A Study on the Lack of Enforcement of Data Protection Acts

Thorben Burghardt[1], Klemens Böhm[1], Erik Buchmann[1], Jürgen Kühling[2], and Anastasios Sivridis[2]

[1] Universität Karlsruhe (TH), 76131 Karlsruhe, Germany, {burgthor|boehm|buchmann}@ipd.uni-karlsruhe.de,
[2] Universität Regensburg, 93040 Regensburg, Germany, {Juergen.Kuehling|Anastasios.Sivridis}@jura.uni-regensburg.de,

Abstract. Data privacy is a fundamental human right, not only according to the EU perspective. Each EU state implements sophisticated data protection acts. Nevertheless, there are frequent media reports on data privacy violations. The scientific and the political community assumes that data protection acts suffer from a lack of enforcement. This paper is an interdisciplinary study that examines this hypothesis by means of empirical facts on juridical assessment criteria – and validates it. We have inspected 100 service providers, from social online platforms to web shops. Our study considers legal requirements of the privacy policy and how providers ask for consent and react to requests for information or deletion of personal data. Our study is based on articles of German law that have a counterpart in the EU Directive 95/46/EC. Thus, our study is relevant for all EU states and all countries with similar regulations.

Key words: privacy, study, lack of enforcement, data protection acts

1 Introduction

In the last years, data protection acts have not kept pace with new developments, with unpredictable consequences for society. Data protection directives like 95/46/EC [5] establish data privacy as a human right and require each EU state to implement privacy regulations. However, global organisations have established various links to internal and external subsidiaries, service providers, etc. It has become difficult to keep track of the whereabouts of personal data, to identify the company responsible and to enforce those privacy rights. Many of the data privacy scandals of the last years might not have happened if existing data protection acts would have been enforced. Thus, the scientific and political communities tend to assume that data privacy acts suffer from a lack of enforcement. However, to our knowledge there is no empirical study that supports this hypothesis by collecting facts on juridical assessment criteria.

In this work, we present an interdisciplinary study of the lack of enforcement of data protection acts. Since it is impossible to analyze company-internal violations of data privacy laws, we focus on privacy violations from an external perspective. We analyze if an individual concerned would be able to assert her privacy rights against a broad range of service providers. Therefore we consider legal requirements of the privacy policy, and how providers ask for consent

and react to requests for information or deletion of personal data. We focus on German law and representative German providers. As the EU directives, e.g., 95/46/EC [5], have harmonized data protection laws throughout the EU, and most of the providers investigated are supra-national companies that operate in many other states as well, we deem our results representative for all EU members and all states with similar privacy legislation.

2 Background

2.1 Related Work

We are first to confirm a lack of enforcement based on juridical assessment criteria. There are some studies that indicate an enforcement problem, but do not implement juridical expertise. [8] uses a web crawler to automatically identify conflicts in machine-readable privacy policies (P3P). However, most privacy violations tend to be more complex than matching P3P policies with the use of cookies or web bugs. [9] is a study of 655.000 German Web pages of 14.000 providers. They study if a provider uses a statistics service like Google Analytics and declares this properly. Another study [10] has browsed 815.000 web sites for contact forms, data requested and how much effort is required to find the privacy policy. As a result, 35% of all providers requesting personal information do not display a privacy policy. However, without juridical expertise such studies cannot detect many typical privacy violations, e.g., if the provider has to specify the purpose of data acquisition, or if it is obvious.

2.2 Legal Background

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [6] introduce principles in order to unify privacy regulations in the OECD countries. The guidelines are intended to establish common privacy standards, and to ease transborder data flow between countries with similar regulations. The principles include openness, collection limitation, data quality, purpose specification, use limitation, security safeguards, and individual participation in data protection. The OECD principles are part of many data protection acts like the Asia-Pacific Economic Cooperation Privacy Framework [7]. While the OECD provides recommendations only, all EU member states must transpose directives of the European Community (EC) to national law. Directive 95/46/EC [5] implements the OECD principles to harmonize data protection legislation throughout Europe. Beyond that, the directive specifies privacy as a human right [4], as laid down in Art.6 p.2 European Union Treaty referring to the European Convention on Human Rights.

