A Report on Recent Changes in European Union Privacy Law and Regulation

John C. Montaña

There have been two very recent developments in European privacy law that are likely to dramatically affect companies doing business in Europe, whether they are Europe–based on whether they are US–resident but offer services or goods in Europe.

The first of these was a decision on October 6, 2015 by the Court of Justice of the European Union (CJEU), invalidating the long-standing EU–US Safe Harbor agreement.[1] European Union privacy law generally restricts transfer of personal data about EU citizens to countries where there is not a similar level of protection in place. Since the United States is not a jurisdiction that offers a comparable level of privacy protection via legislation, the EU rules had the effect of preventing the transfer of data about EU citizens to the United States. The Safe Harbor Agreement was a widely used workaround employed by many companies to permit such transfers to occur. The mechanism for this was a yearly self-certification with the US Department of Commerce, in which the organization agreed to adhere to EU privacy principles and to adopt processes and safeguards which would effectuate that agreement. This self-certification would therefore be supplemented by policies, procedures, technical processes and other aspects of implementation so as to achieve compliance.

The decision of the CJEU was based upon a concern about large-scale access by United States intelligence agencies to data transferred to the US under the Safe Harbor agreement. The court therefore concluded that a US company could not guarantee an adequate level of protection for the personal data.

The net result of this decision was not the outright prohibition of transfer of personal data to the United States, but rather a ruling by the court that national data privacy authorities were not required to recognize the Safe Harbor Agreement, thus putting companies who relied upon it in the position of being uncertain as to whether a transfer to a third country would be legal or not. Although large multinationals that have entered into specific side agreements with EU authorities are unaffected by this, thousands of organizations that relied on the Safe Harbor Agreement as their primary or sole method of compliance with EU privacy law have been thrown into considerable uncertainty. As of this writing, there is

[1] Schrems v. Data Protection Commissioner, C-362/14 (Oct. 6, 2015).

no clear follow-on guidance. Presumably, a national authority can prohibit data transfers to the United States at any time, with no recourse by the affected organization.

The second development, which may or may not affect of the decision of the CJEU, was a tripartite agreement between the European Commission, the European Parliament and the European Council on the adoption of a common set of Europe–wide standards for data protection as part of a reform effort begun in 2012. The implementing regulations are expected to be adopted in early 2016.[2]

The stated goals of the reform are twofold: first, it establishes a uniform framework throughout the EU by which EU citizens can control access to and use of their personal data. second, it establishes "uniform" rules throughout the EU for businesses that collect, manage or process personal data, that are intended to remove bureaucratic obstacles and reduce costs in implementing privacy requirements.[3]

The Purpose and Scope of the Reform

The reform relies upon pre-existing Privacy Principles set forth in earlier EU directives and national legislation. The essential underlying concept of the Principles is that a person has a right of control over *all* of their personal data. Although directives or regulations may explicitly regulate parts of that personal data, it is all governed by the general principle of privacy and control. The original Principles recognized a need on the part of businesses, government agencies and others to collect and process personal data, but these needs were in conflict with the right of control and privacy exercised by the individual. Therefore, the doctrine incorporating a balancing test came into effect, in which in organization that collects or processes personal data must balance its need for the data against the rights of the individual whose data it is. As a practical matter, the rights of the individual were and are given great weight, thus creating a regime in which the ability of an organization to collect and use personal data is relatively restricted absent permissions from the individual in question.

The reform does not seek to revise the underlying doctrine or balancing test. Rather, it is explicitly intended to remediate the Balkanized system of regulation that has evolved over the years. For example, a business with employees in most or all of the EU countries has been faced with a wide variety of scenarios and restrictions on the collection and

---

[2] European Commission–press release; Agreement on Commission's EU data protection reform will boost Digital Single Market; Brussels, 15 December 2015.

[3] Id.; 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) , Brussels, 25.1.2012.

management of personal data about employees, ranging from a relatively hands-off approach in the United Kingdom to extremely detailed and prescriptive rules in places such as France and the Netherlands. Given the reality that much of this data is on a large computer systems that are unable to parse it on a jurisdictional basis, compliance with these jurisdiction–based rules has been problematic at best, impossible at worst. Added to this have been various bureaucratic hurdles such as required notifications to national data privacy authorities concerning proposed data collection and data processing activities.

