EU should follow the German example of mandatory DPOs

Survey results show that the effectiveness of the German model makes a positive case for the introduction of company data protection officers throughout Europe. By **Marcus Belke**.

The new General Data Protection Regulation is being widely discussed. What role this will assign to data protection officers in Europe, however, is not yet certain. At present, it seems rather unlikely that the institution of the data protection officer will be introduced as mandatory in all European countries. Public discourse about the role of the data protection officer is, meanwhile, characterised by understatement, exaggeration, poor technical knowledge and fear. Some see the data protection officer as a "bureaucratic monster hostile to innovation". Others regard it as a heroic spearhead in the struggle against states and organisations that collect data unscrupulously. Both of these viewpoints are far from reality.

"Data Protection Practice 2015", a study conducted by the 2B Advice business consultancy, seeks to make the discussion more objective. In the study, German data protection officers talk about their everyday practice, anonymously and away from the headlines. They provide information and suggestions on how a socially acceptable balance can be struck between commercial interests and the protection of citizens' privacy. The typical data protection officer (81% of those questioned) works part-time. 37% are able to devote a maximum of just 5% of their working time to data protection. They work with high efficiency, however, when it comes to measures such as alerting employees to data protection issues, communicating with the regulatory authorities and advising company departments in the planning phases of projects. The study makes clear that data protection officers offer significant cost advantages. They make it possible for companies to manage their own data protection. It is much more efficient to maintain procedures within one's own system than to report each individual processing of personal data to the regulatory authorities, perhaps with the additional need to wait for the approval of a procedure.

Structure of the companies surveyed

Across Germany, 15% of the 272 participating companies employ up to 50 employees, 45% up to 500, 30% up to 5,000, 9% up to 50,000 and 1% over 50,000. It can be seen that data protection officers from large companies made up a disproportionately large number of the participants. This can be attributed to the data collecting methodology. The survey was addressed to data protection officers known by name, which is why companies without a data protection officer were left out.

The DPO's independence

Because of the data protection officer's function as an expert advisor and as an appeals authority for employees in the event of data protection violations, recognition in the company is, in most cases, a matter of course. Three-quarters (76%) of the data protection professionals stated that they are known within their company as the data protection officer, while the remaining quarter (24%) said that they were at least partly known. Over four out of five (82%) data protection officers state that they are able to pursue their job in a professionally independent capacity although this independence is a mandatory requirement in Germany for the appointment to be have legal effect.

Over half (54%) of the data protection officers stated that, in their view, the management fulfilled their obligations regarding internal data protection management; another 40% stated that the management did so to some extent.

On a separate point regarding management, 21% of data protection officers questioned rated the support received for their work by the management as "unsatisfactory" or "fairly unsatisfactory", while 79% rated the support as "satisfactory" or "fairly satisfactory".

Most find budget satisfactory

The average annual budget of the data protection officers who replied to this question in the survey is €18,822. But 10% of the data protection officers questioned stated that no budget was available to them. It can be seen that a significant majority of data protection officers (80%) receive their budget only on request. The size of the budget also increases with company size. Generally, companies with up to 50 employees are given a budget of up to €5,000 (35%); companies with up to 500 employees are allotted up to €5,000 (25%) or up to €10,000 (6%); companies with up to 5,000 employees generally receive a budget of up to €5,000 (30%), up to €10,000 (7%) or up to €50,000 (11%). In larger companies with up to 50,000 employees, the budget is normally up to €5,000 (21%), up to €10,000 (21%) or up to €50,000 (17%). In companies with over 50,000 employees, the budget is normally up to €50,000 or up to €100,000. 66% of the data protection officers questioned rated their budget as "satisfactory" or "fairly satisfactory".

The staff: Only one or two

261 data protection officers questioned stated that they had an average of 1.7 staff available to them directly for carrying out their duties. This is, nevertheless, 30% more employees available for support on average than was reported in the "Data Protection Practice 2012"[1] results. 54% of the data protection officers nevertheless consider the support of available personnel to be "satisfactory" or "fairly satisfactory" for the fulfillment of their duties. The vast majority of data protection officers see the specialised departments in the company as cooperative.

Expertise and activities

In the ranking of expertise required for the function of data protection officers, data protection law unsurprisingly remains in first place, followed closely by issues of IT security, knowledge of in-house communications and organisation. Knowledge of auditing and business management were regarded by the respondents as the least important.

The ranking of time demands on data protection officers is led by internal requests, followed by provision of training, auditing and checks, upkeep of the privacy inventory tool and providing consultancy to management. The least time is taken up by auditing outsourced data processors and external requests.

