EU Personal Data Protection Laws Require Deleting Data When No Longer Needed

By James M. Jordan III[1]

September 12, 2006

In 1995 (little more than a year after the EU was formed in November 1993), the **EU Personal Data Protection Directive (EUDPD)**[2] was enacted. It declared that personal data protection was a "fundamental human right." The EUDPD required national implementation in each Member State by October 1, 1998. When 10 new countries joined the EU in May 2004, they already had data protection laws that were roughly in line with the Directive.

Looking at the data protection laws that are currently in place at the national level, 18 of the 25 EU Member States (and 22 of 29 EFTA states) make violations punishable by **jail terms** ranging from 1 to 10 years.[3] These have occasionally been imposed in serious cases.[4] All EU and EEA Member States provide for **fines,** ranging from fairly small amounts to "unlimited."[5] It is difficult to get information about actual fines as they are often not officially publicized, but the three largest known fines have been in Spain (with

---

[1] Jim Jordan is the founder of Jordan Legal, P.C., assisting companies with compliance programs and laws pertaining to personal data protection, technology, advertising, IP and e-commerce. He is a Certified Information Privacy Professional (CIPP) and a member of the CIPP Advisory Board of the Intemational Association of Privacy Professionals (IAPP). Until December 2005, he was the Chief Privacy Leader and Senior Counsel for E-Commerce & Information Technology of General Electric Company, responsible for global privacy law compliance. Prior to GE, he was a partner in the Intellectual Property Group of Alston & Bird, LLP. He received both a B.S. degree in Physics and a J.D. from the University of Georgia, and served on active duty for seven years as a U.S. Navy nuclear submarine officer. He can be reached via email at jimjordan3@comcast.net or via telephone at 770.921.2631.

[2] See "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," which may be found online at http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett. The EUDPD established a floor for privacy protection, but national laws in some cases exceed the Directive's base requirements (e.g., France's broad requirement of "prior checking" by the DPA, Germany's requirement to appoint Data Protection Officers, and Spain's requirement to get employee consent before exporting sensitive data).

[3] See Data Protection Legislation in the European Union 2005 at 4, http://www.linklaters.com/publications/pubdetail.asp?publicationid=1620&IssueID=. The following countries do not have a jail term punishment for data protection violations: Potential jail terms include: 10 years (Greece), 5 years (Cyprus, France), 3 years (Czech Republic, Hungary, Iceland, Italy, Norway, Poland), 2 years (Belgium, Finland, Germany, Portugal, Sweden), 1 year or less (Austria, Denmark, Liechtenstein, Luxembourg, Malta, Netherlands, Slovenia, Switzerland), No jail terms (Spain, UK, Ireland, Slovakia, Estonia, Latvia, Lithuania).

[4] Id. At 5. In Sweden, a 2 year jail term was imposed. In Switzerland, there have been at least 5 criminal convictions, one including a one-year jail term. In the Netherlands, a one year suspended sentence was imposed in September 2004 in the case of an information agency (Bureau X) that was gathering personal data fraudulently from illegal sources.

[5] Id. At 5. Potential fines are: Unlimited (Denmark, Finland, Germany, Iceland, Italy, Liechtenstein, Norway, Sweden, UK), 600,000 euros (Spain), 500,000 euros (Belgium), 200,000-400,000 euros (Czech Republic, France, Slovakia, Slovenia), 100,000 euros (Ireland, Luxembourg, Poland), <100,000 euros (Austria, Cyprus, Estonia, Greece, Hungary, Latvia, Malta, Netherlands, Portugal, Switzerland).

the largest over 1 million euros),[6] and serious fines have also been handed out in Greece, and to a lesser extent in the Czech Republic, France, Netherlands and Portugal, among others.

In practice, Data Protection Authorities (DPAs) have to date mostly worked behind the scenes, resolving cases with companies without publishing their decisions and outcomes, or publishing the decisions without providing the names of the parties. It is, therefore, difficult to get a clear picture of how severe enforcements and punishment have been. However, monetary fines seem to be the most common punishment, particularly in some countries (e.g., those mentioned in the paragraph above). In addition, DPAs in Europe (e.g., France, Belgium, UK) have used **public reprimand** against companies by issuing harsh statements about their business practices. These public rebukes and the significant unwanted publicity that follows often have a larger financial impact on a company than a fine.

