



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 07, No. 44, 11/10/2008, pp. 1615. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

EU Data Protection

Proportionality Principle

Every company needs to pay close attention to the proportionality principle when considering its compliance with European data protection law. The paucity of explicit references to proportionality in data protection legislation may give the misleading impression that it is of little importance. In fact, proportionality is recognized as a fundamental principle of EU law. The bright side to the challenges the proportionality principle poses for companies is that since the principle is so fundamental, attention to complying with it can actually reduce other compliance burdens, the author writes.

Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies

By CHRISTOPHER KUNER

Many important issues of European data protection law are determined by application of general legal principles that may not be fully apparent to companies that have to apply them in practice. One of the most important such principles is that of proportionality, and its application has frequently led to decisions by courts and data protection authorities with

significant implications for data processing by companies. An understanding of the proportionality principle is thus of fundamental importance for companies that process personal data in the European Union (the EU).

I. Background

Proportionality is referred to only a few times in the text of the EU Data Protection Directive 95/46/EC¹ and

Christopher Kuner is a partner in the Brussels law offices of Hunton & Williams. He can be reached at ckuner@hunton.com.

¹ Directive (EC) 95/46 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 [1995] OJ L281/31. For example, Article 11(2) states that information about data processing need

the Directive on Privacy and Electronic Communications 2002/58,² as well as in the EU Data Retention Directive 2006/24.³ The paucity of explicit references to proportionality in data protection legislation may give the misleading impression that it is of little importance. In fact, proportionality is recognized as a fundamental principle of EU law,⁴ and is even mentioned explicitly in the Treaty on the European Union.⁵ It is also a basic principle of human rights law under the European Convention on Human Rights,⁶ and the European Court of Human Rights routinely uses proportionality as a criterion for determining whether data processing is legal.⁷ The European Court of Justice has also applied the proportionality principle in relation to data protection,⁸ and proportionality is applied by courts at the Member State level as a basic principle of national constitutional and administrative law.⁹ Thus, the principle is broadly

not be given in the context of data processing for statistical purposes or for the purposes of historical or scientific research when the provision of such information “proves impossible or would involve a disproportionate effect”; and Article 12(c) limits the duty to notify third parties to whom data have been disclosed of any rectification, erasure, or blocking of the data when such notification “proves impossible or involves a disproportionate effort.”

² Directive (EC) 2002/58 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 [2002] OJ L201/37. For example, Article 3(2) states that the Directive applies to subscriber lines connected to analogue exchanges “where technically possible and if it does not require a disproportionate economic effect”; and Article 15(1) allows Member States to restrict the scope of certain rights and obligations “when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society” to safeguard certain important interests (such as national security, defence, etc.).

³ Directive (EC) 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 (EC) 2002/58 [2006] OJ L105/54, which mentions the proportionality principle in Recital 25 and Article 4.

⁴ See C. Calliess and M. Ruffert, *Kommentar des Vertrages über die Europäische Union und des Vertrages zur Gründung der Europäischen Gemeinschaft* (Luchterhand 2002) 399-400.

⁵ Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2008] C-115/01. Article 5(4) of the Treaty reads: “Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties. The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality.”

⁶ C. Grabenwarter, *Europäische Menschenrechtskonvention* (C.H. Beck 2005) 110.

⁷ See, e.g., *Leander v. Sweden*, Judgment of 26 March 1987, Series A, no 116, ECHR, finding that there was no breach of the proportionality principle and the European Convention on Human Rights when the Swedish government refused employment to the petitioner based on his being listed in a secret police register.

⁸ See, e.g., *Productores de Música de España (Promusicae) v Telefónica de España SAU* (C-275/06) [2007] E.C.D.R. CN1; C-138/01 *Rechnungshof* [2003] ECR I-6041.

⁹ For example, in Belgium (see Cour d'arbitrage, arrêt no. 16/2005, 19 janvier 2005), France (see Cour de cassation, Ch. soc., 11 décembre 2001, no. 99-43.030), and Germany (see Bundesverfassungsgericht, Urteil vom 15.12.1983, BVerfGE 65, 1).

applicable to many areas of EU and Member State law, including data protection law, even if it is not mentioned in a particular statute or regulation.

