Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?

Stephen A. Oxman

Follow this and additional works at: http://lawdigitalcommons.bc.edu/iclr

Part of the European Law Commons, and the Internet Law Commons

Recommended Citation
http://lawdigitalcommons.bc.edu/iclr/vol24/iss1/8

This Notes is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College International and Comparative Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.
EXEMPTIONS TO THE EUROPEAN UNION PERSONAL DATA PRIVACY DIRECTIVE: WILL THEY SWALLOW THE DIRECTIVE?

STEPHEN A. OXMAN

Abstract: This Note analyses the probable effectiveness of the European Union Data Protection Directive, which was passed in order to curtail the invasion of personal privacy that has accompanied the development of the Internet, in light of three potentially expansive exemptions contained within the Directive. The author concludes that the goals of the Directive will be achieved only if Member States interpret these exemptions restrictively when enacting legislation pursuant to the Directive.

INTRODUCTION

"Personal data" is any information relating to an identifiable person.1 It includes both basic factual information pertaining to an individual's identity, such as his or her name, address, and social security number, and information revealing an individual's personal preferences, such as records of purchases or visits to websites.2 The processing and exchange of personal data has increased dramatically due to rapidly advancing technological resources, such as the Internet.3 This technology has been a boon to entities such as direct marketers, journalists, and law enforcement officials, who rely on acquiring this information in order to achieve their objectives.4

The widespread access to personal data facilitated by new technology increasingly has been viewed as a serious threat to personal privacy.5 The European Union (EU) Directive on the Protection of

---


3 See Directive, supra note 1, rec. 4.


Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (the Directive), which came into effect on October 24, 1998, represents the first major international legislative effort to curtail this intrusion.6

At the time the Directive was passed, some individual European countries, such as Germany, already had passed their own legislation regulating the processing of personal data.7 Disparities among these various regulations, however, created potential obstacles to the free flow of personal data among Member States.8 The purpose of the Directive, therefore, was to create EU-wide privacy rights that would remove those obstacles and harmonize the transfer of personal data within the EU.9

The Directive is designed to regulate the collection, storage, use, and dissemination of personal data.10 It embraces the right to privacy as a fundamental right and seeks to give the individual control over the distribution of his or her personal data.11 The Directive provides data subjects with a number of rights with respect to their personal data, including: (1) the right of access to data;12 (2) the right to withhold permission to use data;13 (3) the right to have inaccurate data rectified;14 and (4) the right of recourse in the event of unlawful processing of data.15 The Directive also provides that personal data may not be transferred to third countries unless the recipient country is deemed by the European Commission (Commission) to have adequate privacy laws.16 The Directive directs Member States to adopt their own legislation implementing the provisions of the Directive,17 and to create their own supervisory bodies to monitor the application of the laws adopted pursuant to the Directive.18

Although the Directive provides comprehensive protection for personal data privacy, it also recognizes that “[t]here must be a bal-

---

7 See Murray, supra note 5, at 933–34.
8 See Directive, supra note 1, ref. 7.
9 See id., rec. 8.
10 See Murray, supra note 5, at 942.
11 See Directive, supra note 1, ref. 2.
12 See id., art. 12.
13 See id., art. 14.
14 See id., art. 6.
15 See id., art. 22.
16 See Directive, supra note 1, art. 25.
17 Id. art. 32.
18 Id. art. 28.
ance between the right to be let alone and the legitimate interests of a society." Therefore, the Directive exempts from its reach the processing of personal data when the societal interests in that data outweigh the subject's interest in personal privacy. When personal data are processed for certain enumerated purposes, the Member States may permit derogation from the strict privacy requirements of the Directive. Many of these exemptions were drafted in broad terms in order not to infringe on the abilities of the Member States to legislate in the interests of their citizens.

The Directive specifically states the legislature's intent to give Member States a "margin for manoeuvre" when implementing their own personal data privacy legislation. This "margin for manoeuvre" has the potential to undermine effective enforcement of the privacy principles on which the Directive is based. In addition, the derogations that Member States are allowed to permit under the Directive potentially could undermine the Directive's goal of harmonization of data privacy laws in the EU.

This Note focuses on the shortcomings in three categories of exemptions enumerated in the Directive. Part I of this Note examines the category of exemptions contained in Articles 3(2) and 13, which exempt from the scope of the Directive all activity falling "outside the scope of Community law," such as actions necessary to safeguard national security or actions pertaining to criminal proceedings. Part II focuses on the Article 13(2) exemptions, which exempt activities that are conducted solely for research purposes. Part III considers Article 26, which contains exemptions from Article 25.

