the Regulation if the violation or the complaint only relates to an establishment in its member state or substantially affects data subjects only in its member state. In that situation, the local DPA must inform the lead DPA without delay. Within three weeks, the lead DPA decides whether or not it will deal with the case. In case the lead supervisory authority decides not to deal with it, the local DPA deals with the matter. If the lead DPA decides to deal with the case, the cooperation procedure will apply. In that context, the local DPA may submit a draft decision to the lead DPA, which must take utmost account of it. In case of disagreement, the consistency mechanism applies.

  In all other matters, the lead DPA must, without delay and before taking a decision, communicate all relevant information on the matter and a draft decision to the other DPAs (i.e., concerned DPAs). Each local DPA has the right to give its opinion. If within four weeks any of the local DPAs expresses a relevant and reasoned objection to the draft decision and if the lead DPA does not follow the objection (or is of the opinion that the objection is not relevant and reasoned), it must submit the matter to the consistency mechanism. If the lead DPA intends to follow the objection made, it must submit to the other DPAs a revised draft decision for their opinion. If none of the other DPAs has objected to the draft decision submitted by the lead DPA, the lead and local DPAs are considered to be in agreement and are bound by it.

  Once a decision is reached, the lead DPA must adopt and notify it to the main establishment or single establishment of the controller or processor and inform the other DPA and the EDPB of the decision, including a facts and grounds summary. The local DPA to which the complaint has been lodged must inform the complainant on the decision. If the complaint is dismissed or rejected, the local DPA must adopt the decision and notify it to the complainant and inform the controller. This allows the controller or the processor, as well as the complainant, to challenge the decision in court when an unfavorable decision is adopted against them. The Regulation also provides for the possibility to dismiss or reject part of a complaint and to act on other parts of the complaint. In that situation, a separate decision will be adopted for each part of the matter. The lead DPA will adopt the decision for the part that must be enforced against the controller or processor and notify it to the main establishment, and inform the complainant, while the DPA of the complainant will adopt the decision for the dismissal or rejection and notify it to the complainant, and inform the controller or processor.

- **Consistency mechanism.** Both the Council and the Parliament propose amendments that turn the EDPB into an appellate body, which can take legally binding decisions in case of disagreement between DPAs about a matter or on the determination of the lead DPA (Article 57 (3)). According to the Council, the EDPB can take binding decisions in three cases: (1) if there is disagreement between DPAs with regard to a draft decision (e.g., a local DPA objected to a draft decision of the lead DPA); (2) if there is disagreement between DPAs with regard to what DPA is competent for the main establishment; and (3) if a DPA does not request an opinion to the EDPB while this is required by the Regulation, or when a DPA does not follow an EDPB opinion. In addition, the EDPB can issue nonbinding opinions in a variety of matters: data protection impact assessments, code of conduct, certification, standard contractual clauses, ad hoc contract or BCRs (Article 57 (2)). Furthermore, any DPA, the chair of the EDPB or the Commission may request that any matter of general application or that produces effects in more than one member state be examined by the EDPB with a view to obtaining an opinion, in particular where a DPA does not comply with the obligations for mutual or joint operations (Article 57 (4)). EDPB opinions are generally adopted at the majority, while legal binding decisions are adopted by a majority of two-third. Granting the EDPB binding legal powers raises a host of questions that cannot be gone into here, but that will likely lead to increasing controversy.

K. Sanctions and Fines

- The Commission's proposal provided for administrative fines for data protection violations of up to two percent of a company's annual worldwide turnover or up to 1 million euros ($1.12 million) (whichever is greater). The Parliament increased the level of fines to up to 100 million euros ($112 million), or up to five percent of a company's annual worldwide turnover, but the Council returns to the maximum fine provided in the Commission's proposal (i.e., up to two percent of a company's annual worldwide turnover) (Article 79a (3)).

L. Other Aspects

- **Employment context.** The Commission allowed member states to enact local laws to regulate the employment sector. Many commentators have criticized this as leading to fragmentation of the internal market and undermining the objective of harmonization. The Parliament added some minimum standards for data processing in the employment context that must be respected in all member states, but these were not taken over by the Council (Article 82).

Next Steps and Outlook

The European Union has made significant progress toward the adoption of a new EU data protection framework. Now that both the Parliament and the Council have adopted their own text concerning the Commission's proposed text, the three EU institutions can start their final negotiations, which should lead, ultimately, to the adoption of the Regulation. There is momentum now on which the EU institutions should build to reach a final agreement.

However, while there is broad agreement between the EU institutions on many of the key principles, the exact wording of the final text of the Regulation still remains unclear and will have to be agreed on as the result of a compromise via the Trilogue meetings.

The Trilogue phase will consist of informal meetings between the three institutions with a view to reaching an agreement. The procedure for the Trilogue is highly untransparent, so that it will be difficult for stakeholders to know what happens during this final stage of the legislative process. At the time this article was being finalized, a timetable published on the website of the Group of the European People's Party in the European Parliament[20] was indicating that the Trilogue meetings would start June 24 with an aim to reaching an agreement by December 2015. The Trilogue will be led by the Luxembourg Presidency and, if no agreement is reached by the end of 2016, by the Dutch Presidency. Both countries have substantial experience in handling European matters, which allows for some optimism.

It now seems reasonable to believe that a final text of the Draft Regulation could be agreed on by the end of 2015, or during the spring of 2016.

The main challenge of the Trilogue will be to reconcile diverging or opposing views. The Parliament is seen as the most privacy-oriented institution in the EU, while the Council is often quite business-friendly. The text that results from these negotiations is often the outcome of intense negotiations and the result of significant trade-offs. It sometimes produces compromises that are difficult to apply or interpret in practice. It thus remains to be seen how the EU institutions will manage to reach an agreement and what the final text of the Regulation will look like.

So far, all predictions have failed, but it now seems reasonable to believe that a final text of the Draft Regulation could be agreed on by the end of 2015, or during the spring of 2016. The Draft Regulation will enter into force two years after its adoption, which means—at the earliest—the end of 2017 or the spring of 2018.

As is always the case, the devil is in the details, but it now seems likely that the Regulation could be adopted within the foreseeable future and that its core principles will become law. Companies doing business in the EU or targeting EU individuals should start planning for the new EU data protection framework and assess how these new core principles will affect their business.

[20] The timetable is *available at* http://www.eppgroup.eu/news/Data-protection-reform-timetable.