In the context of EU law, applying the proportionality principle entails a two-part assessment of 1) whether the means employed by the measure to be evaluated are suitable and reasonably likely to achieve its objectives; and 2) the adverse consequences that the measure has on an interest worthy of legal protection and a determination of whether those consequences are justified in view of the importance of the objective pursued.¹⁰ However, application and interpretation of the proportionality principle can differ between the Member States.¹¹ Lord Diplock memorably summarized the principle as it is applied in English law as follows: “In plain English, it means ‘You must not use a steam hammer to crack a nut, if a nutcracker would do’”.¹² German law (upon which the proportionality principle in EU law seems to be based¹³) applies a three-part test based on the criteria of suitability (*Geeignetheit*), i.e., whether the measure in question can fulfil the desired purpose; necessity (*Erforderlichkeit*), i.e., whether another less intrusive measure cannot fulfil the desired purpose with equal effectiveness; and appropriateness (*Angemessenheit*), i.e., whether the measure in question stands in a reasonable relationship to the intrusions it will cause.¹⁴

In data protection law, the proportionality principle may be applied in two ways: (1) as an element of another provision, principle, or rule, or (2) as a fundamental principle underlying all data protection law. It can be difficult in practice to differentiate these two possible applications of the principle, and in their decisions, the courts and data protection authorities may not make it entirely clear whether they are evaluating the proportionality of data processing as part of some other concept, or as a fundamental concept in itself.

Whenever a company processes personal data, proportionality is lurking in the background and may cause the processing to be found illegal if it is not taken into account when structuring compliance with data protection law.

With regard to (1), proportionality is often articulated as a component of other data protection rules. For example, the Article 29 Working Party (the group of data protection authorities from all EU Member States)

¹⁰ T. Tridimas, *The General Principles of EU Law* (Oxford University Press 2007) 139.

¹¹ See, e.g., A. van Arnauld, ‘Theorie und Methode des Grundrechtsschutzes in Europa—am Beispiel des Grundsatzes der Verhältnismäßigkeit’ (2008) *Europarecht* 41 Beiheft 1, analyzing differences in the proportionality principle in English, French, and German law.

¹² *Regina v. Goldstein* [1983] WLR 151, HL.

¹³ See E. Pache, ‘Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung der Gerichte der Europäischen Gemeinschaften’ (1999) *Neue Zeitschrift für Verwaltungsrecht* 1033, 1035-36.

¹⁴ *Id.* 1036.

tends to apply the principle in terms of the criteria of Article 6(1)(c) of the EU Data Protection Directive (which states that personal data must be “adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed”). The principles of “legality”¹⁵ and “purpose limitation”¹⁶ contained in the Directive seem to include within them the concept that the processing be proportionate, and proportionality seems to underlie some other provisions of the Directive as well.¹⁷ Proportionality has also led to creation of the concept of “data minimisation,” meaning that the processing of personal data must be restricted to the minimum amount necessary.¹⁸

¹⁵ Article 6(1)(a), providing that personal data must be “processed fairly and lawfully”.

¹⁶ Article 6(1)(b), providing that personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”. See L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002) 58.

¹⁷ See E Ehmann and M Helfrich, *EG Datenschutzrichtlinie* (Verlag Dr. Otto Schmidt 1999) 124, 194, mentioning Articles 7(d)-(e) and 13(1) as containing the principle of proportionality.

¹⁸ See, e.g., § 3a of the German Federal Data Protection Act.

With regard to (2), proportionality is an underlying principle of the law which applies even if other explicit statutory requirements have been satisfied. Even if a company complies with all explicit statutory data protection requirements, its data processing may still be found illegal if it violates the underlying, fundamental principle of proportionality, even if the relevant data protection legislation does not explicitly mention the principle. Thus, whenever a company processes personal data, proportionality is lurking in the background and may cause the processing to be found illegal if it is not taken into account when structuring compliance with data protection law.