Involvement in projects

Only involvement of the data protection officer at an early stage can prevent wrong decisions and bad investments. A half (49%) of data protection officers stated that they become involved at the project planning phase to assess the project's implications in relation to data protection law; 10% become involved in the investment decision when the project commences, and 26% only become involved once the project is underway. A further 15% of data protection officers are never involved in projects at all.

The Privacy Inventory Tool

In the overview of all automated processes, which is mandatory in Germany, the data controller, the group of data subjects affected, the type of data, the intended purpose and the data security precautions are to be documented. When asked about the number of individual procedures within one processing overview, the data protection officers reported an average of 57 procedures. Naturally, this number varies considerably with the size of the company. Thus, one data protection officer in a company with over 50,000 employees stated that their privacy inventory tool covered more than 500 individual procedures. These figures make it clear that maintaining the inventory is a substantial piece of work in organisational terms that requires significant resources. Among the companies with under 50 employees, by contrast, almost 90% of privacy inventory tools contain 50 or fewer different procedures. 41% have introduced a process that ensures that the privacy inventory is up-to-date. In three-quarters (74%) of the companies, the departments are involved in creating and updating the process descriptions.

Monitoring of outsourced Data Processing

Under section 11 of the BDSG (Germany's Federal Data Protection Act), the client remains legally responsible for data protection when he commissions a third party to process personal data. He has extensive inspection obligations which, however, he may exercise at his discretion. No specific form of monitoring is legally prescribed. Self-inspection (35%) is among the inspection procedures used most frequently. Despite the fact that the situation is clearly unlawful, 13% of respondents stated that no inspections were carried out. Only in a few cases were on-site audits carried out, either by service providers paid by the company, or by independent third parties paid by the contractor.

The EU General Data Protection Regulation

Four out of five (80%) of all data protection officers questioned consider standardised data protection throughout the EU to be generally the right way forward. Although a majority argue against variations at the national level, 40% of the data protection officers nevertheless would like member states to have the option of deviating from the data protection level set out in the EU DP draft Regulation.

Nearly a quarter (23%) of the data protection officers questioned expect an increase in the level of data protection in Germany, while over three-quarters (77%) of those questioned anticipate it to become lower.

In the German understanding of data protection, the right to informational self-determination is intended to allow data subjects to have control over their data. The data protection practitioners are largely doubtful about the feasibility of realising this objective. Over three-quarters (77%) do not believe that the data subject will regain control over his or her data as a result of the EU General Data Protection Regulation.

The right to remove personal data in social networks is considered correct by 58% of respondents, though 40% see it as not technically feasible. The proposed obligation to notify data recipients of an intention to delete ("deletion chain") is considered correct by 40% of the data protection officers. But 60% doubt its enforceability considering it as too harmful to the enterprise, technically unrealisable, too easily bypassed or a combinations of these.

Only one third (32%) of the participating data protection officers consider it correct for the obligation to appoint a data protection officer to be linked to the number of data sets regularly processed in the company. A clear majority of two-thirds (68%) consider this the wrong approach.

Summary of the results

"Data Protection Practice 2015" collected and evaluated information on the everyday work of German data protection officers. The study gives a realistic insight into the work of data protection officers, the resources they use, and approaches to improvements which are being put into practice. The most important results of the study include the following:

- 69% consider existing data protection laws unworkable, particularly in the areas of cloud computing, international data processing, and social media. 77% are worried that the EU General Data Protection Regulation will result in a deterioration in the level of data protection.
- Data protection officers offer significant cost advantages. The study makes a positive case for the introduction of company data protection officers throughout Europe.
- 81% of the interviewed data protection officers work part-time. 37% devote a maximum of 5% of their working time to data protection.
- 48% of the interviewed data protection officers have too little time to fulfill their legal obligations.

- 44% are dissatisfied with the work of the regulatory authorities. They criticise insufficient action against data protection violations and want more guidance and training courses.
- 80% of data protection violations are corrected by internal action. In 2012, this number was only 49%.
- 37% of detected data protection violations involved customer data; 48% involved internal employee data.
- 42% of the interviewed data protection officers are not sufficiently informed of data protection violations.
- 62% do not have a complete privacy inventory tool available.
- 43% consider certification to be a reasonable option, but only 5% of companies have already obtained certification.

REFERENCE

1 "Data Protection Practice 2015" is available in German and English: 2B Advice GmbH / Technische Universität Dortmund (Publisher): Data Protection Practice 2012. The study can be downloaded here: https://www.2b-advice.com/GmbH-en/Study-Data-Protection-Practice-2015

AUTHOR

Marcus Belke, an attorney and CEO, 2B Advice, an international data privacy consulting group. www.2b-advice.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK