Bloomberg BNA

Privacy and Security Law Report®

EU Regulation

In what is the most important European Union data protection legislation in a generation, the European Council, European Parliament and European Commission reached agreement on the text of a new data protection regulation that is likely to influence data protection law around the world over the next 20 years, the authors write.

The Final European Union General Data Protection Regulation

By Cedric Burton, Laura De Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot and Sára G. Hoffman

It has been four years[1] since the European Commission proposed its reform to the European Union (EU) legal data protection framework.[2] On Dec. 18, 2015, the Permanent Representatives Committee (Coreper) of the Council confirmed that the compromise texts on the legislative package had been agreed with the European Parliament. The agreement between the Council, European Parliament and European Com-

Cedric Burton is of counsel for Wilson Sonsini Goodrich & Rosati in Brussels.

Laura De Boel is senior associate for Wilson Sonsini Goodrich & Rosati in Brussels.

Christopher Kuner is senior privacy counsel for Wilson Sonsini Goodrich & Rosati in Brussels.

Anna Pateraki is senior associate for Wilson Sonsini Goodrich & Rosati in Brussels.

Sarah Cadiot is an associate at Wilson Sonsini Goodrich & Rosati in Brussels.

Sára G. Hoffman is an associate at Wilson Sonsini Goodrich & Rosati in Brussels.

The authors are grateful to Anna Ciesielska, legal intern in the firm's Brussels office, for her excellent research assistance.

[1] See our past detailed analyses of the progress of the proposed GDPR: Cédric Burton, Christopher Kuner and Anna Pateraki, The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report, Bloomberg BNA Privacy & Sec. L. Rep. (Jan. 21, 2013), *available at* https://www.wsgr.com/eudataregulation/pdf/011713.pdf (12 PVLR 99, 1/21/13); Cédric Burton and Anna Pateraki, Status of the Proposed EU Data Protection Regulation: Where Do We Stand?, Bloomberg BNA Privacy & Sec. L. Rep. (Sept. 2, 2013), *available at* https://www.wsgr.com/publications/PDFSearch/burton-090213.pdf (12 PVLR 1470, 9/2/13); 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); and Cédric Burton, Laura De Boel, Christopher Kuner and Anna Pateraki, The Proposed EU Data Protection Regulation Three Years Later: The Council Position, Bloomberg BNA Privacy & Sec. L. Rep. (June 29, 2015), *available at* https://www.wsgr.com/eudataregulation/pdf/BNA-0615.pdf (14 PVLR 1164, 6/29/15).

[2] 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 (GDPR), 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 data, COM (2012) 10 final, *available at* http://src.bna.com/b55; this article will only deal with the GDPR.

 ISSN 1538-3423

mission was reached on Dec. 15, 2015.[3] This was the last major step in the adoption process of the EU General Data Protection Regulation (GDPR).[4]

The GDPR was originally based on a proposal issued by the European Commission (Commission) in 2012.[5] The European Parliament (Parliament) approved its own version in 2014.[6] After the Council had also adopted its version (known as ''General Approach'')[7] in June 2015, the EU institutions were ready to enter the final stage of the legislative process. Known as the ''Trilogue'', this final step is a negotiation between representatives of the Council, the Commission and the Parliament, in which the three institutions aimed to reach an agreement on the text of the GDPR. That agreement has now been reached.

The text of the GDPR may still undergo some last changes as it is now being finalized by the EU's legal services. The importance of these changes is not to be underestimated, as any change to the wording of such a complex instrument as the GDPR can be significant (note that the numbering of the provisions will also change). However, the version of the GDPR agreed on Dec. 15, 2015, can be regarded as very close to the final text, and it is this version that we will analyze in this article.

Political Agreement on a Compromise Text: Key Elements, Analysis, and Takeaways

The latest version of the GDPR is a compromise text encompassing 204 pages that will replace the current EU Data Protection Directive 95/46/EC (Data Protection Directive).[8] The following analysis covers some of the main topics of interest to the private sector, and explains how the GDPR will govern key aspects of privacy and data protection law in the future.

I. General Remarks

1. *The Parliament and Council Versions: Who Prevailed?*

Since the first draft of the GDPR was proposed by the Commission in Jan. 2012 to replace the Data Protection Directive, both the Parliament and the Council approved their own versions. The Parliament issued its first draft report on the proposal in early 2013, the text of which was heavily debated in Parliament and triggered many comments from stakeholders. After lengthy debates in different committees, the Parliament adopted its amendments to the Commission's proposal on March 12, 2014.

The GDPR introduces a new concept that does not exist under the Data Protection Directive, namely, pseudonymization.

In parallel with 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 was spread over the Presidency of various Member States.[9] During this period, the Council reached non-binding political agreements at the Justice and Home Affairs (JHA) ministers level on certain topics (known as ''Partial General Approach'').[10] After lengthy debates, the Council finally reached a General Approach[11] covering amendments in relation to all topics and articles of the GDPR on June 15, 2015.

The Council and Parliament had diverging views on several key topics in the GDPR. A compromise was reached during the Trilogue negotiations, with some

[3] *See* Council's press release of Dec. 18, 2015, *available at* http://src.bna.com/b54.

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

[5] *Supra* Fn. 2 and 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), *available at* https://www.wsgr.com/eudataregulation/pdf/kuner-020612.pdf (11 PVLR 215, 2/6/12).

[6] See the European Parliament legislative resolution of March 12, 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://src.bna.com/b6c; Cédric Burton, Christopher Kuner 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)

[7] *See* Council document no. 9565/15 at http://src.bna.com/b6d.

[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, 23.11.1995, p. 31–50, *available at* http://src.bna.com/b6r.

[9] This includes 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), the Latvian Presidency (first half of 2015) and the Luxembourg Presidency (second half of 2015).

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

[11] 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. In the ordinary legislative procedure, once the agreement on a joint text is 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 GDPR will be finally adopted. For more information on the ordinary legislative procedure, see http://src.bna.com/b6z.

  PVLR ISSN 1538-3423

provisions drafted closer to the position of either the Parliament or the Council.[12]

2. *The Court of Justice of the European Union: Influences on the Legislative Process*

Between the Commission's proposal for a comprehensive data protection package issued on Jan. 25, 2012, and the compromise GDPR text of Dec. 15, 2015, the Court of Justice of the European Union (CJEU) issued several landmark data protection judgments that substantially influenced the GDPR's legislative process.

The controversial purpose limitation principle as included in the final text of the GDPR entails that personal data collected for a specific purpose can only be further processed for a purpose compatible with the purpose of collection, except where the processing of personal data is based on the individual's consent or a legal requirement to process data for further purposes.