In Germany, Directive 95/46/EC has been cast into national laws, such as the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG [1]) and acts for specific application areas. The German Telemedia Act (Telemediengesetz, TMG [2]) is one of the core Internet regulations in Germany. It includes a number of articles that implement Directive 95/46/EC, thus consider the OECD Guidelines. The scope of the TMG includes all providers that operate under

German law and offer services via the Internet, but exclude telecommunication or related services.

Our goal is to investigate the lack of enforcement of Internet data protection acts throughout the EU. Since legal issues cannot be investigated based on a directive, we rely on the TMG [2] and on the BDSG [1]. In the following, we will enumerate regulations relevant for our study, and we will name corresponding articles of Directive 95/46/EC. The regulations will be described in Section 4. Relevant privacy regulations fall into two categories:

Data Acquisition and Usage According to 95/46/EC, data protection follows the principles of (1) purpose specification and (2) prohibition with the option of authorization. §12 p.1 and 2 TMG (Art. 6 and 7 of 95/46/EC) implement these principles. The articles require the provider to request a consent from the user if data acquisition and usage goes beyond what is necessary for service delivery or what is allowed by the legislator.

Information Duties §13 p.1 s.1 TMG (Art.10 of 95/46/EC) obliges the provider to inform the individuals concerned on the kind of data acquired, the purpose of the data acquisition and the storage period, and if data is processed in countries not addressed by 95/46/EC. According to §13 p.1 s.2 TMG (Art.5 p.3 of 2002/58/EC), each provider has to inform about automated processes that manage personal data. §13 p.2 TMG specifies the electronic declaration of consent. §13 p.1 s.1 TMG requires to inform the user on forwarding data to other companies. In particular, §4 p.3 BDSG (Art.10 of 95/46/EC) requires to categorize the receivers, e.g., dispatcher or credit agency. According to §13 p.7 TMG and §34 BDSG (Art.12 of 95/46/EC), each provider has to answer requests for information from an individual concerned about her personally identifiable data. The request has to be answered precisely to allow to assert subsequent rights, e.g., to block, correct or delete data as outlined in §35 BDSG (Art.12 of 95/46/EC).

This set of regulations is not exhaustive. However, all of these regulations have a counterpart in the Directive 95/46/EC, i.e., a study based on these articles is relevant for other countries with similar privacy regulations. Furthermore, those regulations are important for almost all service providers on the Web.

3 Study Setup

Provider Sample We have examined 100 providers on the Internet (first row of Table 1). Our complementary website[1] lists all providers and details of the study data. Our sample is based on usage statistics on teenagers [12] and young adults [11], and considers statistics from an online marketer group [3] and similar sources. We have chosen a representative sample of providers according to their *Impact*, *Relevance* and *Comparability*.

Impact The number of customers and customer interactions defines the impact.

Our sample contains providers with a high market share. Further, we take

[1] http://privacy.ipd.uka.de

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Number of providers investigated	*100*	21	48	8	6	10	7
Number of registrations	*89*	21	38	8	6	9	7

Table 1. Provider Sample

into account that individuals of different age and from different social groups might prefer different providers.

Relevance We have selected a provider mix from various categories, i.e., news portals, web shops, auction platforms, messaging services and social community platforms. These categories are relevant for a wide range of society. Note that we do not investigate the same number of providers from each category, because in some categories a few providers dominate the market.

Comparability Providers are comparable only as long as they follow the same regulations. Thus, we have decided to focus on providers that fall under German law. Our selection still includes international providers, but we have verified that they operate under German law.

Study Procedure We cannot expect meaningful results if providers realize that they are subject of a study. Thus, we have constructed an artificial identity including name, day of birth, post office box, address, phone, fax and cellphone number, email and a pseudonym. Our study consists of four phases:

1. **First Visit** Before registering, we investigate if the privacy policy is visible, and if it contains all mandatory information.
2. **Registration** We register our artificial person at the web site of the providers (cf. Table 1, second row) and analyze the registration process. Only 11 providers did not require a registration before it was necessary, e.g., to pay products bought in a web shop.
3. **Request for Information** We send an email in the name of our artificial person to each provider where the person is registered. The email asks for all information (1) stored and (2) forwarded to other companies.
4. **Right of Deletion** We let our artificial person assert her right of deletion, i.e., we send an email to each provider that asks for all personal data to be deleted.

