

# eLaw Working Paper Series

No 2018/011 - ELAW- 24 April 2019

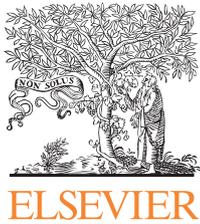
**A comparison of data protection legislation  
and policies across the EU**

Bart Custers, Francien Dechesne, Alan M.  
Sears, Tommaso Tani and Simone van der Hof



**Universiteit  
Leiden**  
eLaw

Discover the world at Leiden University

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

[www.compseconline.com/publications/prodclaw.htm](http://www.compseconline.com/publications/prodclaw.htm)


---



---

**Computer Law  
&  
Security Review**


---



---



# A comparison of data protection legislation and policies across the EU

Bart Custers <sup>a,\*</sup>, Francien Dechesne <sup>a</sup>, Alan M. Sears <sup>b</sup>, Tommaso Tani <sup>b</sup>,  
Simone van der Hof <sup>a</sup>

<sup>a</sup> eLaw, Center for Law and Digital Technologies, Faculty of Law, Leiden University, Leiden, The Netherlands

<sup>b</sup> Law and Digital Technologies graduate, eLaw, Center for Law and Digital Technologies, Leiden, The Netherlands

---

## A B S T R A C T

---

### Keywords:

Privacy  
Data protection  
Comparative law  
Personal data  
Data protection authorities

Although the protection of personal data is harmonized within the EU by Directive 95/46/EC and will be further harmonized by the General Data Protection Regulation (GDPR) in 2018, there are significant differences in the ways in which EU member states implemented the protection of privacy and personal data in national laws, policies, and practices. This paper presents the main findings of a research project that compares the protection of privacy and personal data in eight EU member states: France, Germany, the UK, Ireland, Romania, Italy, Sweden, and the Netherlands. The comparison focuses on five major themes: awareness and trust, government policies for personal data protection, the applicable laws and regulations, implementation of those laws and regulations, and supervision and enforcement.

The comparison of privacy and data protection regimes across the EU shows some remarkable findings, revealing which countries are frontrunners and which countries are lagging behind on specific aspects. For instance, the roles of and interplay between governments, civil rights organizations, and data protection authorities vary from country to country. Furthermore, with regard to privacy and data protection there are differences in the intensity and scope of political debates, information campaigns, media attention, and public debate. New concepts like privacy impact assessments, privacy by design, data breach notifications and big data are on the agenda in some but not in all countries. Significant differences exist in (the levels of) enforcement by the different data protection authorities, due to different legal competencies, available budgets and personnel, policies, and cultural factors.

© 2017 Bart Custers, Francien Dechesne, Alan M. Sears, Tommaso Tani, Simone van der Hof. Published by Elsevier Ltd. All rights reserved.

---

\* Corresponding author. eLaw, Center for Law and Digital Technologies, Leiden University, Kamerlingh Onnes Gebouw, Steenschuur 25, Leiden 2311 ES, The Netherlands.

E-mail address: [b.h.m.custers@law.leidenuniv.nl](mailto:b.h.m.custers@law.leidenuniv.nl) (B. Custers).

<https://doi.org/10.1016/j.clsr.2017.09.001>

0267-3649/© 2017 Bart Custers, Francien Dechesne, Alan M. Sears, Tommaso Tani, Simone van der Hof. Published by Elsevier Ltd. All rights reserved.

## 1. Introduction

The protection of personal data in the European Union largely depends on existing legislation. The EU Data Protection Directive (Directive 95/46/EC),<sup>1</sup> valid until May 25th 2018 and the General Data Protection Regulation (GDPR, Regulation 2016/679),<sup>2</sup> in force after May 25th 2018, predominantly determine the legal framework for rights and obligations of persons whose data are collected and processed (data subjects) and for companies and governments that collect and process these personal data (data controllers). The actual protection, however, does not only depend on the legal framework, but also on the actual implementation and interpretation of the legislation and the ways in which it is enforced by courts and Data Protection Authorities (DPAs). The legislation on privacy and the protection of personal data contains many open norms that need further translation into workable, sector-specific, and context-specific rules and practices. Because of differences in legal systems and cultures, the *legal* implementation of the Data Protection Directive varies across EU member states. Similarly, open norms combined with cultural differences also result in different *practical* implementations of the protection of personal data in EU member states.<sup>3</sup> Although the GDPR aims to further harmonize law and practice, it may be expected that differences in both will continue to exist.

The differences in the extent to which personal data are protected raise the question of which country best protects personal data (which is an important aspect of privacy). In this research, the personal data protection frameworks of eight different EU member states have been compared.<sup>4</sup> This comparison shows the position of these different countries in relation to each other. Based on this research, areas of improvement concerning the protection of personal data can be identified in the event that a particular country provides less protection in comparison with other EU member states. The central research question of this study is:

*What is the position of different countries with regard to the protection of personal data in comparison with other EU member states?*

The focus of this research is on the protection of personal data (informational privacy), and not on the protection of privacy in a broad sense. Although a considerable number of the re-

search questions have a legal nature, this is not typical legal or legally positivistic research. Rather, the focus is on the question of how the protection of personal data for residents is implemented in practice and experienced by residents. Previous research has shown that the way people experience privacy does not always match the goals of legislation.<sup>5</sup> This research does not provide a normative judgment on where a country should be positioned in comparison with other European countries, but it does provide suggestions for how a country could move in a specific direction regarding particular aspects of its data protection framework.

## 2. Methodology

An international comparison requires decisions to be made on which aspects (of the protection of personal data) to compare and on which countries to compare.