Most notably, the CJEU's *Schrems* decision[13] invalidated the EU-U.S. Safe Harbor framework (Safe Harbor) as a data transfer mechanism between the EU and the U.S. The CJEU judgment was delivered shortly before the compromise GDPR text was reached, giving the Council, Parliament and Commission time and opportunity to consider the impact of *Schrems* on the GDPR's data transfer mechanisms.[14]

During the legislative process, the CJEU also issued judgments that highlighted the current fragmentation of data protection laws within the EU internal market. In *Weltimmo*[15], the CJEU clarified the territorial scope of application of national data protection laws in a bilateral enforcement conflict.[16] In 2014, the CJEU ruled two landmark cases regarding individuals' rights which have had a lot of public exposure and influenced legislators and advocacy groups during the negotiations on the GDPR. The CJEU invalidated the Data Retention Directive[17] in *Digital Rights Ireland*[18] as it considered that the data retention obligations under this directive created serious interferences with the fundamental rights to privacy and data protection, without that interference being limited to what is strictly necessary. A month later, the CJEU upheld in *Costeja*[19] that individuals have a right under the Data Protection Directive to be 'forgotten' i.e., to have their personal data erased.

II. Key elements of the Compromise Text

1. *Modification or Addition of Key Concepts*

The GDPR amends some of the key concepts of EU data protection law currently contained in the Data Protection Directive and introduces new concepts:

- **Concept of personal data.** The GDPR broadly maintains the definition of personal data provided by the Data Protection Directive (i.e., personal data means any information relating to an identified or identifiable natural person or 'data subject'), but added to that definition are examples of identifiers such as location data or online identifiers (Article 4 (1)). The GDPR further specifies that online identifiers, provided by devices, applications, tools and protocols, including Internet Protocol (IP) addresses, cookie identifiers, as well as other identifiers such as Radio Frequency Identification tags (RFID), could be used to identify individuals, in particular when combined with unique identifiers (Recital 24).

  The Parliament proposed to explicitly state in the GDPR that identifiers, such as cookies and IP addresses, constitute personal data, unless they do not relate to an identified or identifiable individual. The Council took a more flexible approach by adding that data such as identification numbers, location data, online identifiers or other specific factors may identify an individual, but not necessarily.

- **Pseudonymization, pseudonymous data and encrypted data.** The GDPR introduces a new concept that does not exist under the Data Protection Di-

[12] On the one hand, the inclusion of non-EU processors to the scope of application of the GDPR (Article 3 (2)) and of biometric data as a special category of sensitive data (Article 9) and the use of standardized icons to inform individuals about the data processing activities (Article 12 (4b) and (4c)) were legislative efforts by the Parliament. On the other hand, it was mainly the Council's effort to include a definition of genetic data (Article 4 (10)), limit the processing of data relating to criminal convictions and offences (Article 9a), and determine the situations where the appointment of a data protection officer is mandatory (Article 35). Aside from a select few ''champion'' topics, the GDPR is a compromise text that incorporates elements of both the Council's and Parliament's efforts. We have discussed the respective input of the legislative bodies wherever possible in our analysis below.

[13] CJEU Judgment, delivered on Oct. 6, 2015, in Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (request for a preliminary ruling from the High Court (Ireland)), *available at* http://src.bna.com/b6B.

[14] For a detailed analysis, see ''WSGR Client Alert EU's Highest Court Declares Safe Harbor Invalid'', Oct. 6, 2015, *available at*: http://src.bna.com/b6C.

[15] CJEU Judgment, delivered on Oct. 1, 2015, in Case 230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, *available at* http://src.bna.com/b6E.

[16] See our analysis ''Landmark Decision Clarifies Territorial Scope of Application of National Data Protection Laws in the EU,'' WSGR Data Advisor, Nov. 2015, *available at*: https://www.wsgr.com/publications/PDFSearch/the-data-advisor/Nov2015/.

[17] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54-63, *available at* http://src.bna.com/b6H.

[18] CJEU Judgment, delivered on April 8, 2014, in Case C-293/12 *Digital Rights Ireland and Seitlinger and Others*, *available at* http://src.bna.com/b6J.

[19] CJEU Judgment, delivered on May 13, 2014, in Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, *available at* http://src.bna.com/b6K.

rective, namely, pseudonymization. Pseudonymization is 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 information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person'' (Article 4 (3b)). In practice, pseudonymization refers to privacy-enhancing measures that aim to reduce the risk of singling out one individual in a data pool. It is also a tool for compliance, helping data controllers and processors meet their data protection obligations (Recital 23a).

The initial intent behind the insertion of the concept of pseudonymization in the GDPR was to provide for some flexibility for companies. However, the final text of the GDPR 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). In addition, the GDPR explicitly states that pseudonymous data that could be attributed to an individual by the use of additional information should be considered personal data (Recital 23). However, if companies pseudonymize personal data, they may see some of their obligations reduced indirectly. For instance, the outcome of a privacy impact assessment is likely to be more positive for the processing of pseudonymized data than for the processing of fully identifiable data.

The Parliament's proposal for considering encrypted data as a separate category of personal data did not make it into the final version of the GDPR. The Parliament's proposal defined encrypted data as ''personal data, which through technological protection measures is rendered unintelligible to any person who is not authorised to access it''.

- **Genetic and biometric data.** The GDPR introduces definitions for specific categories of sensitive data, namely genetic data and biometric data. Genetic data are defined 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 GDPR clarifies that genetic data uniquely identifying an individual is considered to be sensitive data.

  The GDPR also introduces the concept of biometric data, meaning ''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)). Similar to genetic data, biometric data is considered a type of sensitive data when such data uniquely identifies an individual (Article 9 (1)). Photographs will be considered to be biometric data when they are processed through a technical means allowing the unique identification or authentication of an individual (Recital 41). The processing on a large scale of special categories of data, including genetic and biometric data, may trigger some specific obligations such as the requirement to conduct a data protection impact assessment (Article 33 (2) (b)).

  The GDPR allows Member States to adopt further conditions, including limitations, for the processing of genetic data, biometric data or health data (Article 9 (5)). This might lead to a situation where the processing of such data in different Member States will be subject to different national laws, resulting in fragmentation. The GDPR mitigates this risk to a certain extent by stating that Member State laws regulating these types of data should not hinder the free-flow of data within the EU (Recital 42a).

- **Data relating to criminal convictions and offences.** Similar to the current regime, the GDPR provides that processing of personal data relating to criminal convictions and offences or related security measures may only be carried out under the control of official authority. Alternatively, EU or Member State law may authorize such processing provided that adequate safeguards are in place (Article 9a). A comprehensive register of criminal convictions must be kept under the control of official authority only (i.e., a public or governmental authority).

