European Union Data Privacy Law Developments

W. Gregory Voss

European Union Data Privacy Law Developments

*By W. Gregory Voss**

During the past year, many developments occurred in European Union ("EU") data privacy law both under the 1995 EU Data Protection Directive ("Directive")[1] and in the reform of the EU data protection law framework. This evolution is attributable to advisory guidance, enforcement actions, and an EU case, as well as legislative action by the European Parliament ("Parliament"). Note that Edward Snowden's revelations on the surveillance programs of the U.S. National Security Agency ("NSA") cast a shadow over many aspects of the work of the European Commission (the "Commission") and the Parliament during this period.[2]

EU Article 29 Working Party Guidance on Anonymizaton Techniques

The EU's independent privacy advisory panel—the Article 29 Data Protection Working Party ("WP29")—recently offered guidance regarding anonymization techniques that may be used for data security purposes, as well as in open data and big data services.[3] WP29 issued Opinion 05/2014, which highlighted that, "[o]nce a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies."[4] In order for this to be the case, the data must be made anonymous "in such a way that the data subject is no longer identifiable."[5] For this to be so, the anonymization must be "irreversible."[6] In fact, WP29 suggested that personal data should generally be anonymized "by default," and it affirmed that anonymization itself is a "further processing" of personal data and thus would be subject to the purpose limitation principle.[7]

* W. Gregory Voss is a Professor of Business Law at Toulouse University, Toulouse Business School and a Member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC) in Toulouse, France.

1. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive].

2. *See, e.g.*, W. Gregory Voss, *Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17 J. Internet L. 1, 12, 20–22 (2014).

3. Article 29 Data Prot. Working Party, Opinion 05/2014 on Anonymisation Techniques (Apr. 10, 2014) (WP 216) [hereinafter Opinion 05/2014], *available at* http://goo.gl/0FQC8c.

4. *Id.* at 5.

5. Directive, *supra* note 1, para. 26, at 33.

6. Opinion 05/2014, *supra* note 3, at 5.

7. *Id.* at 7.

"Further processing" to achieve anonymization is "compatible with the original purposes of the processing but only [to the extent the] . . . process is such as to reliably produce anonymized information in the sense described" in Opinion 05/2014.[8] In this regard, Opinion 05/2014 provides:

> An effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records with a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended.[9]

WP29 highlighted that pseudonymized data is not the same as anonymized data and therefore continues to be subject to the EU data protection law regime (including the provisions of the Directive).[10] Opinion 05/2014 then continues with a more technical discussion of the robustness of different technologies, typical mistakes, and recommendations, followed by a "primer on anonymisation techniques."[11]

Google Privacy Policy Enforcement Action

In March 2012, Google revised its privacy policies for its various services into one merged policy,[12] which resulted in enforcement actions that provide insight into the expectations of data protection authorities ("DPAs") regarding privacy policies. WP29 sent the search engine company a letter in October 2012,[13] which, together with an appendix thereto,[14] detailed recommendations for Google's new privacy policy.[15] In addition, WP29 encouraged Google "to engage with [DPAs] when developing services with significant implications for privacy,"[16] and to comply with its recommendations within four months.[17] In April 2013, following Google's failure to implement "any significant compliance measures," the DPAs of France, Germany, Italy, the Netherlands, Spain, and the United Kingdom simultaneously launched enforcement actions against Google.[18]

8. *Id.*
9. *Id.* at 9.
10. *See id.* at 10.
11. *Id.* at 11–37.
12. Letter from Article 29 Data Prot. Working Party to Larry Page, Chief Exec. Officer, Google Inc. 1 (Oct. 16, 2012), *available at* http://goo.gl/kL1Wg6.
13. *Id.*
14. *Id.* at app. 1–9, *available at* http://goo.gl/9twc4w. (Appendix: Google Privacy Policy—Main Findings and Recommendations).
15. *Id.* app. at 2–3.
16. *Id.* at 3.
17. Press Release, Commission nationale de l'informatique et des libertés, Google Privacy Policy: Six European Data Protection Authorities to Launch Coordinated and Simultaneous Enforcement Actions (Apr. 2, 2013), *available at* http://goo.gl/Zkhzz.
18. *Id.*