### 2.1. Aspects to compare

Based on preparatory research,<sup>6</sup> five aspects were determined as points of comparison in this research. These aspects are: (1) general situation, (2) national government policies, (3) laws and regulations, (4) implementation, and (5) regulatory authorities and enforcement. For each country investigated in this research, information was collected on these aspects by means of desk research, an extensive questionnaire, and follow-up expert consultations. During the desk research stage, available literature and online data (for instance, websites and reports of data protection authorities, governments, and civil rights organizations) were collected. In this research, no survey was conducted among EU citizens, but secondary analyses and/or reuse of existing surveys were used to collect further information, which was combined with the expert consultations. Surveys used include the CONSENT survey (2012),<sup>7</sup> the Eurobarometer (2011),<sup>8</sup> and the Oxford Internet Survey.<sup>9</sup> Information that was not available via desk research was requested through an extensive questionnaire sent to experts in the respective countries. Furthermore, employees at the data protection authorities in the different countries were contacted for further information. These experts and data protection authorities did not receive the entire questionnaire, but only those questions that yielded limited results during the desk research. For aspects on which limited or no information was available after desk research and expert

<sup>1</sup> Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, [http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf).

<sup>2</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf).

<sup>3</sup> See also Mulligan, D.K. and Bamberger, K.A. (2015) *Privacy on the Ground in the United States and Europe*, MIT Press.

<sup>4</sup> For the full report, see Custers, B.H.M., Dechesne, F., Georgieva, I.N., and Van der Hof, S. (2017) *De bescherming van Persoonsgegevens; acht Europese landen vergeleken*. Den Haag: SDU.

<sup>5</sup> Custers B.H.M., Hof S. van der & Schermer B. (2014), *Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy and Internet* 6(3): 268–295.

<sup>6</sup> Roosendaal, A., Ooms, M., Hoepman, J.H. (2015) *Een raamwerk van indicatoren voor de bescherming van persoonsgegevens*. Delft: TNO.

<sup>7</sup> CONSENT (2012). *Consumer sentiment regarding privacy on user generated content (UGC) services in the digital economy*. <http://web.archive.org/web/20161019183048/consent.law.muni.cz/>.

<sup>8</sup> Eurobarometer Survey 431 (2015). *Attitudes on Data Protection and Electronic Identity in the European Union*. Brussels, June.

<sup>9</sup> Dutton, W.H., and Blank, G. (2013). *Cultures of the Internet: The Internet in Britain*. Oxford Internet Survey 2013. <http://oxis.oii.ox.ac.uk/reports>.

consultations, the results were supplemented with additional desk research, media analyses and interviews. For the follow-up interviews, experts on personal data protection, policy makers, companies processing personal data, data protection authorities, and civil rights organizations were contacted.

Finally, the collected material was clustered into 23 categories (labels). For the general situation, these are internet use, control, awareness, trust, protection actions, national politics, media attention, data breaches, and civil rights organizations. For national government policies, these are national policies and privacy impact assessments, privacy and data protection in new policies, societal debate, and information campaigns. For laws and regulations, these are implementation of the EU directive, sectoral legislation, self-regulation and codes of conduct. For implementation, these are privacy officers, security measures, and transparency. For regulatory authorities and enforcement, these are supervisory authorities, main activities, the use of competencies, and reputation.

## 2.2. Countries to compare

The following countries were analyzed in this comparison: Germany, Sweden, the UK, Ireland, France, the Netherlands, Romania and Italy. The countries were selected to ensure a distribution on several selection criteria. These are strict/lenient approaches towards privacy protection, different approaches to personal data protection (due to cultural dimensions, the legal system, and the monistic/dualistic approach to international law), maturity of privacy protection (history, particularly accession to the EU), and geographical distribution (North-South and East-West). In total, the five aspects of personal data protection were mapped for eight European countries. After that, the countries were compared on these aspects and the position of each country was determined by a comparison with the other countries.

## 3. Results

### 3.1. The right to privacy

Before focusing on data protection, first, an inventory was made on how the right to privacy was implemented in each country. The right to privacy exists in all the countries that were investigated via international and European legal instruments and via their constitutional law. All the countries examined are signatories to international and European legal instruments that include the right to privacy, such as the Universal Declaration of Human Rights (UDHR, Article 12), the International Covenant on Civil and Political Rights (ICCPR, Article 17), the European Convention on Human Rights (ECHR, Article 8), and the Charter of Fundamental Rights of the European Union (Articles 7 and 8). In France, Romania and the Netherlands, there is a monistic approach towards international law, meaning that international and national law are considered as one legal system in which provisions in international treaties have direct applicability in national law, without further implementation

required. In Germany,<sup>10</sup> the UK,<sup>11</sup> Ireland,<sup>12</sup> Sweden,<sup>13</sup> and Italy,<sup>14</sup> there is a dualistic approach towards international law, meaning that international and national law are considered as separate legal systems and provisions in international treaties require implementation in national law before being applicable in national law.

With regard to their constitutional law, apart from the UK, which has no written constitution,<sup>15</sup> all countries investigated include privacy rights in their constitution regarding the respect for their home and correspondence. The constitutions of the Netherlands, Sweden, and Romania contain explicit provisions on the right to privacy. In the UK and France, the right to privacy is laid down in other legislation (the Human Rights Act<sup>16</sup> and the Code Civil, respectively). In the other countries, i.e., Germany,<sup>17</sup> Ireland,<sup>18</sup> and Italy,<sup>19</sup> the right to privacy is construed by courts on the basis of other constitutional rights.

### 3.2. Internet use

When focusing more specifically on informational privacy and personal data protection, several aspects on the use and perception of personal data were selected to provide the general context and setting for each of the countries in this research.

When looking at internet use, 57% of EU citizens use social networks at least once a week. Of the countries investigated, in Ireland and Sweden, citizens use social networks the most and only France and Germany are below this average.<sup>20</sup> Instant

<sup>10</sup> Kommers, D.P. (2012) *The Constitutional Jurisprudence of the Federal Republic of Germany*. Durham NC: Duke University Press.

<sup>11</sup> Atkin, J. and Atkin, B. (1997), *Akehurst's Modern Introduction to International Law*. London: Harper Collins, p. 45.