The EUDPD regulates a broad category of **"personal data"** which is defined as **"any information relating to an identified or identifiable natural person ('data subject')."**[7] A **"natural person"** is a human being, as opposed to a "legal person" such as a corporation.[8] An **"identifiable"** person is one who "can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[9] EUDPD Preamble section 26 recites: "whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." Data may be deemed "identifiable" to a person if the person can be identified by cross-reference to other data in the database, or to data in a second database that is available to someone who has access to the first database, so (for example) merely replacing names with unique ID numbers in the first database will not be enough to make it unregulated if someone with access also has access to a database enabling them to identify the names with the unique ID numbers.[10] Thus, the EUDPD regulates data that can be identified to a person, even if it is not particularly sensitive or private (such as name, address and telephone information that is publicly available on a website or in a phonebook), and

---

[6] Id. At 5. The Spanish DPA imposed a fine of over 1million euros on Zeppelin, the producer of a reality television show that allowed Internet hackers to obtain personal data about 1,700 potential contestants on the show. It also imposed a fine of 420,708 euros on Telefonica, a telecom company that had disclosed some personal data to an affiliate for marketing purposes without the consent of the data subject.

[7] EUDPD Art 2(a).

[8] However, it is noteworthy that at least 4 countries (Switzerland, Austria, Italy and Luxembourg).go beyond the requirements of the EUDPD and extend personal data protection to data identifiable to "legal persons" as well. This has fortunately not been rigorously enforced. EUDPD Preamble section 24 recites: "Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;…."

[9] EUDPD Art. 2(a).

[10] EUDPD Preamble section 26 recites: "whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"

even if the data was collected in the context of a business-to-business transaction rather than a consumer or employee transaction.[11]

Regulated personal data includes data that is processed "wholly or partly by **automatic means**," and data processed "otherwise than by automatic means" that "forms part of a filing system or are intended to form part of a **filing system**."[12] This does not leave much out, except for data on paper that is not kept in any sort of organized way that would allow it to be manually searched. In other words, a box of documents kept in alphabetical order would likely be considered a "filing system" and therefore regulated, whereas a box of documents in kept randomly might not be.[13]

Regulated personal data normally does not, however, include: (1) data that is **"anonymous**" (names removed and data is not otherwise "identifiable" to the persons);[14] (2) data that is **"aggregated"** (summarized for a group in such a way that it is not identifiable to an individual); (3) data identifiable to persons who are **no longer living**, (4) data being processed by a natural person in the course of a purely **personal or household activity**, or (5) processing operations concerning **defense, public security, Member State security**, or Member State activity in areas of **criminal law**.[15]

The basic requirements of the EUDPD are:
(1) Fairness & Lawfulness, (2) Purpose Specification, (3) Relevance, (4) Accuracy & Currency, (5) Deletion or De-Identification, (6) Security, Confidentiality & Vendor Management, (7) Notice to the Data Subject, (8) Consent of the Data Subject (or establishing another legitimate basis for processing), (9) Data Subject's Right to Object to Processing, (10) Data Subject's Rights of Access, Rectification, Erasure, & Blocking, (11) Limits on Automated Decisionmaking, (12) Works Council Notifications and Approvals, (13) DPA Notifications and Approvals, (14) Maintaining a Controller Register, (15) Requirements for Cross-Border Transfers, and (16) Staffing and Governance Requirements. This article will briefly focus on deletion and de-identification and the data subject's right to object to processing.

---

[11] EUDPD Preamble section 30 recites: "whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies;…." However, DPAs regularly interpret personal data shared by or about a person in his role as a company representative as regulated personal data.

[12] EUDPD Art. 3. (c). "Personal data filing system" (or "filing system") means "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." EUDPD Art. 2(c).

[13] EUDPD Preamble section 27 recites: "whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data;…."

[14] EUDPD Preamble section 26 recites: "whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable;

[15] EUDPD Art 3.

Deletion or De-Identification

EUDPD Art. 6(1)(e) requires that personal data be "kept in a form which permits identification of data subjects for **no longer than is necessary for the purposes for which the data were collected** or for which they are further processed." This means that personal data must either be deleted or "de-identified" in some way once it is no longer necessary to retain it for the original purpose. Companies should have **document retention policies** (for many reasons other than just personal data protection laws) and should include retention periods for records containing personal data in those policies.

Data Subject's Right to Object to Processing.

The data subject be extended an "opportunity to object to processing" under Article 14, which operates similarly to an "opt out" form of consent. For processing for the purposes of **direct marketing**, data subjects must be given an opportunity "to object, on request and free of charge," to such processing or (if they prefer) to ask to be "informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses." The data subject may opt-out of direct marketing without meeting any particular standard of scrutiny for his objection.

For processing for purposes **other than direct marketing**, the data subject must be extended the opportunity to object at any time, but the objection will only be considered "justified" if the data subject has **"compelling legitimate grounds** relating to his particular situation," in which case the controller must stop the data processing that is the subject of the justified objection. Since "processing" includes "storage," this may require "blocking" of access to the data or even "erasure" of the data. There is little guidance from the DPAs at this point as to what may constitute "compelling legitimate grounds."

For these reasons, it is important, particularly for personal data collected in the EU, to have a means of deleting data from your systems.