On June 20, 2013, the French DPA ("CNIL") ordered Google to comply with the French law implementing the Directive and to remedy breaches thereof.[19] In particular, CNIL required Google, within three months, to (1) clearly define the purposes of processing users' personal data, (2) define non-excessive retention periods for personal data, and (3) inform users and obtain consent prior to storing cookies on their devices.[20] The breeches identified by the DPAs of the other five countries also resulted from: "insufficient information," "undefined or insufficiently defined data retention periods," and "unlimited combination of data."[21] After Google failed to comply with the French order, the CNIL initiated a formal procedure against the company,[22] which led to a decision imposing France's highest data protection violation fine (€150,000), enjoining the related personal data processing, and requiring the publication of a communique regarding the fine and data breaches, as well as linking the decision, for a period of forty-eight consecutive hours, on its French home page.[23] The publication sanction was perhaps the most prejudicial (at least from an image standpoint) to Google, which unsuccessfully challenged this aspect of the CNIL's decision in summary proceedings before France's highest administrative court.[24]

The CNIL's decision follows that of the Spanish DPA on December 18, 2013, imposing individual fines of €300,000 each for three serious violations of Spain's data protection law, for a total of €900,000,[25] and comes after the Dutch DPA's finding on November 28, 2013, that the "combining of personal data by Google since the introduction of its new privacy policy on 1 March 2012 is in breach of the Dutch data protection act."[26]

Subsequent to the CNIL decision, the Italian DPA, as part of the simultaneous European DPAs' enforcement actions, ruled on July 10, 2014, that Google must take various measures related to its Gmail, Google Search, and other services within eighteen months from service of the decision.[27] These measures include the requirement (i) that Google provide "effective information notices" to

19. Press Release, Commission nationale de l'informatique et des libertés, CNIL Orders Google to Comply with the French Data Protection Act, Within Three Months (June 20, 2013), *available at* http://goo.gl/mV84M4.

20. *Id*.

21. *See* Press Release, Commission nationale de l'informatique et des libertés, Google Privacy Policy: State of Play of the Enforcement Actions Taken by European Data Protection Authorities (July 23, 2013), *available at* http://goo.gl/jJZkLf.

22. Press Release, Commission nationale de l'informatique et des libertés, Google: Failure to Comply Before Deadline Set in the Enforcement Notice (Sept. 27, 2013), *available at* http://goo.gl/hGYX8Z.

23. Deliberation No. 2013-420 of the Sanctions Committee of CNIL Imposing a Financial Penalty Against Google Inc. 28 (Jan. 3, 2014), *available at* http://goo.gl/exjL12.

24. CE, Feb. 7, 2014 (Société Google Inc. No. 374595), *available at* http://goo.gl/hvFwfp.

25. Legal Grounds of the Decision R/02892/2013 of 18 December 2013 on the Infringement Proceedings Instigated by the Spanish Data Protection Agency Against the Entities Google Inc. and Google Spain, S.L., *available at* http://goo.gl/9gTpOi.

26. Press Release, College Bescherming Persoonsgegevens [Dutch DPA], Dutch DPA: Privacy Policy Google in Breach of Data Protection Law (Nov. 28, 2013), *available at* http://goo.gl/xw1sbu.