<sup>12</sup> Review of implementation of the United Nations Convention against Corruption, Ireland: Executive Summary, CAC/COSP/IRG/2015/CRP.12 (1 June 2015), § 1.1.

<sup>13</sup> Hermida, J. (2004) *Legal basis for national space legislation*. Dordrecht: Kluwer, p. 141.

<sup>14</sup> With verdicts nr. 348 and 349 of 2007, the Constitutional Court clarified that only European Union laws have direct applicability, whilst other international laws require to be implemented by national laws or be object of constitutional check by the same Court. See also Cartabia, M. (2007) *Le sentenze gemelle: diritti fondamentali, fonti, giudici* ([Osservazione a] Corte cost., sent. 24 ottobre 2007 n. 349). *Giurisprudenza costituzionale* 52.5 (2007): 3564-3574.

<sup>15</sup> Blick, A., and Blackburn, R. (2012) *Mapping the Path to Codifying – or not Codifying – the UK's Constitution*, Series paper 2. London: Centre for Political and Constitutional Studies, King's College.

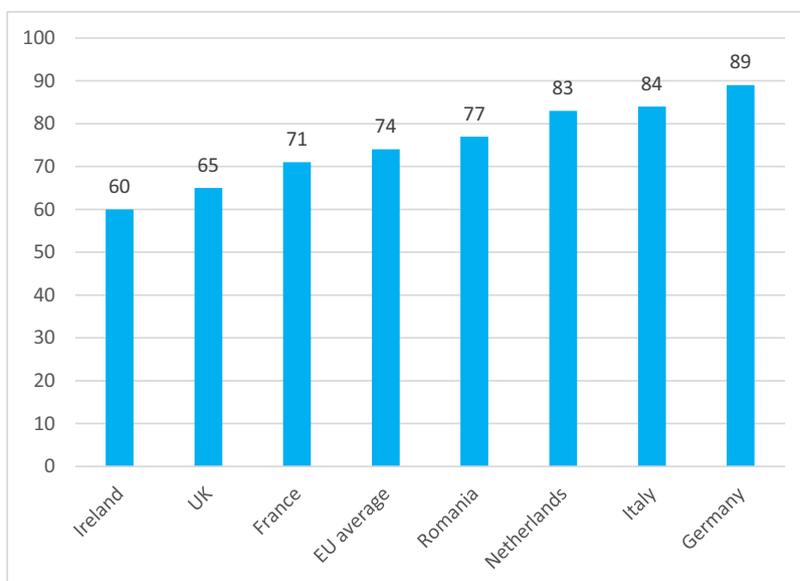
<sup>16</sup> Human Rights Act 1998 (c42).

<sup>17</sup> *Mikrozensus*, 27 BVerfGE 1, 6 (1969). See also ook Dörr, D. and Aernecke, E. (2012) *A never ending story: Caroline v Germany*. In D. Dörr and R.L. Weaver (eds.) *The right to privacy in the light of media convergence*, Berlin: De Gruyter, p. 114.

<sup>18</sup> *McGee v. Attorney General* [1974] IR 284; *Kennedy and Arnold v. Attorney General* [1987] IR 587.

<sup>19</sup> In Italy, before the obligations imposed by EU Directive 95/46/EC, the right to privacy was first introduced by the Court of Cassation in 1975 (Corte di Cassazione, sez. III civile, sentenza 27/05/1975, n. 2129) on the basis of different rights granted by the Constitution. See also Granara, D. (2015) *Il fronte avanzato del diritto alla riservatezza*. Riv. it. dir. pubbl. com (2015): 3-4.

<sup>20</sup> Eurobarometer Survey 431 (2015). *Attitudes on Data Protection and Electronic Identity in the European Union*. Brussels, June. p. 109.



**Fig. 1 – Percentage of people that are aware of the use of personal information by website owners. Based on the CONSENT survey (2012) (Consumer sentiment regarding privacy on user generated content (UGC) services in the digital economy. <https://www.consent.law.muni.cz/>.) Data for Sweden is missing.**

messaging and chat websites [sic] are used at least once a week by 53% of EU citizens. Of the countries investigated, only Italy is above this average, whereas the other countries are below this average.<sup>21</sup> Online banking is used at least once a week by 43% of EU citizens. The Netherlands, Sweden, Ireland and the UK are above this average, whereas Germany, France, Romania, and Italy are below this average.<sup>22</sup> Phone calls and video messaging over the internet are used at least once a week by 27% of EU citizens. The Netherlands and Germany are below this average; the other countries investigated are above this average.<sup>23</sup> Online games are used at least once a week by 25% of EU citizens. The UK, Sweden and Germany are below this average, the other countries investigated are above this average.<sup>24</sup> Online shopping is used at least once a week by 17% of EU citizens. The UK and Ireland are above this average, and the other countries investigated are below this average.<sup>25</sup> In general, across the EU there is frequent use of the internet.

### 3.3. Control over personal data

When asked about how much control over their personal data, 15% of EU citizens indicate that they feel completely in control. Romania, Sweden, the Netherlands, and Germany are below this average, whereas the UK, Ireland, France, and Italy are above this average.<sup>26</sup> In general, feelings of control are rather low. When asked about the level of concern people have regarding their personal data, concern is relatively high in the UK and Ireland, medium in Germany, Italy, and France, and relatively low in the Netherlands, Romania, and Sweden.<sup>27</sup> In general, levels of concern are quite high throughout the EU. Levels of acceptance, i.e., accepting that your personal data are processed as part of modern life, are quite high across the EU, at 71%. Only Italy, France and Romania are below this average.<sup>28</sup> Nevertheless, a large minority considers the processing of personal data to be a big issue (EU average 35%). Only Romania and France

are below this average.<sup>29</sup> When asked how comfortable people are with companies using personal data to tailor advertisements and content, only an average of 6% feel very comfortable with this. Ireland, the UK, Italy, and Romania are above this average, whereas Sweden, Germany, the Netherlands, and France are below this average.<sup>30</sup>

<sup>21</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 110.

<sup>22</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 110.

<sup>23</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 111.

<sup>24</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 111.

<sup>25</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 112.

<sup>26</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 10.

<sup>27</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 13.

<sup>28</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 29.

<sup>29</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 32.

<sup>30</sup> Eurobarometer Survey 341 (2015). Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June. p. 40.

### 3.4. Awareness

When it comes to awareness, Fig. 1 shows the percentage of people that are aware of the use of personal information by website owners. In general, there are high levels of awareness across the EU. Awareness in Romania, the Netherlands, Italy, and Germany is above average. Although these are only a few characteristics indicating awareness, it can be argued that awareness across the EU regarding the processing of personal data is rather high. In addition, other indicators, such as awareness regarding cookies (EU average 65%) and privacy policies (EU average 47%), further illustrate this.<sup>31</sup>

### 3.5. Political debate

The extent to which there is an active debate on privacy and data protection in national politics varies among countries. Even when there is an active political debate in a country, the focus and perspectives are sometimes different. In Ireland<sup>32</sup> and Romania,<sup>33</sup> there is hardly any political debate on privacy and the protection of personal data. While there is some level of political debate on this issue in France, the strongest debates are found in the Netherlands, Germany,<sup>34</sup> Sweden,<sup>35</sup> the UK, and Italy. In some countries, such as the Netherlands and Italy, the debate is also initiated by supervisory authorities who have legal rights to advise on legislative proposals in which the processing of personal data plays a role.

The political debates on privacy and the protection of personal data have a different focus in different countries. In the Netherlands, France, and Italy, the debate is often on the balance between privacy on the one hand and (national) security on the other hand. The political debate in the UK is much more focused on the (digital) economy. This is also the case in Sweden, but in Sweden the debate on the digital economy is also intertwined with the issue of what constitutes the proper construction of an open and democratic society. Hence, apart from economic aspects, societal and human rights aspects also play a role in the Swedish political debate. In Germany, the focus of the political debate is much more on human rights. Furthermore, there seems to be increasing consensus in Germany towards more protection for privacy and personal data.

<sup>31</sup> CONSENT (2012). Consumer sentiment regarding privacy on user generated content (UGC) services in the digital economy. <http://web.archive.org/web/20161019183048/consent.law.muni.cz/>.

<sup>32</sup> An exception is the Cyberbullying Bill in 2013, see [http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/\(indexlookupdail\)/20131106-W?opendocument#W03000](http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/(indexlookupdail)/20131106-W?opendocument#W03000).

<sup>33</sup> An exception is the proposed Cyber Security Act in 2015, see: <https://privacy.apti.ro/2015/01/29/romanian-cybersecurity-law-sent-to-the-constitutional-court/> This legislative proposal was declared unconstitutional in January 2015, see: <https://privacy.apti.ro/2015/01/29/icing-on-the-cake-romanian-cybersecurity-law-unconstitutional/>.

<sup>34</sup> A typical example is the debate on camera surveillance, see Eddy, M. (2016) Reports of Attacks on Women in Germany Heighten Tension Over Migrants. *The New York Times*. 5th January 2016.

<sup>35</sup> Münch, M. (2013). Do as the Swedes do? Internet policy and regulation in Sweden – a snapshot. *Internet Policy Review*, 2(2). DOI: 10.14763/2013.2.127.

### 3.6. Media attention

In many of the countries investigated, there is media attention for privacy and data protection issues. There are high levels of media attention in the Netherlands, Germany, France, the UK, and Ireland, although the topics addressed vary. For instance, the media attention in Ireland has focused on the court case of privacy activist Max Schrems against Facebook (the EU headquarters of Facebook are located in Ireland).<sup>36</sup> In France, media attention focuses also on the privacy of public figures, including politicians. In Sweden and Italy, there is some media attention, but it is not as extensive as in other countries. In Romania there is hardly any media attention for these topics. The media attention in the UK is high and seems to even be increasing.

A typical indicator for media attention may also be the so-called Big Brother Awards, which are annual 'awards' for people, companies, or government institutions whose initiatives violate privacy. Obviously, the Big Brother Awards may either be the cause or the result of media attention for privacy and privacy violations. These awards exist in 17 countries. Of the countries investigated, France, Germany, Italy,<sup>37</sup> the Netherlands, and the UK have annual Big Brother Awards. Ireland, Romania, and Sweden do not have Big Brother Awards.<sup>38</sup>

### 3.7. Civil rights organizations

In all countries investigated, civil rights organizations are present. These include national organizations as well as national branches of international organizations. The latter category includes, for instance, Amnesty International and the International Commission of Jurists (ICJ). These organizations promote human rights. In this research we focused on civil rights organizations that specifically focus on the protection of privacy and personal data. Such organizations exist in all of the countries that were investigated, but their budgets and influence vary significantly.

On one side of the spectrum are the countries with organisations with limited budget and influence. In Sweden, the DFRI (Föringen för Digitala Fri- och Rättigheter) has no staff, but it has approximately 80 volunteers and an annual budget of approximately 10,000 Euros.<sup>39</sup> They indicate that their influence is limited. In Romania the situation is similar. There are civil rights organizations, but their public support and influence is limited. In Italy, the Italian Institute for Privacy (IIP), funded by private donors and the European Union,<sup>40</sup> is mostly a study and advocacy centre; Federprivacy is the association for data protection officers and consultants. In the Netherlands, Bits of Freedom, Privacy First, and other organizations are relatively small and have annual budgets of approximately 100,000 Euros. Despite their limited size and budgets,

<sup>36</sup> CJEU 6 October 2015, case C-362/14, Facebook/Schrems, ECLI:EU:C:2015:650.

<sup>37</sup> Last edition of the Italian Big Brother Awards was held in 2012. See <http://bba.winstonsmith.org>.

<sup>38</sup> <http://www.bigbrotherawards.org/>.

<sup>39</sup> <https://www.dfri.se/dfri/>.

<sup>40</sup> European Union funds the IIP inside the Horizon 2020 funding programme for the Privacy Flag project. See <http://www.istitutoitalianoprivacy.it/it/chi-siamo/>.

**Table 1 – Privacy impact assessments.**

	Legal obligation	Other regulation/obligation	Model/standard available	Guidance from DPA?
Netherlands	No	Yes <sup>a</sup>	Yes <sup>b</sup>	No
Germany	No	No	Yes (for RFID)	No <sup>c</sup>
Sweden	No	No	No	No
UK	No	Yes (DPA policy for government)	Yes	Yes
Ireland	No	No	No	No
France	Yes <sup>d</sup>	No	Yes	Yes
Romania	No	No	No	No
Italy	No	Yes (DPA policy)	No	No

<sup>a</sup> For legislative proposals, not for data controllers.

<sup>b</sup> Many models available.

<sup>c</sup> The federal DPA (BfDI) does not offer guidance. Privacy Impact Assessment Guideline for RFID Applications, available at [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy\\_Impact\\_Assessment\\_Guideline\\_Langfassung.pdf?\\_\\_blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1).

<sup>d</sup> For data controllers, not for legislative proposals. See Art. 34 DPA.

they manage to attract media attention frequently. In Ireland, Digital Rights Ireland has a budget of less than 100,000 Euros and is composed of volunteers. Nevertheless, Digital Rights Ireland does have an impact, given the litigation they do, most notably in their case on the EU data retention directive (EU directive 2006/24/EC) which the CJEU declared invalid in 2006.<sup>41</sup>

On the other side of the spectrum are the countries with organizations with significant budgets and much more influence. In Germany there are many civil rights organizations (including the following: Verbraucherzentralen, the German Privacy Association, Netzwerk Datenschutzexpertise, the Association for Data Protection and Data Security, and Stiftung Datenschutz). Some of these organizations also have considerable budgets. For instance, Stiftung Datenschutz received a starting budget of 10 million Euros from the federal government when it was established in 2013.<sup>42</sup> The German civil rights organisations are known as influential with regard to legislative proposals and the public debate. In the UK, there are also professional civil rights organisations, such as Big Brother Watch and Privacy International. Privacy International is known worldwide (for instance, for its global privacy rankings) and has an annual budget of approximately 1.4 million GBP.<sup>43</sup> They publish high quality research reports (including for the UN) and have considerable influence on the political and societal debate. In France, there are many civil rights organizations, but the major player is La Quadrature.<sup>44</sup> Compared to German and UK organizations, La Quadrature has a much smaller budget (the annual budget was 320,000 Euros in 2017), but they can be considered professional and influential regarding the public debate.

### 3.8. Privacy Impact Assessments

Although the GDPR mandates the use of Privacy Impact Assessments (PIAs), or more precisely Data Protection Impact Assessments (DPIAs), in some situations where there may exist high risks for the rights and freedoms of individuals, such as-

assessments are not yet mandatory in any of the investigated countries. An exception, to some extent, is France, in which article 34 of the data protection act<sup>45</sup> contains a legal obligation for data controllers to map the risks of processing personal data. However, PIAs are not mandatory for new legislation or regulations in France. In the Netherlands, the situation is more or less the opposite: data controllers are not under any obligation to perform PIAs, but the central government has the duty to perform PIAs for legislative proposals that involve the processing of personal data. In other countries, like the UK, and Italy, the data protection authorities have issued guidelines for executing PIAs. In some countries, models and standards for PIAs are available, and in a few countries the data protection authorities (DPAs) offer guidance. Table 1 provides an overview.

### 3.9. Legislation and regulations

EU member states had a legal obligation to implement EU directive 95/46/EC in national law. The deadline for implementation was at the latest at the end of three years from the adoption of the directive, i.e. in 1998.<sup>46</sup> Five countries did not meet this deadline (France, Luxembourg, the Netherlands, Germany, and Ireland). However, after some extra years, all countries had implemented the directive. In 2004, France was the last country to do so. After having been implemented, the relevant national legislation has already been revised in many countries. An overview is provided in Table 2. EU member states are allowed to implement more provisions, offering additional protection for privacy and personal data. However, only some countries implemented such additional provisions. Typical examples are breach notification laws in the Netherlands, data protection audits in Germany, privacy by design methods in the UK<sup>47</sup> and special provisions for health care data and children in France.

<sup>41</sup> Case C-293/12. Court of Justice of the European Union. 8 April 2014.

<sup>42</sup> <https://stiftungdatenschutz.org/ueber-uns/vermoegen/>.

<sup>43</sup> This budget is generated by private donations and governments, but not by companies.

<sup>44</sup> <https://www.laquadrature.net/>.

<sup>45</sup> Loi numéro 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, see [https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17\\_definitive-annotee.pdf](https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive-annotee.pdf).

<sup>46</sup> See Article 32 (1), EU Directive 95/46/EC.

<sup>47</sup> Trilateral Research & Consulting (2013) *Privacy impact assessment and risk management Report for the Information Commissioner's Office*, 4 May 2013. <https://ico.org.uk/media/1042196/trilateral-full-report.pdf>.

**Table 2 – Implementation of EU Directive 95/46/EC.**

	Implementation	Important updates
Netherlands	2001	2012, 2016
Germany	2001	2003, 2009
Sweden	1998	2007
UK	1998	2000
Ireland	2003	N/A
France	2004	2011
Romania	2001	2005
Italy	1996	2003 <sup>a</sup>

<sup>a</sup> This update came into force in 2004.