23 See Directive, supra note 1, rec. 9.
24 See Simitis, supra note 22, at 451 (arguing that political pressures for accommodating existing laws in the Member States pose a threat to a high level of protection).
25 See Directive, supra note 1, rec. 9 ("within the limits of this margin for manoeuvre ... disparities could arise in the implementation of the Directive").
26 Id. arts. 3(2), 13.
27 See id. art. 13(2).
28 See Cate, supra note 6, at 437.
the most controversial provision of the Directive, prohibits Member States’ firms from transferring personal data to third countries that lack adequate privacy laws. Article 26 exempts parties from Article 25 if the transfer is pursuant to a contract or if the transferor adduces adequate safeguards by the transferee. Following a description of each of these exemptions, this Note suggests ways that Member States should interpret and implement these exceptions so as to avoid subverting the goals of the Directive.

I. Article 3(2) Exemption

The most sweeping exemption to the Directive is contained in Article 3(2), which states that the Directive “shall not apply to the processing of personal data . . . in the course of an activity which falls outside the scope of Community law.” These activities, according to the Directive, include “processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters), and the activities of the State in areas of criminal law.” While these examples give some guidance as to what types of personal data the Commission intended to cover with this exemption, the Directive does not strictly delineate the scope of EU law in this context, thereby leaving the exemption open to potentially divergent interpretations by the Member States.

The Directive further extends this exemption by granting Member States the right to adopt legislative measures to restrict the obligations and rights provided to the data subject under the Directive in these areas. In order to “avoid any negative consequences for the restrictive policies of most Member States,” this provision deliberately leaves it up to the Member States to determine the scope of these restrictions. In the exemption for areas of criminal law, for example, the Directive enumerates every aspect of police activity with “astonish-

---

29 See Directive, supra note 1, arts. 25, 26.
30 See id. art. 26.
31 Id. art. 3(2).
32 Id. arts. 3(2), 13.
34 See Directive, supra note 1, art. 13.
ing meticulous[ness]" in order to give the States the broadest discretion possible in restricting the scope of the Directive.36

Authorities in the Member States could interpret these provisions as license to infinitely restrict the data subject's right of access in these areas.37 This interpretation is particularly likely because data privacy has been a low priority in most Member States.38 Because the Member States are concerned chiefly with the efficient operation of their police forces, they have "never particularly welcomed the data subjects' right to know" when it potentially could interfere with this efficiency.39 Thus, local authorities could restrict access to data in any situation that they could claim was remotely related to national security or to a criminal proceeding.40

England, for example, validates this concern. The Data Protection Act 1998, England's legislative enactment pursuant to the Directive, provides a similar exemption to that contained in the Directive.41 It provides that the data subject shall not have the right of access to the data if the data are processed for the purpose of "preventing[ng] or detecting[ng] a crime" or "apprehending[ing] or prosecuting[ing] . . . offenders."42 Thus, England has not defined the scope of the restrictions at all, as the Directive suggests it should, but rather has passed this determination on to the data processors themselves.43 Furthermore, the English law seems to exceed the restrictions allowed under the Article 3(2) exemption by providing that personal data processed for the enumerated purposes does not need to be processed "fairly

36 See Simitis, supra note 22, at 460.
37 See Jacqueline Klosek, The Development of International Police Cooperation Within the EU and Between the EU and Third Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Therefrom, 14 Am. U. Int'l L. Rev. 599, 645 (1999) (arguing that the Directive provides little practical protection to individuals concerned about police use of personal data).
38 See Simitis, supra note 22, at 460.
39 Id.
40 See id.; Klosek, supra note 37, at 645.
42 DPA, supra note 41, § 29.
43 See id.
and lawfully."44 This additional restriction, which is not mandated by the Directive, practically courts violations of personal data privacy.45

According to Professor Spiros Simitis, the first data protection commissioner in the German State of Hesse,46 the Commission’s refusal to define the scope of these restrictions was a mistake.47 Simitis argues that what is really needed are rules clearly stating that the data subject’s right to access can “never be totally excluded, but rather can at most be partially restricted or temporarily suspended in a series of unequivocally defined and exhaustively listed cases.”48 The Directive, on the other hand, leaves it up to the Member States to enumerate these cases.49

Niall Perry, head of Information Technologies with the Mid-Bedfordshire, England District Council, recently stated that, although he realized that he would be exempt from some of the requirements to seek consent of the data subject as a requirement for processing data, he would “probably seek consent as a belt-and-braces thing.”50 While Perry’s intent is admirable, it may not reflect the pervading attitude among the Member States towards compliance with the Directive.51

On one hand, the Member States must be able to protect national security and conduct criminal investigations in an efficient manner,52 and the need to obtain the subject’s consent for all processing of personal data could hinder these efforts.53 On the other hand, national and local authorities with license to infinitely restrict privacy rights in any case that they choose could lead to a Big Brother situation in which citizens are defenseless against governmental intrusions into their personal spheres.54 Such routine flouting by a Member State of the principles on which the Directive is based not only could threaten the privacy rights of its citizens, but also could hamper the

44 See id. (providing that personal data processed for the purposes of “prevent[ing] or detect[ing] a crime” or “apprehen[ding] or prosecut[ing] ... offenders” are exempt from the first data protection principle, which provides that “personal data shall be processed fairly and lawfully.”).
45 See id.
46 See Gellman, supra note 35, at 167.
47 See Simitis, supra note 22, at 460.
48 Id.
49 See Directive, supra note 1, art. 13.
50 Alison Classe, Protection Racket, COMPUTER WkLY., June 10, 1999.
51 See Simitis, supra note 22, at 460.
52 See id.
53 See id.
54 See Klosek, supra note 37, at 645.
effectiveness of the Directive by showing other Member States that it is possible to comply technically with the Directive while ignoring the privacy principles on which it is based.\(^55\)

**II. Article 13(2) Exemption**

Article 13(2) contains another potentially broad exemption. It states that Member States may restrict the data subjects’ rights of access to data when the data are processed “solely for purposes of scientific research or ... for the sole purpose of creating statistics.”\(^56\) Unlike the sweeping exemption for criminal proceedings, the Directive places limits on this exemption in an attempt to balance the rights of data subjects against the need for scientific and sociological research.\(^57\) First, Member States’ restrictions are “subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual.”\(^58\) Second, the restrictions must pose “no risk of breaching the privacy of the data subject.”\(^59\) Finally, Member States may only restrict a data subject’s right of access for statistical purposes when the data are kept by the processor “for a period which does not exceed the period necessary for the sole purpose of creating statistics.”\(^60\)

Although these restrictions narrow the scope of the Article 3(2) exemption, the exemption actually is quite broad because it does not enumerate the types of “research purposes” to which it applies.\(^61\) All public or private institutions with their own research departments theoretically could fall within the exemption.\(^62\) Furthermore, any business seeking to avoid the restrictions of the Directive could simply establish its own “research” department.\(^63\)

The provision in Article 3(2) stating that the exemption applies when data are processed “solely for research purposes” appears to prohibit the use of data collected for research purposes outside the realm of research.\(^64\) This prohibition is particularly important when sensitive

\(^{55}\) *See id.; Simitis, supra* note 22, at 460.
\(^{56}\) *Directive, supra* note 1, art. 13(2).
\(^{57}\) *See id.*
\(^{58}\) *Id.*
\(^{59}\) *Id.*
\(^{60}\) *Id.*
\(^{61}\) *See Simitis, supra* note 22, at 457.
\(^{62}\) *See id.*
\(^{63}\) *See id.*
\(^{64}\) *See Directive, supra* note 1, art. 13(2) (emphasis added).
data are involved, as in medical or criminological research.\(^65\) Article 6(1)(b), however, provides that “further processing” may be allowed “provided that Member States provide appropriate safeguards.”\(^66\) The Directive does not define “appropriate safeguards,” nor does it indicate which types of measures might be considered as such.\(^67\) Therefore, “the Member States will probably keep the door open for uses other than research and thus unnecessarily erode the protection of the data subjects in the name of improved research conditions.”\(^68\)

Another provision that appears to limit the scope of the exemption is a provision providing that the rights of the data subject may be restricted for research purposes “subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual.”\(^69\) The effectiveness of this provision may be minimal, however, given its inherent vagueness.\(^70\) For instance, it does not state expressly whether other uses still are permitted.\(^71\) In addition, it neglects to define “measures or decisions.”\(^72\) Vague provisions such as this one jeopardize the efficient protection of the privacy of data subjects.\(^73\)

If the privacy principles advocated by the Directive are to have any force, the Member States must not permit unbridled interpretations of these types of provisions.\(^74\) In their legislative enactments pursuant to the Directive, the Member States should enumerate exactly which research purposes fall under the exemption.\(^75\) In addition, they should create clear and strict limits on the ability to use research data for purposes other than research.\(^76\) At the very least, Member States should define, or provide guidelines for determining, what constitutes “adequate safeguards” and “measures or decisions.”\(^77\)

\(^{65}\) See Simitis, supra note 22, at 459.
\(^{66}\) Directive, supra note 1, art. 6(1)(b).
\(^{67}\) See Simitis, supra note 22, at 458.
\(^{68}\) Id.
\(^{69}\) Directive, supra note 1, art. 13(2).
\(^{70}\) See Simitis, supra note 22, at 459.
\(^{71}\) See id.
\(^{72}\) Id.
\(^{73}\) See id.
\(^{74}\) See id. at 457–58.
\(^{75}\) See Simitis, supra note 22, at 457–58.
\(^{76}\) See id. at 458.
\(^{77}\) See id. at 459.
III. ARTICLE 26 EXEMPTION TO ARTICLE 25

Article 25 of the Directive contains the important provision that no data processor in a Member State shall transfer personal data to a third country unless that country “ensures an adequate level of protection.” 78 This provision is meant to address the fact that if personal data from a country with privacy regulations can be transferred freely to a country with no privacy rules, the legal protections available in the source country may be lost. 79 According to Article 25, whether or not a third country provides an “adequate level of protection” shall be assessed “in light of all the circumstances.”

[P]articular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation, . . . the country of origin and country of final destination, the rules of law . . . in force in the third country and the professional rules and security measures which are complied with in that country. 80

The Member States and the Commission must inform each other of cases where a third country does not provide an adequate level of protection. 81 Then the Commission may determine whether the third country has failed to ensure adequate protection. 82 If the Commission determines that adequate protection is lacking, the Member States must prevent transfers of data to the country in question. 83

Many countries, including the United States, lack what the Commission would deem an “adequate” level of data protection legislation. 84 However, an absolute ban on the transfer of personal data to these countries would pose a serious trade barrier or even a data or information embargo. 85 “Information sharing now takes place on an international scale and involves a tremendous amount of data referring to individuals.” 86 Information regarding credit transactions, for example, flows routinely from the country where charges are in-

---

78 Directive, supra note 1, art. 25(1).
79 See Gellman, supra note 35, at 158.
80 Directive, supra note 1, art. 25(2).
81 See id. art. 25(3).
82 Id. art. 25(4).
83 See id.
85 See Murray, supra note 5, at 938.
86 Schwartz, supra note 84, at 471.
curred to the country where the bill is ultimately sent. A broad ban on the transfer of data to third countries, such as the United States, would be "disruptive, expensive and, seemingly, unlikely." In light of these economic realities, the Directive provides certain exemptions to this provision of Article 25. There is considerable uncertainty, however, concerning how the Member States will interpret and apply some of these provisions.

Perhaps the most ambiguous exemptions to the "adequate protection" requirement are the "contract exemptions" contained in Article 26(c) and (d). They provide that a Member State may allow the transfer of data to a country that does not ensure an adequate level of protection when the transfer is necessary for the performance of a contract that either is between the data subject and the controller or is between the controller and a third party if the contract is "in the interest" of the data subject. These exemptions are likely to apply, for example, to transfers necessary to reserve an airline ticket for a passenger or to transfers of personal data necessary for the operation of an international bank or credit card payment. They also would apply to multinational corporations that make contracts with local subsidiaries in order to enable their personnel records to be moved.

In a paper adopted on July 24, 1998, the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (the Working Party), an organization established by the Directive to analyze the Directive's provisions and to issue opinions and recommendations to the Commission on matters relating to data protection, suggests that although the Article 26(c) and (d) exemptions appear generous, the requirement that all of the data transferred be necessary for the performance of the contract is likely to limit them. The Working Party optimistically believes that "if additional non-essential data are transferred or if the purpose of the transfer is not the performance of the contract but rather some other purpose (follow-up marketing, for example) the exemption will be lost."