The Substance of the Reform

The reform makes it clear that when the term "personal data" is used, that means *all* data about a person (the "data subject").[4] Likewise, the processing of data by an entity (the "data controller") must still comport with pre-existing principles, e.g., processing must be transparent and lawful; collected for specific and legitimate purposes and not used thereafter for other purposes; limited to the minimum amount of information necessary for the original purpose; accurate and up-to-date; if kept longer than the original purpose for scientific or other legitimate long-term purposes that it be de - identified; and that the controller is responsible and liable for the accurate implementation of these principles.[5]

At this point, the reform adds to prior practice by establishing explicit burdens and responsibilities:

- Data controllers bear the burden of proof concerning a data subjects consent to capture or process data;[6]
- Processing of data of children below the age of 13 years requires explicit parental consent;[7]
- Certain categories of personal data such as ethnic origin political matters, trade union membership and similar private information cannot be collected except under very specific circumstances;[8] and
- Use of personal data for profiling purposes is explicitly limited;[9] and organizations whose core activities revolve around personal data processing are required to have a data protection officer.[10]

---

[4] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) , Brussels, 25.1.2012, Art. 4.

[5] Id., Art. 6.

[6] Id., Art. 7.

[7] Id., Art. 8.

[8] Id., Art. 9.

[9] Id., Art. 20.

[10] Id., Art. 35.

The reform then goes on to establish a series of procedural mechanisms for the purpose of ensuring transparency on the part of the data processor, and accessibility by the data subject. So, the data processor must have "transparent and easily accessible policies" regarding data processing, and must use “clear and plain language"[11] in communicating with data subjects. The data controller must respond promptly, and at latest within a month recording requests by a data subject concerning the personal information.[12]

As can be seen from the above, attempted clarity isn't necessarily as clear as one would wish. Exactly what constitutes a "transparent and easily accessible" policy isn't entirely clear, at least at this point; nor is exactly what constitutes "clear and plain language." And it gets worse: article 13 states: “the controller shall communicate any rectification or erasure carried out in accordance with articles 16 [rectification of errors] and 17 [right to be forgotten] to each recipient to whom the data have been disclosed unless this proves impossible or involves a disproportionate effort." Again, what at first blush appears to be clarity is not so clear: the draft reform does not define what constitutes impossibility or disproportionate effort, and these are concepts that are likely to be the subject of some considerable dispute in practice. In practice, what this means is that a body of decisional law must build up over time as tribunals deal with these questions. Only then will we begin to have some understanding of what is meant by these terms.

Procedural Burdens on Data Processors

The reform imposes some very explicit demands on a data processor should the data subject choose to exercise their rights. Thus, the data subject has the right to obtain, and the data processor has the obligation to provide, detailed information about exactly what is being collected about the data subject, how and by whom it is being processed, the significance and envisaged consequences of the data processing,[13] corrections to the data asserted by the data subject,[14] the "right to be forgotten" should the data subject choose to exercise that right.[15], the right to receive a copy of any data that the data processor may have about the data subject,[16] and the right of the data subject to object to and prevent the use of personal data, absent specific proofs on the part of the data processor.[17]

Implementing policies and procedures are explicitly required.[18] Data capture processes and systems must be designed so that, by default, the only capture the minimum necessary

[11] Id., Art. 11.
[12] Id., Art. 12.
[13] Id., Art. 15.
[14] Id., Art. 16.
[15] Id., Art. 17. “The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data. . . .”
[16] Id., Art. 18.
[17] Id., Art. 19.
[18] Id., Art. 23.

data, and retain it only for the required period of time.[19] And, if the data are being processed by a third party on behalf of the controller, appropriate contractual language and technical implementations must be in place to ensure that the processor can perform all duties incumbent on the controller.

Data controllers are required to implement appropriate technical and operational measures to ensure the security of personal data, including the performance of risk evaluations.[20] In the event of a data breach, notification to the national supervisory authority is required within 24 hours.[21] If the data breach is likely to adversely effect the protection of the personal data or privacy of the data subject, the data subject must likewise be notified.[22]

In cases where the processing of personal data presents specified risks to the data subjects, the data controller is required to conduct a data protection impact assessment. The risks specified include:

- Analysis of data for predicting a person's economic situation, location, health, personal preferences, reliability or behavior and which may produce legal effects upon the person;[23]
- Information on sex life, health, race and ethnic origin for the provision of healthcare, epidemiological research, or surveys of mental or infectious diseases, where the data is processed for the purpose of making large-scale decisions; [24]
- Monitoring publicly accessible areas on a large scale;[25]
- Personal data in large systems on children, genetic data or biometric data;[26] and
- any other situation for which the national supervisory authority requires it after consultation.[27]

The scope and other details of the assessment are not specified in the reform document.

For most organizations, a good deal of this is not likely to be new. Much of it was previously in place in the form of a hodgepodge of existing directives, national guidance and other authority. The difference now is that it's in one place, organized as a coherent whole. As far as its effects, go, most organizations, particularly larger organizations,

[19] Id., Art. 24.
[20] Id., Art. 30.
[21] Id., Art. 31.
[22] Id., Art. 32.
[23] Id., Art. 33 (2)(a).
[24] Id., Art. 33 (2)(b).
[25] Id., Art. 33 (2)(c).
[26] Id., Art. 33 (2)(d).
[27] Id., Art. 33 (2)(e).

already have policies and procedures in place regarding privacy, and the implementation of privacy policy; and are at least considering ways to minimize data capture in the first place, so as to minimize the burden of privacy compliance. Other parts of it may or may not be burdensome depending on the organization, the amount and kind of data it captures, and what it does with that data. Thus, the right to be forgotten may have a heavy impact upon search engines such as Google, news sites and other similar operations, but may have very little effect on most organizations. Likewise, limitations on profiling using personal data may affect some classes of the controllers very heavily, but not impact others at all. Data privacy impact assessments are likely to be limited to a relatively narrow class of data controllers that do such profiling as part of their core business model, e.g. Google, Facebook and similar organizations; and research–based organizations that collect data for other analytical purposes.

Effects on Data Controllers Outside of the European Union

The Commission is charged with deciding whether third countries, or subdivisions within third countries, or international organizations ensure an adequate level of protection for personal data. [28]A list of such countries will be published in the Official Journal of the European Union.[29] If the Commission has concluded that an adequate level of protection is in place, transfers to that third country are authorized. If the Commission concludes that the third country does not have an adequate level of protection for personal data, transfers to that country are prohibited. [30] if the Commission has not taken a decision one way or the other respecting a particular country, data may be transferred to that country only if the processor commits to appropriate safeguards in a legally binding instrument such as binding corporate rules, policies containing the standard data protection clauses adopted by the Commission, policies containing standard data protection clauses adopted by a national supervisory authority, or contractual clauses containing appropriate protections between the controller in the recipient of the data that have been authorized by a national supervisory authority.[31]

Article 44 provides a specific list of circumstances under which data may be transferred even in the absence of the above controls, including fully informed consent by the data subject, performance of a contract between the parties, unspecified grounds of public interest, the establishment or defense of legal claims, or publicly available information.[32]

Organizations with more than 250 employees that are based outside of the EU must appoint a representative in the EU, unless the country that they are based in has ben determined by the EU to have an adequate level of protection for personal data.[33]

---

[28]Id., Art. 41 (3).

[29]Id., Art. 41(7).

[30]Id., Art. 41 (6).

[31]Id., Art. 42. *See also* Art. 43 concerning binding corporate rules.

[32]Id., Art. 44.

[33]Id., Art. 25.

The net result of these provisions should be relative certainty, and possibly much easier compliance, at least in those cases were a data transfer to a third country is not outright prohibited. The requirement for a representative within the EU obviously adds a layer of bureaucracy to the management aspect of compliance, but assuming that the representative need only deal with the national privacy authority in one country (for which, see below), that may prove worth whatever additional cost or burden is associated with having the representative, as compared with the current state of having to deal with privacy authorities in the various countries individually.

On the other hand, for data transfers to countries that are deemed by the EU to have inadequate levels of protection, the reform appears to be a real problem. The Safe Harbor Agreement provided a safety valve that permitted companies from the United States in other countries deemed not to have an adequate level of privacy protection to transfer data back and forth from Europe. The reform does not appear to contain any such safety valve, and thus poses a significant problem to such organizations. With the invalidation of the Safe Harbor Agreement, a great many such organizations are now potentially out of compliance with EU law, and therefore at risk of significant penalties. Restructuring systems and processes to become compliant (such as, for example by reconfiguring computer systems and adding servers, such that EU–origin data resides on EU–based servers, with appropriate protections to prevent data transfers to the United States) is likely to be a costly proposition for anyone forced to do so. And such a transformation could not be achieved very rapidly–it would likely take any organization a significant period of time to do such a reconfiguration of their systems and to conduct all the data transfers and data purges necessary to get everything in the right place.

The United States and the European Union are currently in discussions about a replacement for Safe Harbor, in the form a so-called Data Privacy Shield Framework, but this process is still in a very preliminary stage, As of this writing, there is no time frame for adoption, and indeed so assurances that an agreement can be worked out, And of course, as the Court's Ruling on Safe Harbor demonstrated, there is no guarantee that any such arrangement will withstand legal challenge.

The Role of National Data Privacy Authorities

Notwithstanding the goal of uniformity, national authorities will continue to exist under the new regime. And as in the prior scheme, they have considerable power and independence, including:

- Taking, investigating in ruling on the complaints by the subjects;[34]
- Conducting investigations on their own initiative or based on the complaint of another supervisory authority;[35]

[34] Id., Art. 52 (1) b).