Many countries have sectoral legislation that further protects the processing of personal data. Typical sectors include health care, telecommunications, finance, criminal law, and the public sector. Almost all the countries investigated have sectoral legislation in these areas. And even if there is no sectoral legislation, in many cases there are guidelines, codes of conduct, or other forms of soft law regulations on the processing of personal data.

Article 27 of EU Directive 95/46/EC prescribes that member states should encourage the use of codes of conduct and self-regulation. Sweden and the UK are countries with a long tradition of self-regulation and have developed legislation and regulation accordingly. Countries like the Netherlands, Germany, Ireland and France typically use a combination of self-regulation and government regulation. Romania and Italy typically focus on government regulation.

### 3.10. Privacy officers

In many countries it is not (yet) mandatory to have privacy officers. However, after the GDPR will come into force in May 2018, many organizations will have an obligation to appoint privacy officers. It is estimated that worldwide, approximately 75,000 privacy officers will be needed.<sup>48</sup> These privacy officers are not only required within the EU, but also in other countries, when companies cooperate or trade with organizations within the EU.

In the countries investigated, privacy officers are not mandatory, with the exception of Germany. In Germany, privacy officers are required for organizations with 10 employees or more. Germany was also the first country (in 1970) where someone actually fulfilled the role of privacy officer. Since privacy officers are not mandatory in most countries, there are no statistics available about their numbers. In some countries, the DPA offers registration possibilities. In Germany there are over 700,000 privacy officers registered, 16,400 in France,<sup>49</sup> 7513 in Sweden, and 722 in the Netherlands.<sup>50</sup> For the other countries no data were available. In Romania there are virtually no privacy officers. Obviously, more privacy officers may

be expected in countries with larger populations. When comparing the numbers per capita, Germany still has the most privacy officers, followed by Sweden and France.

### 3.11. Transparency

In general, transparency regarding the processing of personal data is limited.<sup>51</sup> It is generally assumed that data controllers are offering transparency on the personal data they are processing and for which purposes via privacy policies, terms and conditions, or both.<sup>52</sup> However, the problem is that people do not read these privacy policies (the EU average of people who read the entire text is 11%).<sup>53</sup> Reading privacy policies is very time consuming; research shows that reading all privacy policies would take an annual 244 hours per person.<sup>54</sup> At the same time, people are only prepared to spend between 1 and 5 minutes on this.<sup>55</sup> Even the people who make an effort to read privacy policies may have troubles with the (sometimes highly) legalistic and technological texts. In some cases, clear and brief privacy policies are available, but these raise the question as to how much information they really offer.<sup>56</sup>

There were no big differences found with regard to transparency among the countries investigated. That makes it hard to identify the best practices. Nevertheless, the lack of transparency is a significant problem, since it complicates the use of data subject rights by individuals. This relates to a much broader problem that is based in the complexity of technology.<sup>57</sup> In short, this boils down to the fact that it is difficult to explain the complexity of data processing in clear and plain language; when trying to use simple explanations, the complexity is reduced in a way that may no longer adequately reflect the reality of data processing.

### 3.12. Data protection authorities

All countries investigated have a data protection authority (DPA) dedicated to privacy and personal data protection. Only in Romania was this task (initially) committed to the national ombudsman, but after an EU audit, a separate supervisory authority

<sup>51</sup> Custers B.H.M., Hof S. van der & Schermer B. (2014), Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, *Policy and Internet* 6(3): 268–295.

<sup>52</sup> Custers B.H.M., Hof S. van der, Schermer B.W., Appleby-Arnold S., Brockdorff & N. (2013), Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law, *Scripted: a journal of law and technology* 10(4): 435–457.

<sup>53</sup> Consent Country Report: The Netherlands (2012), p. 4.

<sup>54</sup> McDonald, A. M. & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S Journal for Law and Policy for the Information Society*. <http://www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf>.

<sup>55</sup> Van den Berg, B. en Van der Hof, S. (2012) What happens to my data? A novel approach to informing users of data processing practices, 17 *First Monday*.

<sup>56</sup> Toubiana, V., and Nissenbaum, H. (2011) An Analysis of Google Logs Retention Policies, *Journal of Privacy and Confidentiality* 3 (1): Article 2.

<sup>57</sup> Zie ook: Custers B.H.M., Hof S. van der & Schermer B. (2014), Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, *Policy and Internet* 6(3): 268–295; Custers B.H.M. (2016), Click here to consent forever; Expiry dates for informed consent, *Big Data & Society* : pp 1–6.

<sup>48</sup> <http://www.v3.co.uk/v3-uk/news/2477538/gdpr-will-require-at-least-75-000-data-protection-officers>.

<sup>49</sup> <https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx>.

<sup>50</sup> <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming>.

**Table 3 – Budgets and number of employees of each DPA.**

	Budget (M Euros)	Number of employees (FTE)
Germany (2016)	13.7 (federal) <sup>a</sup>	110 (federal)
UK (2016)	26.5 <sup>b</sup>	442 <sup>c</sup>
Italy (2015)	19.2	121
France (2016)	19.0	192
Netherlands (2015)	8.1	73
Ireland (2017)	7.5 <sup>d</sup>	60
Sweden (2014)	4.6	40
Romania (2015)	0.7	41

<sup>a</sup> The budgets of the 16 state level DPAs are not included in this number.

<sup>b</sup> Annual budget in 2016 was 23 million British pounds.

<sup>c</sup> Of which 409 employees were fulltime employed.

<sup>d</sup> In 2017. The budget for the Irish DPA has increased significantly in recent years: in 2015 the budget was 3.65 million euro, in 2016 the budget was 4.7 million euro and in 2017 it was 7.5 million euro.

was established.<sup>58</sup> Budgets and number of employees differ significantly between countries, however.