The GDPR also emphasizes that consent must be freely given, requiring that utmost account be taken of whether the processing of data was made conditional on the individual's consent.

2. *Extraterritorial Effect*

The GDPR has extraterritorial effect by extending its scope of application to non-EU controllers or processors, where the processing activities are related to: (a) the offering of goods or services to individuals located in the EU; or (b) the monitoring of their behavior (Article 3). Non-EU controllers and processors that are subject to EU data protection law must appoint in writing a representative in the EU (Article 25). The GDPR clarifies that the concept of 'offering goods or services' is not limited to offerings that require a payment from the individuals. The GDPR further clarifies that:

(a) To determine whether a controller or processor is offering goods or services to individuals located in the EU, it should be assessed whether it is apparent that the controller aims for its products or services to be offered to individuals in one or more Member States in the EU. A number of factors can help in completing this assessment, including the use of a language or currency that is common in one or more Member States with the possibility of ordering goods and services in that language. However, the mere accessibility of the controller's or an intermediary's website in the

  PVLR ISSN 1538-3423

EU or of an e-mail address and other contact details or the use of a language generally used in the third country where the controller is established, is insufficient as such to trigger the applicability of the GDPR (Recital 20).

(b) To determine whether individuals' behavior is being monitored, it should be assessed whether individuals are tracked on the Internet including subsequent profiling, in particular to take decisions regarding individuals for analyzing or predicting their personal preferences, behaviors and attitudes (Recital 21).

The right for individuals 'to be forgotten', which was explicitly provided in the Commission's proposal and affirmed by the European Court of Justice, was renamed and merged by the Parliament with the right to erasure.

3. *Legal Basis for Data Processing*

- **Individual's consent.** The GDPR defines consent as ''any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed'' (Article 4 (8)). The definition is broadly similar to the concept of 'consent' under the current Data Protection Directive. The GDPR also emphasizes that consent must be freely given, requiring that utmost account be taken of whether the processing of data was made conditional on the individual's consent (Article 7 (4)). Consent can be an oral statement or written, including in electronic form. Pre-ticked boxes on an internet website or mere silence or inactivity do not constitute valid consent (Recital 25).

  The issue of consent has been one of the most hotly debated issues of the GDPR. Originally, the Commission's proposal required consent to be ''explicit''. The Parliament added additional requirements for consent to be valid. The Council asked solely for unambiguous consent as a general rule and explicit consent in select cases, removing the requirement that consent must always be explicit. This latter approach is followed in the GDPR compromise text.

  The GDPR stipulates that controllers bear the burden of proof that consent was actually given by individuals (Article 7 (1)). If individuals' consent is obtained in the context of a written declaration which also concerns other matters (e.g., a subscription order which includes various terms and conditions, and also asks for individuals' consent to data processing), the request for consent must be clearly distinguishable from the other matters and presented in plain and easily accessible language (Article 7 (2)). This will force companies to review their consent forms and to include specific sections on data protection. Individuals may withdraw consent at any time (Article 7 (3)).

- **Consent from children.** The GDPR introduces new conditions for children's consent to the processing of their personal data in relation to information society services. When processing personal data of a child, the controller must obtain the parent's consent. Without parental consent or authorization by the holder of parental responsibility, the data processing activity is not lawful (Article 8 (1)). The GDPR sets the age of 16 as the maximum age for parental consent, but Member State law may set a lower age limit provided that it is not below the age of 13. This matter is thus partially left to the EU Member States. The controller must take reasonable efforts and use available technology to verify that consent has been obtained in the prescribed fashion (Article 8 (1a)).

- **Legitimate interest legal basis.** The GDPR keeps the legitimate interest legal basis with some limitations and clarifications. A novelty is that the reasonable expectations of individuals should be taken into account when assessing whether companies can rely on this legal basis. A legitimate interest for data processing exists ''when there is a relevant and appropriate connection between the individual and the controller in situations such as the individual being a client or in the service of the controller,'' fraud prevention and certain marketing activities (Recital 38). Also, companies should be able to rely on their legitimate interest to process personal data, for example for intra-group data disclosures for internal administrative purposes (without prejudice to data transfer restrictions) (Recital 38a); ensuring network and information security (Recital 39); fraud prevention (Recital 38); 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 principal of purpose limitation was a controversial element throughout the legislative process. The purpose limitation principle as included in the final text of the GDPR entails that personal data collected for a specific purpose can only be further processed for a purpose compatible with the purpose of collection, except where the processing of personal data is based on the individual's consent (i.e., a new valid consent allows processing personal data for a new purpose) or a legal requirement to process data for further purposes. The GDPR also provides that the controller must ascertain whether the processing for another purpose is compatible with the purpose of the data collection.

  The GDPR lists a number of elements to take into account for that assessment (i.e., the link between the purpose of collection and further processing, the context and relationship between the controller and the individual including the individual's reasonable expectations, the nature of the data and whether or not they constitute sensitive data, the consequences of the processing for individuals, the

existence of appropriate safeguards such as encryption and pseudonymization) (Article 6 (3a)). The Council proposed to 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 override the interests of the individuals. This was presumably designed to facilitate the use of big data applications. The fact that this suggestion did not make it into the compromise text of the GDPR does not come as a surprise as already during the vote on the Council's General Approach on June 15, 2015, 11 Member States expressed reservations[20] and the Council's Legal Service stated that it considered this provision to be incompatible with Article 8 (2) of the Charter of Fundamental Rights of the EU. The Article 29 Working Party had also raised concerns regarding this point.[21]

4. *Rights of Individuals*

The GDPR generally strengthens individuals' rights (i.e., notice obligation, rights of access, rectification, erasure, right to object, and right not to be subject to automated decision making, including profiling) and includes a number of new rights (i.e., restrictions of processing, data portability). We have summarized below some of the key developments.

- **Notice obligations.** The controller must provide the individual with information describing the purpose of the data collection. This notice obligation under the GDPR is enhanced compared to the Data Protection Directive and includes elements such as the contact details of the controller, its representative and data protection officer (if any), the legal basis for the processing, references to legitimate interest where relevant, specific information on data transfers, the right to withdraw consent, the right to data portability, the right to lodge a complaint and information on profiling where relevant (Article 14 (1) (a) through (e)). The Parliament's suggestion to include the use of standardized icons to enhance transparency is included in the GDPR, but should be further specified by the Commission via a delegated act (Article 12 (4b) and (4c)).

- **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 CJEU in its 2014 *Costeja* decision, was renamed and merged by the Parliament with the right to erasure. The Council's version of the GDPR did not offer any substantial deviation from the Parliament's approach, and was adopted in the current version of the GDPR. Under the GDPR, individuals have a right to obtain from controllers the erasure of their 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 their personal data; (4) the data were unlawfully processed; (5) a law requires the controller to erase the data; or (6) the data have been collected in relation to the offering of information society services to children (Article 17 (1)).