27. Decision Setting Forth Measures Google Inc. Is Required to Take to Bring the Processing of Personal Data Under Google's New Privacy Policy into Line with the Italian Data Protection Code (July 10, 2014), *available at* http://goo.gl/EgAT1x.

users;[28] (ii) that it obtain "the prior consent of both authenticated and non-authenticated users" regarding the processing of their information "including the processing of the information arising from the automated processing of authenticated users' personal data" regarding the use of Gmail services, *inter alia*, for behavioral advertising, navigation monitoring and analysis, and profiling purposes;[29] and (iii) that it respond to requests for data deletion (other than in the exercise of the "right to be forgotten"[30]) within a two-month period for "active systems"[31] and within a 180-day period for "information stored in so-called back-up systems,"[32] with a data retention policy to be "adopted in line with the purpose limitation principle."[33] In addition, on September 30, 2014, the Hamburg Commissioner for Data Protection and Freedom of Information, which had acted with the other European DPAs as representative of Germany on the Google privacy policy task force, announced the issuance the week before of a formal administrative order against Google for data protection law violations involving the combining of data from various Google services and user profiling.[34]

Finally, on September 23, 2014, WP29 wrote to Google, providing a list of possible compliance measures in an appendix to its letter, referring to the European DPA actions and a meeting held in Paris on July 2, 2014, with Google, WP29, and five European DPAs (at which a draft of such list was presented), and stating that WP29 "may also consider issuing guidance on specific issues to the entire industry, at a later stage."[35]

The CNIL case, the related European DPAs' actions, and WP 29 correspondence show the importance of providing specific information for distinct services, prohibiting data collected for one service from being available for another

28. *Id.* at dec. para. 1.

29. *Id.* at dec. para. 2.

30. *Id.* The decision specifically carves out "right to be forgotten" deletion requests, and in the grounds for the decision, the Italian DPA refers to the Court of Justice of the European Union Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (May 13, 2014), as well as guidelines then to come from the Article 29 Data Protection Working Party for treatment of "right to be forgotten" deletion requests, stating that "the Garante will limit itself, at this stage, to issuing specific instructions with regard to data deletion requests lodged by . . . users holding Google accounts . . . and will limit the scope of application of this decision to data deletion requests that concern features other than Google Search." *See id.* at dec. para. 5

31. *Id.* at dec. para. 3(a). The Italian DPA further required that "the relevant data should be deactivated over the initial 30 days." *Id.*

32. *Id.* at dec. para. 3(b). It was further stipulated that "during the period in question the only processing operation allowed in respect of the relevant data shall be the recovering of lost information," while encryption must be used, or "where necessary" anonymization techniques, in order to protect the data against unauthorized access. *Id.*

33. *Id.* at dec. para. 3(c).

34. Press Release, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit [Hamburg Comm'r of Data Prot. & Freedom of Info.], Major Changes in Google's Data Processing Required—Data Protection Commissioner Issues Administrative Order (Sept. 30, 2014), *available at* http://goo.gl/3kjBYk.

35. Letter from Article 29 Data Prot. Working Party to Larry Page, Chief Exec. Officer, Google Inc. (Sept. 23, 2014), *available at* http://goo.gl/5lxDe2. The appendix, which deals with the issues of information requirements (including those for specific services such as YouTube, Google Analytics, and DoubleClick), user controls, and data retention policies, is available at http://goo.gl/t7sLSZ.

without appropriate data subject consent, limiting personal data retention periods to what is strictly necessary, and cooperating with DPAs. Although the fines imposed were relatively low, these decisions foreshadow a potential major increase in data protection violation fines contained in the proposed EU data protection reform.[36]

Data Retention Directive Declared Invalid

On April 8, 2014, in response to requests for review by the High Court of Ireland and the Constitutional Court of Austria, the Court of Justice of the European Union ("ECJ"), the highest court of the EU, declared invalid Directive 2006/24/EC[37] regarding data retention (the "Data Retention Directive").[38] The Data Retention Directive was adopted to harmonize obligations of

> providers of publicly available electronic communications services or of public communications networks [such as internet service providers and telecom operators] with respect to the retention of certain data [such as location and traffic data that could be used to identify subscribers and users] . . . to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime.[39]

The Data Retention Directive required retention of the data for a minimum of six months and a maximum of two years[40] for fixed, mobile, or internet telephony as well as e-mail communications.[41]

The ECJ found that, even though the retained data did not include the content of the communications, that data could

> allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[42]

Consequently, the retention of data "might have an effect on . . . [users'] exercise of the freedom of expression guaranteed by Article 11 of the Charter [of Fundamental Rights of the EU]."[43] Moreover, "[t]he retention of data for the purpose of possible access . . . by . . . national authorities . . . directly and specifically effects

36. *See infra* note 61 and accompanying text.