4 Study Results

4.1 The Privacy Policy

We have analyzed the privacy policies of our 100 providers regarding (1) availability, the obligation to inform about (2) data acquisition and handling, (3) data forwarding and (4) automated processing.

Anytime Availability §13 p.1 s.3 TMG: *Each customer must be able to obtain the privacy policy easily and at any time. The provider should offer links on each page which direct the user to a valid privacy policy.* □

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Directly accessible	90	16	45	8	6	8	7
Can be found	9	5	2	0	0	2	0
Undiscoverable	1	0	1	0	0	0	0
Based on outdated laws	10	2	6	0	0	2	0

Table 2. Anytime Availability

Table 2 shows that 90 providers offer privacy polices directly reachable via highlighted links from every web page. The policies are either part of the general terms and conditions or are presented on a standalone web page. 9 providers require their users to follow a sequence of links. It depends on the concrete design of the web site if this procedure would be considered acceptable by court. We did not find the privacy policy of one provider, i.e., the provider is in conflict with law. Finally, 10 providers refer to outdated laws that are invalid by now.

Information on Data Acquisition and Handling §13 p.1 s.1 TMG: *A provider has to inform on (i) the kind of data, i.e., which attributes are acquired, (ii) the storage period and (iii) the purpose of data acquisition and usage. The purpose specification can be omitted when obvious.* □

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Kind of data							
Detailed specification	47	12	18	2	4	5	6
Coarse categories	21	5	10	2	1	2	1
Unspecific terms	31	4	19	4	1	3	0
Storage period							
Data stored for a specified period of time	68	15	26	8	5	8	6
No information	31	6	21	0	1	2	1
Purpose of acquisition							
Specific information	78	10	42	7	5	7	7
Unspecific terms	21	11	5	1	1	3	0

Table 3. Information on Data Acquisition and Handling

Kind of data The 99 providers with a privacy policy specify the data acquired in different ways. As the first part of Table 3 shows, 47 providers explicitly specify each single attribute they store, and 21 of them name coarse but intuitive categories of data, e.g., 'shipping address'. 31 providers use unspecific terms like 'information necessary for order processing'. 6 providers do not specify the kind of data they acquire, i.e., they are in conflict with law.

Storage period 68 providers (second part of Table 3) state that data is stored for a specific period of time, namely until the user revokes her account; after that the data will be locked for legal obligations. 31 providers do not address storage time, thus conflict with the regulations.

Purpose of acquisition 78 providers (third part of Table 3) explicitly state the purpose of the data acquisition. 21 providers use unspecific statements, e.g., 'for service provision'. Legislation accepts this only if the purpose is obvious. However, this holds only for 6 of the 21 providers, which operate common web shops. The other 15 providers run information portals or email services and integrate additional services, i.e., that purpose is not obvious.

Information on Data Forwarding §13 p.1 s.1 TMG: *Each provider has to inform about personal data being forwarded. The privacy policy should explain which data is transferred to whom.* □

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Provider forwards data	*64*	13	30	5	6	7	3
Reason							
To execute the contract	*23*	2	18	2	0	1	0
Unspecific reason	*27*	9	5	0	6	5	2
Receivers							
Logistics services or credit agencies	*26*	0	24	1	0	1	0
Associated companies	*27*	7	6	2	5	6	1
... Receiving companies are named	*7*	5	0	2	0	0	0
Unspecific partners	*22*	4	9	0	3	4	2
... Partners are named	*1*	0	0	0	0	0	1
Receiving countries							
Outside of the EU	*12*	0	4	1	3	3	1
... Receiving countries are named	*8*	0	2	1	3	1	1

Table 4. Information on Data Forwarding

As shown in Table 4, 64 providers state in their privacy policy to forward personal data. While 23 providers state to forward data in order to execute the contract, 27 providers give an unspecific reason, e.g., to provide better services.