  As concerns data that has 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 (2a) and Recital 54). What constitutes ''reasonable'' steps will depend on the available technology and the cost of implementation.

  Finally, the GDPR provides a number of situations in which the right to be forgotten does not apply, namely when the processing of personal data is necessary for the right of freedom of expression, compliance with a legal obligation, reasons of public interest in the area of public health, archiving purposes or for the establishment, exercise or defence of legal claims (Article 17 (3) and Recital 53).

- **Right to restriction of processing.** The Council proposed a new right to restriction of data processing that made it into the current version of the GDPR (Article 17a). This right could include, e.g., temporarily moving selected data to another processing system, making selected data unavailable to users or temporarily removing published data from a website. In automated filing systems the restriction of data processing should in principle be ensured by technical means; the system should clearly indicate that the data processing is restricted (Recital 54a). The concept is somewhat comparable to the right to blocking, which is currently included in the Data Protection Directive, but rarely applied or enforced in practice.

- **Right to data portability.** The GDPR creates a new right to data portability. This right further strengthens the individuals' control over their own personal data by allowing them to export personal data from one controller to another, without hindrance from the first controller. Controllers must make the data available in a structured, commonly used, machine-readable and interoperable format that allows the individual to transfer the data to another controller (Article 18 (1) and Recital 55). This right applies even where the data processing is based on consent or the performance of a contract and carried out by automated means (Article 18 (2) (a) and (b)).

  The right to data portability is a strong signal to controllers to create and promote interoperable formats when handling personal data. This provision reaches beyond the scope of data portability between two controllers as stipulated in Article 18. It is also a vehicle for an EU policy decision to favor interoperable systems.[22]

[20] Belgium, France, Poland, Malta, Italy, Hungary, Austria, Estonia, Bulgaria, Cyprus, and Lithuania all expressed reservations.

[21] WP29 issued a statement that it is ''very much concerned'' about this aspect of the Council's proposal. See the WP29's press release of March 17, 2015, on Chapter II of the GDPR at http://src.bna.com/b64.

[22] This provision may also influence competition cases revolving around market foreclosures based on application programming interfaces and refusals to deal and license essential input information under Article 102 Treaty on the Functioning of the European Union (TFEU).

  PVLR ISSN 1538-3423

5. *Processing Not Requiring Identification*

The GDPR introduces some flexibility for companies in situations where the purposes for which they process personal data do not or no longer require the identification of an individual. The controller will then not be obliged to maintain, acquire or process additional information in order to identify the individual for the sole purpose of complying with the GDPR (Article 10).

In addition, where a controller is not in a position to identify the individual, the obligations concerning access, rectification, erasure, right to be forgotten, restriction and data portability do not apply, unless the individual provides additional information enabling his or her identification for exercising these 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 for demonstrating 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.

6. *Automated Decision-Making, Including Profiling*

The GDPR defines profiling as ''any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement'' (Article 4 3(aa)). Profiling is subject to general rules governing processing of personal data, including the need to have a legal basis and to comply with the data protection principles (Recital 58a).

However, decisions based solely on automated processing, including profiling, that produce legal effects or significantly affect individuals are only allowed if suitable safeguards are implemented (i.e., right to obtain human intervention and right to express his or her point of view), and if based on one of the following legal grounds: (1) the individual's explicit consent; (2) Member State law or EU law; or (3) a contract with the individual (Article 20). In particular, decision making based on such processing, including profiling, should be allowed when expressly authorized by applicable EU or Member State law including for fraud and tax evasion monitoring and prevention purposes (Recital 58).

The GDPR provides examples of processing activities that significantly affect individuals, such as the automatic refusal of an online credit application or e-recruiting practices without any human intervention (Recital 58). The GDPR prohibits decision-making based solely on automated processing of sensitive data, unless companies can rely on one of the legal bases available for the processing of sensitive data, such as explicit consent (Recital 58).

7. *Accountability, Risk-Based Approach, Data Protection Officer, Data Protection Impact Assessment and Related Principles*

- **Accountability and internal documentation.** The GDPR introduces the concept of accountability into EU data protection law. Accordingly, controllers are obliged to implement appropriate and effective measures and must be able to demonstrate the compliance of processing activities with the GDPR, including the effectiveness of the measures (Article 22 and Recital 60).

  In addition, the GDPR replaces the current obligation to register data processing activities with national DPAs with the requirement to keep internal privacy documentation. Both controllers and processors are required to maintain records of their data processing activities (Article 28). This requirement does not apply when companies employ fewer than 250 persons unless: (i) the data processing activities are likely to result in a risk for the rights and freedoms of individuals; (ii) the data processing activities are not occasional; or (iii) sensitive data, including data relating to criminal convictions and offences, are being processed. The GDPR also provides that adherence by a controller or processor to approved codes of conduct or to approved certification mechanisms may be used to demonstrate data protection compliance (Article 22 (2b); Article 26 (2aa); Article 30 (2a)).

- **Risk-based approach.** Another important novelty of the GDPR is that it introduces a risk-based approach to data protection. 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. For this assessment, the nature, scope, context and purpose of the processing, as well as the likelihood and severity of the risks for the rights and freedoms of individuals posed by the data processing activities is taken into account.

  A two-level risk approach is used (i.e., ''risk'' or ''high risk'') (Recital 60b). Certain obligations only apply to high-risk data processing activities, in particular: (i) data protection impact assessments (Article 33 (1)); (ii) notification of individuals of data breaches (Article 32); and (iii) prior consultation with DPAs (Article 34 (2)). The risk-based approach also appears in the provisions on privacy by design and by default (Article 23), appointment of a representative in the EU by a non-EU controller or processor (Recital 63 and Article 25 (2) (b)), documentation requirements (Article 28 (4)), and security requirements (Article 30).

  Guidance is needed on this topic to help companies assess with a reasonable level of certainty the level of risk related to their data processing activities. The GDPR provides a number of tools to help complete that assessment including approved codes of conduct, approved certifications, guidelines of the European Data Protection Board (EDPB) or the advice of a data protection officer (Recital 60c).

- **Data protection by design and by default.** The GDPR will contain new obligations to implement privacy-enhancing measures at the earliest stage of the conception of products and services that in-

volve the processing of personal data (privacy by design) and to, by default, select the techniques that are the most protective of individuals' privacy and data protection (privacy by default) (Article 23 (1) and (2), Recital 61). These two principles will be important for companies when building new products and services.