Table 3 shows an overview of the annual budgets of the DPAs in each country and the number of employees that serve at each DPA. For Germany, this comparison is difficult to make, because apart from the federal DPA, there are also 16 state-level DPAs. When these state-level figures are also taken into account, Germany would rank at the top of both lists. The larger countries (Germany, the UK, Italy, and France) obviously have committed the largest budgets to their DPAs. However, a fairer comparison would be to compare the budgets in relation to each country's GDP, which is shown in Fig. 2 below.

There are some observations that can be made from Fig. 2. First, it seems that the majority of the countries have similar budgets assigned to their DPA (in relation to their GDP). The relative budgets for France, Sweden, the UK, Italy, and the Netherlands are all in the same range. If the state-level figures in Germany were included (i.e., the federal DPA and 16 state level DPAs), it would rank highest. Most remarkable is Ireland. The budget for the Irish DPA has increased significantly in recent years.<sup>59</sup> The 2017 budget is twice the 2015 budget. The budget of Romania is the lowest, both in absolute and relative terms.

When looking at Table 3, it can be concluded that the number of employees serving for each DPA is closely related to the available budget. Only Romania and the UK manage to employ considerably more employees within the available budgets. In Italy, the number of employees of the DPA is relatively low in comparison to the DPA's budget.

Additionally, when looking at the number of employees, it is not entirely fair to compare absolute numbers. Again, larger

countries would appear to do better than smaller countries. Hence, Fig. 3 shows the number of employees of each DPA in comparison to the number of inhabitants.

When looking at the enforcement powers of the DPAs, they all have several powers and options for sanctioning violations of data protection laws. In the Netherlands, Romania, and partially also in Italy,<sup>60</sup> the DPAs have the possibility to impose (maximum) sanctions that depend on the annual turnover of companies, a type of sanctioning that will be applicable in all countries in 2018 when the GDPR comes into force. In absolute numbers, maximum fines are highest in France (at 3 million Euros) and lowest in Romania (at 22,000 Euros).<sup>61</sup> Criminal sanctions are also possible in most countries, with maximum prison sentences between 6 months and 5 years.<sup>62</sup>

We also tried to compare the number of questions, notifications, investigations and citizen complaints handled by the DPAs and the numbers of sanctions imposed. However, only limited data was available for this and the data that are available are hard to compare. For instance, some countries report the number of questions, notifications, and complaints separately, whereas others report them together. We acknowledge that it may be difficult sometimes to categorize a phone call or e-mail message as a question, notification, or complaint. Also the number of investigations is hard to compare, since some investigations of the DPA may be small-scale and only take a few weeks, whereas other investigations may take several months or even years and involve large teams of people. In summary, these figures are difficult to compare.

In terms of reputation, the DPAs in Sweden (51%) and the Netherlands (50%) are the best known among people. The DPAs in the UK (27%) and Romania (22%) are the least known.<sup>63</sup> The EU average is 37%.

## 4. Conclusions

The comparison of privacy and data protection regimes across the EU shows some remarkable findings, revealing which countries are frontrunners and which countries are lagging behind in specific aspects. With the group of countries compared in this research, Germany is frontrunner in most aspects, and Italy and Romania are at the other end of the spectrum for many aspects. Most other countries perform around or above average, depending on the particular aspect that is considered. For instance, the Netherlands is a frontrunner regarding data breach

<sup>60</sup> All sanctions imposed by the Italian Data Protection Law can be multiplied by four when the standard amount would be ineffective because of the economic conditions of the offender. Article 164 bis (2), Italian Data Protection Code (Legislative decree 196/2003).

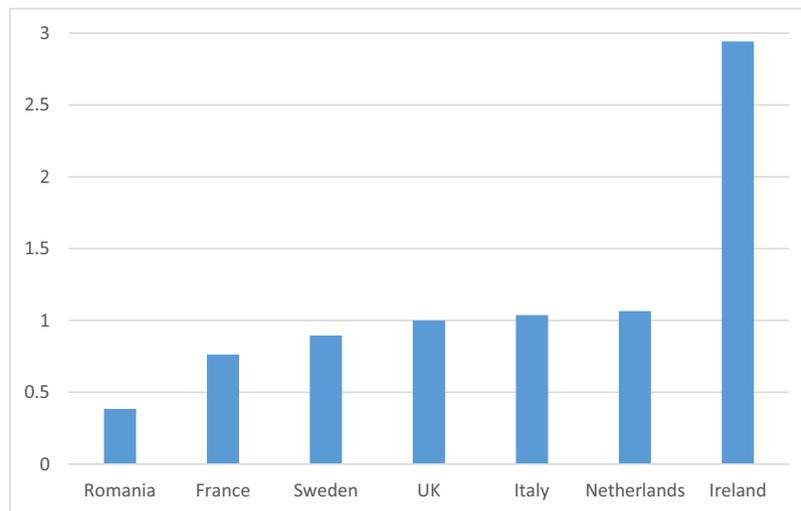
<sup>61</sup> Other maximum fines that can be imposed by DPAs are: Netherlands 820,000 euro, Germany 300,000 euro, Sweden 105,000 euro, Ireland 100,000 euro and Italy 300,000 euro. [https://iapp.org/media/pdf/resource\\_center/BM-2016-Global-Enforcement-Report.pdf](https://iapp.org/media/pdf/resource_center/BM-2016-Global-Enforcement-Report.pdf).

<sup>62</sup> Netherlands 6 months, Ireland 1 year, Germany and Sweden 2 years, Romania and Italy 3 years and France 5 years. [https://iapp.org/media/pdf/resource\\_center/BM-2016-Global-Enforcement-Report.pdf](https://iapp.org/media/pdf/resource_center/BM-2016-Global-Enforcement-Report.pdf).