- Advising State institutions and bodies on legislative and administrative measures regarding personal data protection;[36]
- Authorization of data processing operations of data controllers within its jurisdiction; [37]and
- issuing opinions and approval on draft codes of conduct, binding corporate rules and other data protection language.[38]

National Data Privacy Authorities will also have considerable enforcement power over data controllers. Among other things, they are empowered to enforce data privacy rules[39], suspend international data flows to third countries or international organizations[40] and order corrective actions when they determine it to be necessary.[41] And, they can impose penalties when they deem it appropriate to do so.[42]

There are some provisions concerning national authorities that are clearly beneficial to multijurisdictional organizations. So, rather than being answerable to multiple data privacy authorities in multiple countries, a data controller is now responsible only to the national authority in their primary jurisdiction.[43] That authority must now coordinate with the authorities and other jurisdictions relevant to the data controller to ensure that it is subject to reasonably consistent treatment throughout the EU. [44]This appears to be a considerable improvement over the previous patchwork treatment in different EU jurisdictions that organizations were previously faced with.

In like manner, the power of national authorities to engage in jurisdiction–specific regulation is constrained to some extent. Previously, national data privacy authorities were authorized to create and enforce rules for data controllers in their jurisdiction, regardless of the conformity or lack thereof of those rules to rules in other jurisdictions in which the controller might do business. This often resulted in a plethora of rules that often could not be complied with because they conflicted with each other.

Now, although national authorities are empowered to enact rules within their jurisdiction, those rules must be vetted by the European Data Protection Board and the Commission

---

[35]Id., Art. 52 (1) (d).
[36]Id., Art. 52 (1) (f).
[37]Id., Art. 52 (1) (g).
[38]Id., Art. 52 (h) & (i).
[39]Id., Art. 53 (1) (b).
[40]Id., Art. 53 (1) (h).
[41]Id., Art. 53 (1) (e) & (f).
[42]Id., Art. 53 (1) (#)
[43]Id., Art. 50.
[44]Id., Art. 55 (1).

prior to adoption.[45] The Data Protection Board may issue an opinion on the matter, which the commission may adopt, determining whether the proposed rule affects certain key areas such as free movement of information within the EU. [46]Prior to finalizing and adopting its proposed rule, the national authority must consider the opinion and adjust its proposed rule accordingly.[47] If it elects not to make revisions based upon the opinion, it must notify the Commission and provide a justification.[48] If the parties cannot agree on the final rule, the Commission is authorized to suspend implementation of the rule for up to one year. [49]The stated purpose of this process is to develop and enforce consistent rules, and consistent enforcement of rules throughout the EU.[50]

One thing that experience in the law teaches is that, if there are multiple authorities that have jurisdiction, uniform laws tend to become un - uniform over time. Although the reform requires that national authorities cooperate, and although the reform likewise requires the submission of proposed national rules to the Data Protection Board and the Commission for vetting, at the end of the day, the ability to force a national authority to conform to the consistency regime proposed by the reform is limited. If a national authority decides to promulgate a rule significantly at variance with norms determined by the Board and Commission, the most that the Commission can do is suspend implementation of the rule for a year. It cannot actually stop it. Given this limitation on the authority of the Commission, and also given the very active nature of some national commissions such as those in France, Germany and the Netherlands, it is very likely to be the case that national rules in these and perhaps some other jurisdictions will continue to be very prescriptive and out of step with the rules in other EU jurisdictions. This will, in turn, create a continuation of the current problems that organizations have with Balkanized rulemaking resulting in different and not necessarily compatible rules in the different jurisdictions within the EU, and all of the resulting compliance headaches that come with this.

Where Does This Leave Us?

The reform offers at least the hope of more consistency and certainty in privacy compliance in the EU. However, it will be preceded by a period of considerable uncertainty. As noted above, some of the language is vague enough that it will require judicial interpretation before organizations can gain a high level of confidence as to exactly what it means. Likewise, the consistency and cooperation mechanism that is intended to instill uniformity upon the actions of the national authorities is vague enough and general enough that its

[45]Id., Art. 58 (1).
[46]Id., Art. 58 (2).
[47]Id., Art. 58 (8).
[48]Id., Art. 59 (4).
[49]Id., Art. 60 (2).
[50]Id., Art. 57.

application in practice is uncertain, at least for now. And we do not know how the national authorities are going to respond to EU demands for consistency. If past practice is any indication, the hopes for that are not good, but we cannot know until the whole regime has been in place for a considerable period of time and we are able to observe exactly how these as yet untested concepts and processes play out in real life. And we have yet to have any real indication of exactly what, if anything, will ultimately replace Safe Harbor.

The current document is likely to be supplemented with additional guidance as time goes on. If that guidance comes out in the short-term, it may be extremely beneficial. A great many organizations are undoubtedly looking for that guidance, particularly as it relates to data transfers between the United States and the EU.

So, at the moment we are in a holding pattern. The reform sets forth a new approach, but that approach is untested, and many details of it and its operation have yet to be worked out.

Contact the author at:

jcmontana@montana-associates.com
610-255-1588
www.montana-associates.com

Follow him on twitter at @johnmontana