- **Data protection impact assessments and DPA consultation.** The GDPR requires controllers to carry out a data protection impact assessment in cases when their data processing activities are likely to result in a high risk for the rights and freedoms of individuals (Article 33 (1)). In any case, conducting a data protection impact assessment is required for: (i) profiling activities; (ii) processing on a large scale of sensitive data, including data relating to criminal convictions and offences; and (iii) systematic monitoring of a publicly accessible area on a large scale (Article 33 (2)). The GDPR offers DPAs a possibility to establish a list of types of data processing activities that are 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 is unable to 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 eight weeks (Article 34 (3)).

- **Data Protection Officer.** Under the GDPR, the appointment of a data protection officer (DPO) is only mandatory for controllers and processors when the core data processing activities: (i) involve monitoring of individuals on a large scale; or (ii) encompass sensitive data, including criminal convictions and offences (Article 35 (1)). Importantly, a group of undertakings may appoint a single DPO for the group, as long as the DPO is easily accessible for each undertaking (Article 35 (2)). EU Member States' law or EU law may make the appointment of a DPO mandatory in other circumstances (Article 35 (4)), and controllers and processors may, on their own initiative, appoint a DPO. The GDPR further specifies the role, position and tasks of DPOs (Articles 36 and 37).

- **Codes of conduct.** Associations and other bodies representing controllers or processors may draft codes of conduct for the purpose of specifying the application of the GDPR (Article 38 (1a) and Recital 76). DPAs may approve codes of conducts that do not relate to data processing activities in several EU Member States (Article 38 (2) and (2a)). Codes of conduct relating to data processing activities in several EU Member States should be submitted to the EDPB via the consistency mechanism (Article 38 (2b)). One of the key novelties of the GDPR is that approved codes of conduct are considered a valid mechanism for data transfers (Article 38 (1ab)), provided they meet certain requirements and are accompanied by binding and enforceable commitments.

- **Certification, seals and marks.** Whilst a code of conduct contributes to the proper application of the GDPR, certifications, seals and marks help demonstrate compliance with the GDPR (Article 39 (1)). Independent certification bodies, a DPA or the EDPB will certify companies (Article 39 (2a)) and monitor proper compliance with the certification. This is also a novelty of the GDPR compared to the Data Protection Directive.

8. *Data Security*

- **Security requirements.** Controllers and processors must implement appropriate technical and organizational measures, having regard to the state of the art and costs of implementation, and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity. Examples of security measures that are listed as appropriate include: (a) pseudonymization and encryption; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

  While the Parliament suggested a lighter compliance regime for companies pseudonymizing or encrypting personal data, the GDPR will not contain such a special regime. Rather, pseudonymization and encryption will be quasi-mandatory data security measures. Adherence to approved codes of conduct can be used to demonstrate compliance with data security requirements (Article 30).

- **Data breach notification.** The GDPR creates an obligation for controllers to notify DPAs and individuals of personal data breaches. A personal data breach (or ''data breach'') is defined as ''a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'' (Article 4 (9)). The obligation to notify DPAs only concerns data breaches that are likely to result in a risk for the rights and freedoms of individuals, but the GDPR does not provide clear guidance to assess whether or not such risk is present in a specific data breach. Moreover, when the data breach is likely to result in high risks, the controller must also notify the individuals affected by the breach, unless certain exceptions apply (e.g., the data are protected by security measures such as encryption, the controller has taken measures to reduce the risk for individuals or notifying would involve disproportionate effort and individuals have been informed via public communications) (Article 32 (3)). In any case, DPAs can require controllers to notify individuals about data breaches (Article 32). The GDPR specifies the information that must be provided to DPAs and individuals (Article 31 (3) and 32 (2)).

  Based on the text of the GDPR, it seems that virtually any data breach could have to be notified to DPAs since Recital 67 clarifies that any data breach that may result in ''physical, material or moral damage to individuals such as loss of control over their personal data or limitation of their

  PVLR ISSN 1538-3423

rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned'' should be notified, unless the controller can demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals. Furthermore, the GDPR requires processors to notify any data breach to controllers, irrespective of the risks the data breach entails (Article 31 (2)). Finally, controllers need to document any personal data breach and DPAs can request access to this documentation (Article 31 (4)). The EDPB is expected to issue guidelines regarding data breaches, in particular regarding the specific conditions triggering the notification requirement (Article 66 (1) (bb)).

As proposed by the Council, the notification to the DPA must take place without undue delay and, where feasible, within 72 hours after the controller becomes aware of the data breach (Article 31). This provides a bit more flexibility than the notification period of 24 hours that was originally proposed by the Commission. The notification period of 72 hours is not absolute. Controllers may exceed this time period if they can provide the DPA with a reasoned justification for doing so.

In parallel with the negotiations on the GDPR, the EU institutions have also recently agreed on another piece of legislation dealing with security breach notification requirements, i.e., the Directive concerning measures to ensure a high common level of network and information security across the Union (the ''Network and Information Security Directive'' or ''NIS Directive'').[23] Although the NIS Directive does not specifically deal with personal data but rather with the security of information systems, many IT security incidents will involve personal data and will therefore trigger notification obligations under both the GDPR and the NIS Directive. The NIS Directive requires ''operators of essential services'' to notify competent authorities about incidents having a significant impact on the provisioning of their services. Notably, digital service providers such as cloud computing services providers, search engines and operators of marketplaces established in or providing services in the EU will be subject to the NIS Directive as implemented into national law. Hopefully, the DPAs and the national authorities competent for receiving notifications under the NIS Directive will issue guidance on how companies must react to security incidents in order to ensure compliance with both pieces of legislation.

9. *Roles and Responsibilities of Parties*

- **New rules for joint controllers.** While the Data Protection Directive did not specifically regulate joint controllership, the GDPR includes a new obligation for joint controllers to stipulate in an ''arrangement'' their respective responsibilities under the GDPR, in particular their respective duties to allow individuals to exercise their rights to their personal data and to provide notice to individuals. In addition, the ''essence'' of the arrangement between joint controllers must be made available to individuals. The issue of liability between joint controllers has been heavily debated over the last years. While the Commission and Parliament proposed to impose joint and several liability on joint controllers, the GDPR follows the Council's approach that provides that joint controllers are each liable for the entire damage caused by the processing (Article 77 (4)).

- **Stricter requirements for processing and sub-processing.** The GDPR provides much more detailed requirements for processing agreements than the Data Protection Directive. The new requirements are broadly similar to the ones included in the 2010 Commission's Standard Contractual Clauses for Controller-to-Processor international data transfers.[24] The GDPR requires processors to obtain the prior written consent of the controller to any sub-processing, but specifies that consent can be specific or general. In practice, controllers can thus provide a general authorization for sub-processing in the data processing agreement. As suggested by the Council, the GDPR allows for the adoption of standard contractual clauses for data processing agreements, either by the Commission using implementing acts[25] or by a DPA in accordance with the consistency mechanism[26] (Article 26).