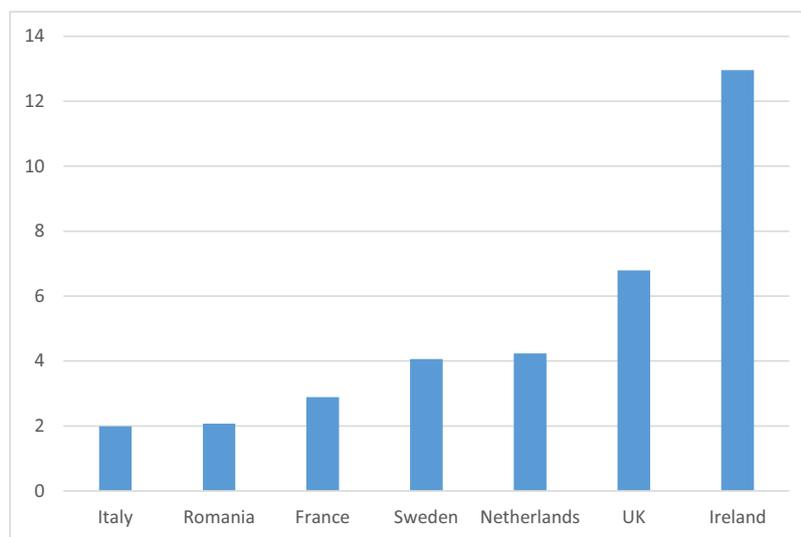
<sup>63</sup> Other figures are: Germany (44 %), Ireland (43 %), France (35 %) and Italy (31 %). Eurobarometer 431 (2015), p. 52.

<sup>58</sup> Manolea, B. (2007) Institutional framework for personal data protection in Romania, p. 1. See [https://www.apti.ro/DataProtection\\_ro.pdf](https://www.apti.ro/DataProtection_ro.pdf). See also COM(2004) 2004 Regular Report on Romania's progress towards accession, 657, Brussels: European Commission, p. 62. [https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/archives/pdf/key\\_documents/2004/rr\\_ro\\_2004\\_en.pdf](https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/archives/pdf/key_documents/2004/rr_ro_2004_en.pdf).

<sup>59</sup> <https://www.dataprotection.ie/docs/13-10-2016-Data-Protection-Commissioner-welcomes-Budget-2017-increase-in-funding/i/1601.htm>.



**Fig. 2 – Budget of national DPAs in relation to the GDP (UK, the median value, was set at 1 for ease of comparison). Germany was left out of this comparison, because only data for the federal DPA are available. When including the DPAs at state level, Germany would show numbers significantly above any other country in this comparison.**



**Fig. 3 – Number DPA employees in relation to the number of inhabitants (FTE per million people). Germany was left out of this comparison, because only data for the federal DPA are available. When including the DPAs at state level, Germany would show numbers significantly above any other country in this comparison.**

notification laws and privacy impact assessments. Ireland is the frontrunner, since recently, regarding the budgets for its data protection authority (DPA) and the number of employees serving at the DPA. At the same time, the Irish people are the least aware of the use of personal information by website owners.

In Ireland and Romania, there is hardly any political debate on privacy and data protection issues. The political debate in Sweden may not be the fiercest, but it could be characterized as perhaps the broadest, in the sense that economic aspects, societal aspects, and human rights aspects all play a role in the Swedish political debate, whereas in most other countries only one of these aspects is focused on. In terms of media attention for privacy and data protection issues, Sweden and Italy have lower levels of media attention and Romania very

little media attention, but other countries show high levels of media attention.

Civil rights organizations are more professional, better equipped, and more influential in the UK and Germany and, to a lesser extent, in France. However, in countries like Sweden and Romania, civil rights organizations have limited budgets and influence. For instance, the Swedish DFRI mainly operates based on volunteers.

Privacy Impact Assessments (PIAs) are not mandatory in many countries. An exception, to some extent, is France, where there exists a legal obligation for data controllers to map the risks of processing personal data. However, PIAs are not mandatory for new legislation or regulation in France. In the Netherlands, the situation is more or less the opposite: data

controllers are not under any obligation to perform PIAs, but the central government has the duty to perform PIAs for legislative proposals that involve the processing of personal data. In other countries, like the UK and Italy, the data protection authorities have issued guidelines for executing PIAs. In some countries, like the UK and France, models and standards for PIAs are available and guidance is offered by the DPAs.

Differences in the implementation of the data protection directive into national legislation are very small in the countries investigated: although EU member states are allowed to implement more provisions than those mentioned in the EU data protection directive, only a few countries implemented such additional provisions for further protection. Typical examples are breach notification laws in the Netherlands, data protection audits in Germany, privacy by design methods in the UK, and special provisions for health care data and children in France. Many countries introduced additional, more specific sectoral legislation in many areas, however.

Germany has by far the largest number of privacy officers and is the only country in which a legal obligation exists in particular situations to appoint a privacy officer. Romania has virtually no privacy officers. Since privacy officers are not mandatory in most countries, there are no data available to compare. Moreover, transparency on personal data processing practices is low in all countries investigated.

The resources of DPAs are comparable in many of the countries investigated, but the DPAs in Germany and Ireland have relatively (i.e., in comparison to their GDP) the largest budgets.

Romania has the smallest budget. Most DPAs manage to get comparable amounts of employees for their budgets. Only Romania and the UK manage to employ considerably more employees within the available budgets. In Italy, the number of employees of the DPA is relatively low in comparison to the DPA's budget. In comparison to the number of people in each country, Ireland and Germany have the most employees serving in their DPAs.

The research results presented in this paper offer many opportunities for policymakers, legislators, data controllers and data protection authorities throughout Europe to learn from experiences, practices and choices made in other countries. It shows that although the protection of personal data is harmonized within the EU by Directive 95/46/EC, many differences exist in the actual protection of personal data. Even though this will be further harmonized by the General Data Protection Regulation (GDPR) in 2018, it may be expected that differences in national laws and practices will continue to exist. Hence, we recommend replicating this research after the GDPR has been in force for a few years.

---

## Acknowledgements

The research on which this paper is based received funding from the WODC (2718), the research and documentation center of the ministry of justice in the Netherlands.