26 providers declare to forward data to logistics services or credit agencies, and 27 forward to associated companies, but only 7 name them explicitly. When the receivers are clearly described, the individual concerned can guess why data is forwarded. On the other hand, 22 providers forward data to vaguely defined business partners, and only one provider names them. Finally, 12 providers declare to transfer data to locations outside the EU, but only 8 explicitly list these locations. If unspecific statements prevent a person from asserting her privacy rights, e.g., request the deletion of personal data from an unnamed partner or a company outside the EU, such privacy policies conflict with law.

Information on Automated Processing §13 p.1 s.2 TMG: *Each provider has to inform about automated data processing if those processes facilitate or give way to the identification of an individual. The obligation to inform includes the (i) kind of data, (ii) storage period and (iii) purpose of processing.* □

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Providers using cookies	*96*	21	46	7	6	9	7
Information on automated data processing							
Cookie usage is specified	*72*	16	35	2	6	7	6
Purpose of the cookie is specified	*65*	14	33	1	5	6	6
Storage time of the cookie is specified	*28*	5	18	0	1	2	2
Legal aspects							
Usage of cookies without information	*24*	5	11	5	0	2	1
No information about storage time	*41*	11	14	2	5	5	4
Wrong information on storage time	*9*	3	3	0	1	1	1

Table 5. Information on Automated Processing

A well-known example of these processes are cookies. Cookies can be used to track the movement of users on a web portal over long periods of time, i.e., they allow to map users to IDs which might be used to build comprehensive user profiles. We have investigated if and how our providers use cookies, and if they declare the use of cookies properly. While 96 of 100 providers use cookies (first row of Table 5), only 72 of them refer to automated processes in the privacy policy. Furthermore, only 65 providers name the purpose of the cookie, and only 28 specify the storage time (second part of Table 5). We found that 24 providers do not inform about the use of cookies at all, 41 providers do not declare the storage time of the cookie, and 9 of them report a wrong storage time[2] (third part of Table 5). Only 19 providers implement the law properly.

[2] Since cookies are stored at the client site, we can observe the storage period.

4.2 Request for Consent

§12 p.1, §13 p.2 TMG: *Acquisition and usage of personal data are allowed only if permitted by law, if required for obvious reasons, or if the user gives her consent. The user must be informed that the consent can be revoked at any time.* □

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Consent required	72	16	27	8	5	9	7
... but no request for consent	12	0	10	1	0	1	0
Consent requested on privacy policy/terms and conditions	47	13	8	6	5	8	7
Information on consent revocation	54	16	16	5	4	6	7
Consent to personalized user profiles							
Consent required for user profiles	27	5	6	2	3	6	5
Consent requested on privacy policy/terms and conditions	23	5	2	2	3	6	5
No request for consent	4	0	4	0	0	0	0
Consent to data acquisition							
Consent required for data acquisition	26	2	9	6	1	1	7
Consent requested on privacy policy/terms and conditions	18	2	3	5	1	0	7
No request for consent	8	0	6	1	0	1	0

Table 6. Request for Consent

Following our analysis, 72 providers would have to ask the user for consent (Table 6). 12 of these 72 providers do not ask for consent at all. 47 expect the user to give her consent to the privacy policy or the general terms and conditions as a whole. It depends on the specifics if this would be accepted by court. For example, a consent is invalid if important information is hidden in a voluminous policy. Only 54 inform on the right to revoke the consent. The other providers conflict with law. The second and third part of Table 6 list our findings in detail. 27 providers build personalized user profiles, but 4 do not ask for consent. 23 ask for consent on a lengthy document. Similarly, 26 providers want to acquire data not needed for the service, but require consent on a large document (18) or do not ask for consent (8).

A valid consent requires that the user can check what she has given her consent to. If a provider has modified its conditions, the user might have consented to a declaration different from the current one. Only a few providers (e.g., Amazon) have previous versions of the privacy policy or of the declaration of consent available. No provider lets the user identify the version of the documents she has consented to.