10. *International Data Transfers*

- **General rules on international data transfers remain.** The GDPR broadly maintains the rules on international data transfers that are included in the Data Protection Directive. The transfer of personal data outside of the EU is prohibited unless the country of the data recipient has been considered to be adequate (based on a finding of ''adequate protection''), companies have implemented a data transfer mechanism (including Binding Corporate Rules) or can rely on a statutory derogation.

- **More stringent criteria for adequacy decisions.** The GDPR provides new criteria for the Commission to consider when assessing the level of protection of a third country, territory, sector or international organization. Some of these criteria are clearly inspired by the judgment of the EU Court of Justice in *Schrems*, which invalidated Safe Harbor for data transfers. For instance, the Commission must assess any national security laws in the third country and how public authorities can access personal data. Other elements to take into ac-

[23] Press release of the Commission regarding the political agreement reached in ''Trilogues'' from December 8, 2015, *available at* http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

[24] Commission Decision 2010/87/EU, *available at* http://src.bna.com/b7i.

[25] See below for more information on secondary legislation to be adopted by the Commission.

[26] See below for more information on the consistency mechanism.

count and which have been emphasized in *Schrems* include the rules on onward transfers, the existence of effective and enforceable rights and effective administrative and judicial redress for individuals, and the existence and effective functioning of an independent supervisory authority which oversees compliance with data protection rules (Article 41 (2) (a) and (b)). In addition, the GDPR clarifies that adequacy decisions can only be granted when the level of data protection is ''essentially equivalent'' to that guaranteed in the EU, as stipulated in *Schrems* (Recital 81).

- **No Sunset Clause for existing Commission's adequacy decisions and DPAs' prior authorizations.** The adequacy decisions adopted by the Commission under the Data Protection Directive will remain in force until amended, replaced or repealed by the Commission (Article 41 (8)). This applies to the adequacy decisions regarding Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay. In addition, the three Commission's decisions for Standard Contractual Clauses and the DPAs' authorizations for ad-hoc contracts or BCRs issued under the Data Protection Directive, will remain valid until amended, replaced or repealed (Article 42 (5b)). In practice, this should ensure continuity and companies that have concluded Standard Contractual Clauses or have received the authorizations for the use of ad-hoc contracts or BCRs will still be able to rely on these mechanisms.

  The Parliament's proposed sunset clause for existing adequacy decisions did not survive the Trilogue negotiations. Still, *Schrems* made it clear that the Commission's adequacy decisions can be declared invalid at any time, even without a sunset clause. Moreover, adequacy decisions should provide for a period review at least every four years (Article 41 (3) and Recital 81b) and the GDPR obliges the Commission to monitor on an on-going basis the developments in third countries that may affect existing adequacy decisions and, where necessary, repeal, amend or suspend an adequacy decision (without retroactive effect) (Article 41 (3, 4a and 5)).

- **Blacklists of non-adequate third countries.** The GDPR provides that the Commission will publish lists of third countries, territories, sectors or international organizations that it considers to no longer provide an adequate level of protection (Article 41 (7)).

- **Data transfer mechanisms.**

  - **Binding Corporate Rules (BCRs).** BCRs (for controllers and processors) are officially recognized in the GDPR. The GDPR lists the type of provisions that should be, at a minimum, included in BCRs (Article 43 (2)). The format and procedures for the exchange of information regarding BCRs between controllers, processors and DPAs may be further worked out by the Commission via implementing acts (Article 43 (4)). As proposed by the Council, the GDPR makes BCRs available to a group of undertakings or group of enterprises ''engaged in a joint economic activity'' (Article 4 (17)). The GDPR does not define this concept, but it seems that BCRs will not only be available to companies that are part of the same corporate group, but also to companies that are business partners (Article 43).

  - **Data transfer agreements.** As is the case under the Data Protection Directive, the GDPR allows for personal data to be transferred to non-adequate third countries on the basis of data transfer agreements. The GDPR provides that Standard Contractual Clauses can be adopted either by the Commission or by an individual DPA (and then approved by the Commission). In these cases, the transfer does not require specific DPA authorization (Article 42 (2)). The GDPR also allows DPAs to authorize data transfers based on contractual clauses between the controller or processor and the controller, processor or the recipient of the data in a third country (Article 42 (2a)). In this case, the DPA must apply the consistency mechanism. This last option is what is called ad-hoc contracts under the current data protection framework.

  - **Influence of *Schrems*.** A novelty that was added to the GDPR during the Trilogues, presumably to incorporate the reasoning of the *Schrems* judgment, is that a data transfer mechanism will only be valid on the condition that enforceable individuals' rights and effective legal remedies for individuals are available, including to obtain effective administrative or judicial redress and to claim compensation in the EU or in a third country (Article 42 (1) and Recital 83). The lack of such effective remedies and redress was one of the key reasons for the CJEU to invalidate the Safe Harbor framework for EU-U.S. data transfers in *Schrems*.

  - **New data transfer mechanisms.** Upon the Council's suggestion, two new grounds for international data transfers are introduced in the GDPR: adherence to an approved code of conduct or to an approved certification mechanism, which must be accompanied by binding and enforceable commitments (see above). While these innovations are welcome, it remains to be seen how they will develop and whether they will be useful to bridge some of the gaps of the current legal framework.

- **Derogations.** Under the GDPR, personal data may still be transferred to third countries in the absence of an adequacy decision or appropriate safeguards (e.g., Standard Contractual Clauses, codes of conduct, certification mechanisms, BCRs), in the same limited number of circumstances as under the Directive. As proposed by the Commission and the Council, the GDPR adds to this list a derogation for data transfers based on compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the individual. This is on the condition that the transfer is not repetitive and concerns only a limited number of individuals. In that situation, the controller also needs to ''adduce suitable

   ISSN 1538-3423

safeguards'' to protect the personal data, taking into account the circumstances surrounding the data transfer, and inform the DPA of the data transfer. However, the GDPR does not specify how the ''suitable safeguards'' should be adduced (Article 44 (1h)). The controller will also need to inform the individual about the data transfer and the compelling legitimate interests it pursues. This additional derogation is a welcome solution for companies that may simply need to transfer personal data abroad in exceptional cases, without being able to rely on other data transfer solutions. However, it is unclear how this will function in practice, and the conditions for that exception are so strict that its concrete utility for companies is yet to be seen.