37. Directive 2006/24, 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, 2006 O.J. (L 105) 54 (EC).

38. Joined Cases C-293 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Comm. Marine & Natural Res., paras. 69–73 (Apr. 8, 2014), *available at* http://goo.gl/qP2ZaL.

39. Council Directive 2006/24, art. 1(1), 2006 O.J. (L 105) 54, 56.

40. *Id.* art. 6, at 58.

41. *Id.* art. 5, at 57–58.

42. Joined Cases C-293/12 & C-594/12, *supra* note 38, at para. 27.

43. *Id.* at para. 28 (citing Charter of Fundamental Rights of the European Union, art. 11, 2000 O.J. (C 364) 1, 11 (EC)).

private lives . . . and the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter . . . ."[44]

The ECJ concluded that the Data Retention Directive interfered with the privacy rights of subscribers because "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[45] The Data Retention Directive failed to ensure that the retention period was "limited to what [was] strictly necessary" by establishing (1) a minimum retention period of six months without distinguishing between different sorts of data or different types of users,[46] and (2) a retention period between six months and two years without requiring any "determination [that the] period must be based on objective criteria."[47] The ECJ also found that the Data Retention Directive did not provide adequate safeguards "to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data."[48] It concluded that, "by adopting [the Data Retention] Directive . . . , the EU legislature . . . exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter."[49] For those reasons, the ECJ declared invalid the Data Retention Directive.[50] The Commission, through its then Commissioner for Home Affairs, Cecilia Malström, stated that it will "now carefully asses[s] the verdict and its impact . . . [and] will take its work forward in light of progress made in relation to the revision of the e-Privacy directive and taking into account the negotiations on the data protection framework."[51]

WP29, which welcomed the ECJ's decision, indicated that the invalidation of the Data Retention Directive was also "motivated by the fact that it does not require that the data be retained *within the EU*," and as such did not comply with the Charter's requirement of ensuring data protection and security "by an independent authority on the basis of EU law." WP29 also called upon Member States to evaluate the consequences of the ECJ decision on national data protection laws and practices, reminding them of the requirement to comply with the e-Privacy Directive and the Charter and to ensure "that there is *no bulk retention of all kinds of data* and that, instead, data are subject to appropriate differentiation, limitation or exception." National authority access to and use of data should be limited "to what is *strictly necessary*" and subject to "substantive and procedural conditions," and Member State laws "should provide for effective

44. *Id.* at para. 29 (citing Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 1, 10 (EC)).
45. *Id.* at para. 37.
46. *Id.* at para. 63.
47. *Id.* at para. 64.
48. *Id.* at para. 66.
49. *Id.* at para. 69.
50. *Id.* at para. 71.
51. *See* Press Release, Eur. Comm'n, Data Retention Directive: Commissioner Malström's Statement on Today's Court Judgment (Apr. 8, 2014), *available at* http://goo.gl/u11A1s.

protection against the risk of unlawful access" and other abuse. Finally, WP29 asked the Commission to provide guidance on the ECJ decision.[52]