4.3 Request for Information

§13 p.7 TMG, §34 BDSG: *Each customer can ask a provider to inform her on her personal data. The provider has to list all data stored or forwarded to support*

the subsequent exertion of rights, e.g., the right of deletion. □

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Number of responses	56	14	27	4	2	4	5
Average response time	2.05	1.38	2.67	2.5	0.5	3,25	2
No information, but reference to privacy policy	8	4	1	1	1	1	0
No information, but reference to user profile page	7	3	2	0	1	0	1
Useless answer	6	2	3	0	0	0	1
States not to have forwarded data	25	6	11	3	1	0	4
Wrong information about forwarding	2	2	0	0	0	0	0
No information about forwarding	16	5	8	0	1	1	1

Table 7. Request for Information

We let our artificial person ask 87 providers to list all information they (1) store and (2) have forwarded to other companies. As Table 7 shows, we have obtained responses from 56 providers, i.e., 33 have ignored our request outright. The others have answered within two days on average.

Some providers have not responded with the data required, but have told us to only store information listed in the privacy policy (8 providers) or shown at the user profile page on their web site (7 providers). 6 providers replied with canned text that had nothing to do with our request. 25 provider stated not to forward data. In 2 cases the answer was sent from a different company within the company group, i.e., the advice was obviously wrong. 16 providers ignored our request for information on the data forwarded.

4.4 The Right of Deletion

§35 p.2 BDSG, §12 p.1 and p.2, §14 p.1 and §15 TMG: *A provider has to delete all personal data if the person concerned asserts her right of deletion. Exceptions include legal obligations or data required for accounting.* □

We let our artificial person send a request for deletion to all 87 providers where the person has been registered. As shown in Table 8, 59 providers answered the request. 35 of them deleted all account information directly or after a confirmation and acknowledged the deletion. 5 providers stated not to store any information beyond the one the user can delete after logging in. 2 providers refused the deletion due to technical reasons, and 5 providers told us that our artificial person is not registered, or the data cannot be found. In total, 35 providers are in conflict with law.

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Number of responses	59	14	31	4	3	2	5
Average response time	1.15	1.07	1.96	1.5	1	1	0.40
Immediate deletion	35	5	17	4	2	3	4
Self deletion	5	1	2	1	0	0	1
Deletion refused	2	1	1	0	0	0	0
Not registered	5	1	4	0	0	0	0

Table 8. The Right of Deletion

5 Conclusions

This paper is an interdisciplinary study on the lack of enforcement of data protection acts on the Internet. We have compared the practices of 100 service providers to requirements from German law that have a counterpart in EU Directive 95/46/EC. Our analyses show that the vast majority of privacy policies use unspecific terms and/or do not display all information required by law. A significant share of the providers does not ask users for consent, as requested by law. Though many providers respond quickly to requests for information or deletion of personal data, such responses often lack mandatory information.

Acknowledgments This work was partly funded by DFG BO2129/8-1. We thank Mathis Schwuchow and Timo Wankmüller for their intensive support.

References

1. Bundesdatenschutzgesetz (BDSG). Bundesgesetzblatt I 2003 S.66, 2003.
2. Telemediengesetz (TMG). Bundesgesetzblatt I 2007 S. 179, 2007.
3. Arbeitsgemeinschaft Online-Forschung e.V. AGOF Internet Facts 2008-IV. http://www.agof.de, 2008.
4. Council of Europe. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. http://www.echr.coe.int, 1950.
5. European Parliament and the Council of the European Union. Directive 95/46/EC. Official Journal L 281, 11/23/1995, p.31., 1995.
6. Organization for Economic Cooperation and Development (OECD). Guidelines on the Protection of Privacy and Transborder Flows of Per-sonal Data, 1980.
7. Privacy Framework. Asia-Pacific Economic Cooperation (APEC), 2004.
8. Carlos Jensen et al. Tracking Website Data-Collection and Privacy Practices with the iWatch Web Crawler. In *Proceedings of the SOUPS '07*, 2007.
9. Niels Lepperhoff and Björn Petersdorf. Datenschutz bei Webstatistiken. *Datenschutz und Datensicherheit - DuD*, 32:266–269, 2008.
10. Niels Lepperhoff and Björn Petersdorf. Wie Unternehmen im Internet bei Konsumenten Misstrauen sähen. XAMIT, 2008.
11. Media Pedagogy Research Assisiation South-West. JIM-Studie - Youth, Information, Multi-Media (German), 2006.
12. Media Pedagogy Research Assisiation South-West. KIM-Studie - Children and Media, Computer and Internet (German), 2006.