II. Application of the Principle in Practice

Perhaps the best way to understand the impact of the proportionality principle on data processing by companies is to examine some cases decided by European data protection authorities (DPAs) and papers they have issued which apply the principle to real-world data processing situations. The following are a few selected examples of decisions and papers issued by the Article 29 Working Party which have cited proportionality as a key factor in evaluating the legality of a specific instance of data processing:

Title	Date	Examples
Working document on privacy on the Internet (WP 37)	November 21 2000	In electronic transactions, only data which are required for the transaction should be collected.
Opinion 8/2001 on the processing of personal data in the employment context (WP 48)	September 13 2001	Employers should always process personal data in the least intrusive way considering the risks at stake, the amount of data involved, the purpose of processing, etc. For example, employers may need to know (for certain posts) if applicants have a car and a driver's license, but it would be disproportionate to ask for the model or the color of applicants' cars.
Working document on the surveillance of electronic communications in the work-place (WP 55)	May 29 2002	Before being implemented in the work place, any monitoring measure must pass a list of tests, which are summarized by the following questions: <ul style="list-style-type: none"> o Is the monitoring activity transparent? o Is it necessary? Could not the employer obtain the same result with traditional methods of supervision? o Is the proposed data processing fair? o Is it proportionate to the concerns that it tries to allay? The proportionality principle rules out blanket monitoring of individual e-mails and Internet use of all staff other than where necessary for the purpose of ensuring the security of the system. Where the identified objective can be achieved in a less intrusive way, the employer should consider this option. Employers should avoid systems that monitor automatically and continuously.
Working document on the processing of personal data by means of video surveillance (WP 67)	November 25 2002	While a proportionate video surveillance and alerting system may be considered lawful if repeated assaults are committed on board buses in peripheral areas or near bus stops, this is not the case with a system aimed either at preventing insults against bus drivers and the dirtying of vehicles, or else at identifying citizens liable for minor administrative offences.
Opinion 1/2003 on the storage of traffic data for billing purposes (WP 69)	January 29 2003	Traffic data may be kept for as long as necessary to enable bills to be settled and disputes resolved. Ordinarily this involves a maximum storage period of 3-6 months and no longer in cases where bills have been paid and do not appear to have been disputed or queried. In addition, only data that are adequate, relevant and not excessive in relation to billing and interconnection payments purposes may be processed. This implies inter alia that if there is no billing for certain types of communications, no traffic data may be processed for these purposes.

Title	Date	Examples
Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes (WP 117)	February 1 2006	Taking the proportionality principle into account, the nature and seriousness of the alleged offence should in principle determine at what level, and thus in what country, assessment of the whistleblowing report should take place.
Opinion 2/2006 on privacy issues related to the provision of email screening services (WP 118)	February 21 2006	The Working Party encourages developers of e-mail software to devise and develop privacy compliant systems in such a manner as to reduce the processing of personal data to the minimum.

From these examples, it can be seen that the proportionality principle may be applied even if it is not referred to by name. In particular, claims that “excessive” amounts of personal data are being processed, or that data processing is not “relevant” or “necessary,” are signals that the principle is being applied.

There are also many decisions of national data protection authorities which are based at least in part on the proportionality principle. For example, in one case, the Berlin Commissioner for Data Protection and Freedom of Information decided that the proportionality principle limited the ability of a company to create a database for the retail sector containing information about actual and suspected criminal violations by employees.¹⁹ The Commissioner found that it was disproportionate to include information in the database that was not based on formal determinations by criminal law authorities. In another case, the Spanish Data Protection Authority issued an instruction for the use of video surveillance, finding that, based on the principles of proportionality and purpose limitation, cameras and video-cameras installed in private spaces should not obtain images of public spaces except if it is indispensable for the surveillance purpose intended, or if their location makes it impossible to avoid it.²⁰ And in a third case, the Austrian Data Protection Commission approved the transfer of employee data outside the EU by a company, after analyzing the transfer under the proportionality principle.²¹ These are just three of many examples of such DPA decisions and recommendations applying the proportionality principle to data processing by companies.

In these examples, there tend to be common threads that result in data processing being found illegal based on the proportionality principle:

- *An imbalance between the interest of the company in processing personal data on the one hand and that of the individual in not having his data processed on the other hand.* In many of these cases, the interference with the rights of the individual caused by the data processing may be much higher than the interest of the company in processing the data.
- *The excessive processing of personal data.* The amount or the extent of the personal data processed may be relatively high, and may be out of relation to the purposes for which they are used.