- **Foreign data disclosure requests.** The GDPR provides that any judgment of a court or tribunal or decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data can only be enforced if it is based on an international agreement concluded between the EU and the requesting third country, such as a mutual legal assistance treaty (Article 43a). In the absence of such international agreement, data disclosures are only allowed if the data transfer conditions of the GDPR are met (e.g., the data disclosure is necessary for an important ground of public interest recognized in applicable EU or Member State law) (Recital 90). This is a compromise between the Parliament and the Council. The Parliament proposed that companies would need to obtain DPAs' approval before disclosing personal data in response to such requests, but the Council disagreed. The final version of this provision shifts responsibility from the companies (that face conflicting legal obligations) and DPAs, to a more appropriate level for dealing with these types of issues (i.e., international agreements between States), which is a welcome development.

- **National prohibitions.** As proposed by the Council, the GDPR provides that Member States can invoke ''important reasons of public interest'' to ''expressly set limits'' to the transfer of certain types of data to a third country or international organization that has not received an adequacy decision. Member States must notify such national provisions to the Commission (Article 44 (5a)). This clause holds the risk of producing fragmentation among the Member States with regard to their data transfer policies.

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

To facilitate compliance with EU data protection law for multinational companies while ensuring a consistent approach to EU data protection law, the GDPR introduces a ''one-stop shop'' for companies that are established in multiple EU Member States and creates a cooperation procedure between DPAs. The DPA of the main establishment of a company in the EU will take the lead in supervising the company's compliance across the EU in accordance with the cooperation procedure. To further ensure the consistent application of the GDPR in the EU and to solve disagreements between the lead DPA and other DPAs, the GDPR creates a consistency mechanism under the authority of the EDPB (which will replace the current Article 29 Working Party).

- **Main establishment.** The ''one-stop shop'' hinges upon the new concept of the ''main establishment'' of a company. The rule is that the lead DPA is the DPA of the company's main establishment or of the single establishment of the controller or processor in the EU (Article 51a (1)). Therefore, determining where a company has its main establishment is essential to establishing which DPA will be considered as the ''lead DPA'' (i.e., the one-stop shop) and will be crucial for multinational companies.

  As proposed by the Council, the criterion for determining where a company has its ''main establishment'' will be the location of the company's central administration in the EU (Article 4 (13)). The ''central administration'' of a controller relates to the ''effective and real exercise of management activities'' that determine the main decisions regarding the purposes and means of processing through ''stable arrangements.'' However, the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore not determining criteria for a main establishment (Recital 27). In addition, the legal form of the establishment will not be a determining factor. Branch offices or subsidiaries can constitute a main establishment (Recital 19). The main establishment of the processor is located where its central administration is established in the EU (Recital 27).

The GDPR harmonizes fines throughout the EU and determines the level of fines that can be imposed for data protection infringements in all EU Member States. The amounts are very high.

There are two exceptions to the rule that the main establishment is the location of a company's central administration in the EU:

- For controllers, if decisions on the purposes and means of the data processing are taken in another establishment of the controller in the EU, and the latter establishment has the power to have such decisions implemented, then that other establishment will be the main establishment (Article 4 (13) (a)).

- For processors without a central administration in the EU, the main establishment will be the processor's establishment in the EU in the context of which the main processing operations are carried out, for the specific obligations that apply to the processor (Article 4 (13) (b)).

In situations where there is a disagreement regarding which DPA is the lead DPA, the EDPB must be notified

of such disagreement and will adopt a binding opinion determining the lead DPA (Article 58a (1b)).

- **One-stop shop and cooperation procedure.** The lead DPA will take the lead as concerns cross-border data processing activities i.e., activities taking place in the context of establishments of the company in multiple Member States or affecting individuals in multiple Member States (Article 51a (1)), and will be the sole interlocutor of the controller or processor for the cross-border processing of that controller or processor (Article 51a (3)). However, individuals will still be able to lodge complaints with their local DPA, even if the company concerned has its main establishment elsewhere. In that situation, DPAs will need to inform the company's lead DPA under the cooperation procedure, which may decide to take the case (Articles 51a (2a) and (2b)).

  At a high-level, the cooperation procedure provides for a process by which DPAs will exchange information and cooperate with a view to reach consensus (Article 54a (1)). In more details, the cooperation procedure will on the one hand allow local DPAs to deal with local matters, prepare draft decisions (Article 51a (2c)) and have their voice heard by the lead DPA (Article 54a (2)). On the other hand, the cooperation procedure will allow the lead DPA to call out a matter, request mutual assistance from other DPAs and initiate joint operations (Article 54a (1a)). In case of disagreement, the consistency mechanism is triggered (Article 54a (3)).

  Under the cooperation procedure, if a local complaint has been filed with a local DPA and both the local DPA and the lead DPA agree on a matter, the lead DPA will notify its decision to the company's main establishment and inform the other DPAs concerned, and the EDPB, of its decision. The DPA to which the complaint was lodged will then inform the complainant. If the complaint is dismissed or rejected, the DPA to which the complaint was lodged must adopt the decision, notify it to the complainant, and inform the company thereof (Article 54a (4b)). The lead DPA together with the other DPAs can also decide to dismiss or reject only some parts of the complaint and to act only on certain parts of the complaint. In such cases, the lead DPA is in charge of notifying the decision to act to the company as well as to the complainant, whereas the DPA that received the complaint is in charge of adopting the decision concerning the dismissal or rejection of parts of the complaint, and to notify the complainant and the company about this decision (Article 54a (4bb)). This should allow companies and individuals to challenge DPAs' decisions before their national courts.

  The ''one-stop shop'' survived the Trilogue negotiations, but the end result is quite different from how the Commission had originally conceived the concept. The Commission's proposal provided for a lead DPA that would be competent for the supervision of all data processing activities of companies established in multiple Member States, not just the cross-border data processing activities. The Parliament and Council amended that original ''one-stop shop'' in such a way that it is weaker and more complex. It is likely that it will take some time to work out the details of the procedure, given the inevitable disagreements between DPAs.

- **Consistency mechanism.** The cooperation rules are supplemented by a consistency mechanism to ensure an harmonious application of the GDPR across the different EU Member States. The consistency mechanism is under the supervision of an independent body, the EDPB (successor to the Article 29 Working Party), functioning as an advisory and appellate body to the national DPAs. At a high-level, the consistency mechanism is triggered in three broad situations:

  1. The EDPB will take binding decisions: (i) if DPAs disagree regarding a decision to be taken in the cooperation procedure; (ii) if DPAs disagree on which DPA is the lead DPA; and (iii) if a DPA does not request an opinion from the EDPB where required, or when a DPA does not follow an EDPB opinion (Article 58a). The required majority for binding opinions is a two-thirds majority (a simple majority is sufficient for non-binding opinions).