Legislative Action on the Proposed Data Protection Framework

Since the Commission proposed a General Data Protection Regulation ("GDPR") on January 25, 2012,[53] committees of the Parliament have reviewed the proposal. Following such review, on March 12, 2014, the Parliament voted overwhelmingly in plenary session (621 votes for, 10 against, and 22 abstentions) for approval of the GDPR Compromise Text.[54] The Parliament's relatively swift approval may be a reaction to the Snowden NSA disclosures, as well as to the then-forthcoming May 2014 parliamentary elections.[55] The Council, through its working parties, also reviewed the proposed GDPR, although the Council has yet to establish common positions on many issues raised by the GDPR.[56] The Parliament and the Council must agree to the text of the GDPR on two successive readings for it to become binding and directly applicable in Member States,[57] but the GDPR would not become effective until two years after a date twenty days after publication in the Official Journal.[58]

Among other amendments to the GDPR, the GDPR Compromise Text would extend the territorial scope of the regulation to the processing of personal data in connection with the offering of goods or services (whether or not for payment) to data subjects in the EU, by either a controller "or processor," even if not established in the EU.[59] Under the GDPR Compromise Text, the requirement to

52. Article 29 Data Prot. Working Party, Statement on the Ruling of the Court of Justice of the European Union (CJEU) Which Invalidates the Data Retention Directive 2–3 (Aug. 1, 2014) (WP 220), *available at* http://goo.gl/MzSNij.

53. *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://goo.gl/D8Yxa. For an earlier discussion of the proposal, see W. Gregory Voss, *Survey of Recent European Union Privacy Developments*, 68 Bus. Law. 205, 210–13 (2012).

54. *See* Press Release, Eur. Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014), *available at* http://goo.gl/JszkAX.

55. *See* Voss, *supra* note 2, at 22.

56. *See id.* at 15–19 (discussing the legislative process in 2013); *see also* Katherine Ritchey et al., *Global Privacy and Data Security Developments—2013*, 69 Bus. Law. 245, 251–52 (2013) (discussing reaction to the GDPR, including amendments proposed by Parliament's Committee on Civil Liberties, Justice and Home Affairs, as well as negotiations between Parliament and the Council).

57. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 288, May 9, 2008, 2008 O.J. (C 115) 47, 171, *available at* http://goo.gl/Jc3StB ("A regulation shall . . . be binding in its entirety and directly applicable in all Member States."); Voss, *supra* note 2, at 15 (discussing the approval process).

58. *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)* art. 91, at 99, COM (2012) 11 final (Jan. 25, 2012), *available at* http://goo.gl/D8Yxa; *see* Voss, *supra* note 2, at 15 (discussing delayed effectiveness). This provision remains unchanged by the GDPR Compromise Text.

59. *See generally* Report by the Committee on Civil Liberties, Justice and Home Affairs 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 (General

designate a data protection officer would change to a more risk-based approach and would hinge on whether "the processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period," or, *inter alia*, whether "the core activities of the controller or the processor consist of processing special categories of data . . . , location data or data on children or employees in large scale filing systems."[60] The GDPR Compromise Text also provides a higher maximum level of administrative sanctions for data protection law violations: "up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher."[61]

Conclusion

During the past year, progress has been made on EU data protection legislative reform, driven in part by disclosures regarding NSA surveillance. Nontheless, much work remains to be done in the Council. EU privacy law concerns about surveillance also contributed to the invalidation of the Data Retention Directive. Meanwhile, a WP29 opinion on anonymization technologies and an analysis of the Google privacy policy enforcement action provide guidance to help businesses better understand and comply with EU privacy and data protection law.

Data Protection Regulation) amend. 97, at 63 (Nov. 21, 2013), *available at* http://goo.gl/IqWQgF (proposing amendments to article 3(1)–(2) of the GDPR). These amendments and those discussed below have been incorporated into the European Parliament legislative resolution of March 12, 2014, on the following proposal: *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.* COM (2012) 11 final (Jan. 25, 2012).

60. *Id.* amend. 132, at 121–23 (proposing amendments to article 35(1) of the GDPR).

61. *Id.* amend. 188, at 172–77 (proposing amendments to article 79(2) of the GDPR).