87 See Gellman, supra note 35, at 161.
88 Id. at 158.
89 See Directive, supra note 1, art. 26.
90 See Gellman, supra note 35, at 157.
91 Directive, supra note 1, art. 26(c) & (d).
92 Id.
93 See Transfers, supra note 20, ch. 5.
95 See Transfers, supra note 20, ch. 5.
96 Id.
The Personal Data Privacy Directive

The Working Party overlooks the inherent ambiguities contained within the Article 26(c) and (d) exemptions. 97 What is “necessary” for the performance of a contract is not defined. 98 In addition, what constitutes a contract “in the interest” of the data subject is left to the interpretations of the Member States. 99 Although the Working Party attempts to delineate the scope of “interest” by saying that it would cover transfer of data about the beneficiaries of bank payments who may not be party to a contract with the transferring controller, 100 the Directive itself provides no such illustrations. 101 This lack of specificity may allow data processors to ignore restrictions on third country transfers through subjective determinations of what contracts are in the interests of the data subject. 102 An EU company that enters into a contract to sell the personal data of a European citizen to a direct marketer in the United States, for example, reasonably could assert that the contract is “in the interest” of the person since the direct marketer could be considered a provider of “valuable” goods or services to the data subject. 103

The ambiguities contained in the Article 26(c) and (d) exemptions offer a practical method for EU companies to avoid the restrictions of Article 25. 104 Business publications already have begun suggesting that companies use the exemptions in order to circumvent the legislation. 105 The exemptions obviously are important for preventing obstacles to the free flow of trade between EU and non-EU countries. 106 If the Directive is going to protect privacy effectively, however, it is equally important that Member States clearly define the limits of these exemptions and apply them uniformly. 107 By enumerating the types of contracts that may fall under this exemption and by defining what constitutes an “interest” of the data subject for purposes of the

---

97 See id.
98 See Directive, supra note 1, art. 26(b) & (c).
99 See id. art. 26.
100 See Transfers, supra note 20, ch. 5.
101 See Directive, supra note 1, art. 26(c).
102 See id.
103 See id.
104 See Classe, supra note 50; Phillips, supra note 94.
106 See Transfers, supra note 20, ch. 5 (stating that Article 26(1) exemptions concern cases where public interests override the data subject’s right to privacy).
exemption, the Member States would ensure that the Directive is not cast aside in the interest of trade relations.108

Another ambiguous exemption to Article 25’s “adequate level of protection” requirement for transfers to third countries is found in section 2 of Article 26.109 This section provides that a Member State may authorize the transfer of data to a third country which does not ensure adequate protection where “the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.”110 The purpose of this provision is to balance the free flow of information with the right to privacy by assessing adequacy in the context of each particular transfer, rather than on a per country basis.111 However, the Directive does not define “adequate safeguards.”112 Although it attempts to give guidance as to what constitutes an adequate safeguard by providing that the safeguards “may in particular result from appropriate contractual clauses,” this language merely creates further ambiguity because the phrase “appropriate contractual clauses” is not defined.113 The Directive leaves it up to the data processors to give meaning to these terms in case-by-case analyses.114 This process can be cumbersome115 and may provide data processors, who are already antagonistic to privacy regulation,116 with another reason to overlook or ignore the terms entirely.

Member States can avoid overly liberal interpretations of this exemption by clearly delineating which safeguards, in addition to the use of contractual clauses, may be deemed adequate by the data controller. Furthermore, a clear definition of what constitutes “appropriate contractual clauses” would avoid reliance on subjective determinations in determining which contracts may evade the scope of the Directive.

108 See id. at 459.
109 See Directive, supra note 1, art. 26(2).
110 Id. art. 26(2) (emphasis added).
111 See Murray, supra note 5, at 997.
112 See Directive, supra note 5, at 26(2).
113 See id.
114 See id.
115 See Murray, supra note 5, at 997.
116 See Classe, supra note 50. (Dr. Simon Murdoch of amazon.com.uk says, “The whole concept of a restriction on information about individuals going outside the EU bothers me.”).
CONCLUSION

The EU Data Privacy Directive cannot effectively protect personal data privacy unless Member States implement the Directive responsibly and vigilantly. To that end, Member States must interpret the potentially expansive exemptions to the Directive restrictively if the goals of the Directive are to be achieved. First, Member States' legislation should limit the exemptions for national security and criminal proceedings to a set of clearly defined cases. Next, Member States should limit the exemptions for research purposes by employing more detailed legislative provisions than are found in the Directive, specifically with regard to what constitutes research purposes and what uses beyond research purposes are permitted once information is collected. Finally, Member States should curtail the exemptions to the "adequacy" requirement for transferring data to third countries in order to prevent the exemptions from serving as a general "escape route" for companies seeking to send personal data outside the EU. The exemptions to the Directive are drafted broadly in order to give the Member States room to maneuver in implementing them. It is important, however, that the Member States use this room not to further expand the exemptions, but rather to strictly define their scope.