  2. In certain cases, national DPAs will need to obtain the opinion of the EDPB before they can take decisions, including in relation to data protection impact assessments, codes of conduct, accreditation criteria of certification bodies and of bodies monitoring compliance with codes of conduct, standard contractual clauses, ad hoc contracts or binding corporate rules (Article 58 (1)). The opinion will not be binding and can be adopted with a simple majority. DPAs will need to take ''utmost account'' of the EDPB opinion. If a DPA does not follow the EDPB opinion, the EDPB can adopt a binding decision (Article 58a (1) (d)).

  3. Upon request of its Chair, a DPA or the Commission, the EDPB will provide an opinion on any matter of general application or producing legal effects in more than one EU Member State (e.g., when a DPA does not comply with its obligations of mutual assistance or joint operations) (Article 58 (2)).

The GDPR's consistency mechanism is entirely new and it remains to be seen how effective it will be in practice; some bumps along the road for companies are to be expected as the DPAs get used to working together in a more formal and legalistic framework than the Article 29 Working Party provided.

12. *Sanctions and Fines*

- **High fines.** An important change from the Data Protection Directive is that the GDPR harmonizes data protection enforcement in the EU. In particular, the GDPR determines the level of fines that can be imposed for data protection infringements in all EU Member States. The amounts are very high; the GDPR introduces two levels of fines: (1) up to €10 million or 2% of the undertaking's global annual turnover, whichever is higher, for certain infringements; and (2) up to €20 million or 4% of

  PVLR ISSN 1538-3423

the undertaking's global annual turnover, whichever is higher, for more severe infringements.

These fines have been the subject of intense debate. Whereas the Commission and Council suggested fines of up to €1 million or 2% of a company's annual worldwide turnover, the Parliament demanded that fines go up to €100 million or 5% of a company's annual worldwide turnover. With the compromise being that fines can go up to €20 million or 4% of global annual turnover, it is fair to say the Parliament won this battle. The amount of fines that will be imposed will depend on various criteria, including the severity and duration of the violation, the intentional character of the violation, any mitigation measures, the categories of personal data affected, the degree of cooperation with the DPAs and previous violations by the same controller or processor (Article 79). These fines add real ''teeth'' to data protection enforcement in the EU.

13. *Other Aspects*

- **Leeway for EU Member States.** The GDPR provides a set of detailed rules on data processing that will apply uniformly in all EU Member States. However, differences between EU Member States may still remain, since the GDPR allows Member States to further determine specific conditions for certain data processing activities, such as the mandatory appointment of a data protection officer beside the three scenarios provided in the GDPR (Article 35 (1) and (4)), the processing of national identification numbers (Article 80b), data processing in the employment context (Article 82) and data processing by controllers or processors that are subject to professional secrecy (Article 84). This approach has been criticized for leading to fragmentation of the EU internal market, thereby undermining the objective of harmonization of the GDPR. The Parliament had asked to limit the leeway that would be given to EU Member States, e.g., by including minimum standards in the GDPR for national legislation on data processing in the employment context, but this approach did not survive the ''Trilogue'' negotiations.

Perhaps the most significant change from the current Data Protection Directive is that the GDPR will be directly applicable in all EU Member States.

Next Steps

The significance of the GDPR speaks for itself, and is illustrated by the discussion above. The following are some important things to remember about the next steps. For companies, the most important point is to use the next two years to prepare for the entry into force of the GDPR, which is the most important data protection legislation in a whole generation, and is likely to influence data protection law around the world over the next twenty years.

- **Adoption and entry into force.** As stated above, the GDPR will now be reviewed by lawyer-linguists at the Commission, so the text may still undergo changes. Once reviewed, the GDPR will be submitted for adoption by the Parliament (in plenary session) and Council. The adopted text will be jointly signed by the Presidents and Secretaries General of both institutions. After signature, the text will be published in the Official Journal, and the GDPR will become effective two years after the date of publication. We expect the votes to take place in the Spring of 2016, so the GDPR will likely be effective as of the Spring of 2018.
- **Secondary legislation.** The GDPR provides that the Commission can determine certain technical details via secondary legislation, i.e., delegated acts (Art. 290 TFEU) and implementing acts (Art. 291 TFEU). Since the Commission is subject to more scrutiny with regard to delegated acts than implementing acts, the Parliament had asked for certain important issues to be worked out via delegated acts. However, the Parliament gave mostly in on this point and accepted that key issues (e.g., adequacy decisions, procedures around BCRs and codes of conduct) can be handled via implementing acts. Nevertheless, the use of icons in privacy notices will be worked out by delegated acts. Originally, the Commission proposed 26 delegated and 22 implementing acts.[27] In the end, only 2 delegated acts and 11 implementing acts were retained in the text of the GDPR agreed on in the Trilogue negotiations. Most of the provisions that the Commission initially proposed to regulate via secondary legislation are now either incorporated into the GDPR or left to be set out by the EDPB or codes of conduct. The Commission is expected to now start preparing this secondary legislation.
- **Direct application in EU Member States.** Perhaps the most significant change from the current Data Protection Directive is that the GDPR will be directly applicable in all EU Member States. In principle, Member States will not need to adopt national legislation to transpose the new rules into their legal system. This means that most national data protection acts will either be repealed or severely reduced in scope (for example, to be limited to points that the GDPR does not cover). In some Member States this may lead to federalism issues (e.g., in Germany). National law will also remain relevant regarding issues that the GDPR leaves largely up to Member States (e.g., data processing in the employment context—see Article 82). The exact interplay between the GDPR and national law will likely be the subject of intense debates.
- **Advance work by DPAs.** We expect DPAs to take advantage of the two year transition period before the GDPR becomes effective to prepare themselves for the significant increase in workload that it will undoubtedly bring. Not only will DPAs have

[27] *See* Council document no. 8833/15 on delegated and implementing acts at http://data.consilium.europa.eu/doc/document/ST-8833-2015-INIT/en/pdf.

greater enforcement powers, they will also need to handle more requests and notifications from companies (e.g., requests for approval of certain data processing activities or data transfer mechanisms, data breach notifications) and claims from individuals. In addition, the one-stop shop mechanism could place a disproportionate burden on the DPAs of EU Member States that host the European headquarters of multinational companies, leading to the possibility of power struggles within the EDPB to share the burden of supervision.

- **Influence on other initiatives for EU legislative reform.** The adoption of the GDPR will influence other EU reform initiatives. In particular, the Commission has been waiting for the GDPR to be adopted in order to launch the reform of the ePrivacy Directive[28], which sets out rules on the use of cookies and e-marketing. The GDPR is by no means the end of regulation that applies to the use of personal data in the EU. Other data-drive initiatives will most certainly emerge at the EU level in the next few years.

[28] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37-47, *as amended by* Directive 2009/136/EC of the European Parliament and of the Council.

  PVLR ISSN 1538-3423