¹⁹ Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2005, 176-78.

²⁰ Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

²¹ Datenschutzkommission, Bescheid Beschwerde, no. K178.240/0006-DSK/2007, 23 May 2007.

- *Processing that goes beyond the purpose for which the data were collected.* The data may be processed for purposes that are not strictly limited to those for which the data were originally collected.
- *No clear showing that the data processing is truly necessary.* It may not be clear that the data processing is truly necessary to fulfill the desired purpose, or that there is not some other way to do so which would result in less interference with individuals’ data protection rights.

III. Conclusions

The proportionality principle is not explicitly mentioned in most data protection statutes, and many companies may not be aware that it exists. Moreover, as a fundamental legal principle of broad application, it can be difficult for a company to know exactly how to satisfy the principle. Finally, companies are often used to thinking of data protection compliance in terms of satisfying a well-defined set of statutory requirements, and may find themselves at a loss in interpreting a broad legal principle which is not explicitly mentioned in the applicable data protection legislation.

However, there are some steps that companies can take in structuring their data processing in order to minimize the chance that they will run afoul of the proportionality principle:

- *Consider proportionality early in the planning process.* Because the proportionality principle is a fundamental legal principle which underlies data protection law, a violation of it can be difficult to remedy, and can ultimately result in the data processing in question being found illegal. Thus, it makes sense to consider proportionality from the moment when a particular database or data processing activity is first being planned, rather than later on when it may be too late to correct any problem.
- *Limit the amount of personal data being processed to what is truly necessary.* There is often a tendency for a company to collect more personal data than it may need to realize a particular project, on the theory that it might need the data for some purpose in the future. While this attitude may be understandable, it carries with it a number of legal risks. Besides the extra liability that storing and processing the data may bring (for example, in case of unauthorized access of the data following a security breach),²² the collection of more personal data than is needed to fulfill the purpose for which

²² See regarding security breaches C. Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press 2007) 288-297.

data are to be processed is always a warning sign that there may be a potential issue under the proportionality principle.

- *Limit the processing of data to the original purposes for which they were collected.* Many issues under the proportionality principle arise because the company uses the data for purposes that go beyond those for which they were originally collected. It is thus highly advisable for a company to take two steps before personal data are processed: (1) have a clear conception of the purposes for which the data are collected and processed, and (2) develop procedures to ensure that the data are processed only in accordance with such purposes. For example, if a database is established to manage customer orders, then it should not be used to send marketing to customers unless a prior evaluation has been made and steps are taken to ensure the legality of such usage.
- *Consider whether there are other means of realizing the same end which would result in less processing of personal data.* It may be possible to realize the purpose of the data processing by means that are less intrusive than originally planned. For example, if a company is planning to collect so-called “sensitive data” (meaning personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life under Article 8 of the EU Data Protection Directive), then it is always worthwhile to consider whether collection or processing of the data is truly necessary; sometimes this may not be the case, and it may be possible to realize the same purpose without the extra risk of processing such data. In addition, the anonymization or pseudonymization of

personal data can reduce the risk of violating the principle of proportionality.

There are a number of areas of data processing where the risk of legal problems caused by application of the proportionality principle can be particularly high, such as the following:

- data transfers to countries outside the European Union;
- the processing of sensitive data, including the data of children;
- the processing of employee data;
- video surveillance;
- the use of biometrics; and
- the large-scale collection of data over the Internet.

The above list is non-exclusive, and just indicates some areas where problems based on proportionality tend to arise most frequently.

There is a bright side to the challenges that the proportionality principle poses for companies, which is that since the principle is so fundamental, attention to complying with it can actually reduce other compliance burdens. For example, by ensuring that data collection and processing are proportionate, it is less likely that a company would be found to breach the principles of legality or purpose limitation. Indeed, paying attention to proportionality when structuring a data processing project can also give valuable insights into other compliance issues, and thus allow a company to “front-load” its compliance by detecting and dealing with issues early on in the process when they are easier to deal with. Thus, although complying with the proportionality principle can be challenging, it can also result in more efficient data protection compliance, and actually save money and effort over the long run. Every company needs to pay close attention to the proportionality principle when considering its compliance with European data protection law.