

De bescherming van persoonsgegevens

Acht Europese landen vergeleken

Bart Custers (eindredactie)

Francien Dechesne

Ilina Georgieva

Simone van der Hof

Met medewerking van:

Alan M. Sears

Tommaso Tani

Sdu Uitgevers
Den Haag, 2017

Summary

The Protection of Personal Data
Comparison of Eight European Countries

Background and research questions

The protection of personal data in the European Union largely depends on existing legislation. The EU Data Protection Directive (Directive 95/46/EC), valid until May 25th 2018 and the General Data Protection Regulation (GDPR, Regulation 2016/679), in force after May 25th 2018, determine the legal framework for rights and obligations of persons whose data are collected and processed and for companies and governments that collect and process these personal data. The actual protection, however, does not only depend on the legal framework, but also on the further elaboration on and interpretation of the legislation and the ways in which it is enforced. The legislation on privacy and the protection of personal data contains many open norms. As a result of differences in legal systems and cultural differences, the legal implementation of the Data Protection Directive is different in EU member states. As a result of the open norms, in combination with cultural differences, the practical implementation of the protection of personal data is also different in EU member states. Although the GDPR will further harmonize this, it may be expected that differences in practices 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). This research focuses on the position of the Netherlands in relation to other European countries and the question whether the Netherlands is a frontrunner or lagging behind. An answer to this question enables further measures for the protection of privacy and personal data in the event that the protection in the Netherlands provides less protection in comparison to other EU member states. This leads to the central research question of this study:

What is the position of the Netherlands with regard to the protection of personal data of citizens in comparison with several other countries in the European Union?

In order to answer this question, six subquestions were formulated:

1. What is the general situation regarding personal data protection?
2. What are the national government's policies regarding personal data protection?
3. What are the national laws and regulations regarding personal data protection?
4. How are legislation and policies implemented in practice?
5. How are supervisory authorities organized and how is enforcement carried out?

6. When comparing the eight countries investigated on the abovementioned aspects, what is the position of the Netherlands?

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 research questions has 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. This research does not provide a normative judgement on where the Netherlands should be positioned in comparison with other European countries, but does provide suggestions for how the Netherlands could move in a specific direction regarding particular aspects of its data protection framework.

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.

Aspects to compare

Based on previous research, five aspects were chosen as points of comparison in this research. These aspects, reflected in the first five subquestions mentioned above 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 expert consultations. During the desk research stage, available literature and online data (for instance, websites and annual 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 (including the CONSENT Survey, the Eurobarometer and the Oxford Internet Survey) were used to collect further information, which was combined with the expert consultations. 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 consultations, the results were supplemented with additional desk research, media analyses and interviews. For additional 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 in 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 competences and reputation.

Countries to compare

This research focuses on the position of the Netherlands. Furthermore, the following countries were analyzed in this comparison: Germany, Sweden, the United Kingdom, Ireland, France, Romania and Italy. The countries were selected to ensure a distribution on several selection criteria. These are strict/lenient approaches towards privacy protection, approaches to personal data protection similar/dissimilar to the Netherlands (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 each aspect and the position of the Netherlands was determined in comparison to the other countries.

Results and conclusions

When comparing the position of the Netherlands with the other countries analyzed, this yields the following conclusions:

- The Dutch people show high levels of awareness and self-reliance with regard to the protection of their personal data. At the same time, there are low levels of concern and high levels of acceptance and resignation.
- In the Netherlands, there is extensive attention for the protection of personal data in the political debate and in the media.
- The Netherlands (together with Germany) is frontrunner with regard to data breach notification laws.
- The budgets, influence and notoriety of civil rights organizations in the Netherlands are limited.
- The Netherlands is among the frontrunners with regard to privacy impact assessments, societal debate, and information campaigns.
- Differences in national legislation are very small in the countries investigated.
- The number of privacy officers in the Netherlands lags behind the other countries compared.
- Guidelines for security measures exist in the Netherlands, but authorities do not offer certification or quality marks like in some other countries.
- Transparency is low in all countries investigated.
- The budget and number of employees of the Dutch Data Protection Authority are in line with other countries.
- Sanction options of the Dutch Data Protection Authority are in line with other countries.

- The Dutch Data Protection Authority maintains a very limited dialogue (at an individual level) with those under supervision and does not process citizen complaints.
- The Dutch Data Protection Authority is well-known among citizens.

Combining these conclusions, it can be argued that personal data are well-protected in the Netherlands. 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. The Netherlands perform above average in most aspects. For instance, there are high levels of awareness and self-reliance of citizens; there is extensive attention for personal data protection in the political debate and the media; the Netherlands is a frontrunner regarding data breach notification laws, privacy impact assessments, societal debate, and information campaigns; the budgets, numbers of employees and sanction options of supervisory authorities are adequate; and the Dutch Data Protection Authority is well-known among citizens.

Further improvement is possible in the Netherlands with regard to the budgets, influence and notoriety of civil rights organizations, the number of privacy officers in organization, certification and quality marks for the security of personal data, transparency, processing citizen complaints, and dialogue between supervisory authorities on the one hand and those under supervision and civil rights organizations on the other hand. However, it has to be mentioned that transparency is low in all countries investigated, that the GDPR will (further) improve a number of these issues and that the Dutch government has already initiated (further) improvements on a number of topics. This confirms the proactive approach of the Dutch government regarding the protection of privacy and personal data. Because of his attitude, the Netherlands is well-prepared for the GDPR and likely to be able address future (specifically technological) developments that may affect the protection of personal data.