2B Advice®

THE PRIVACY BENCHMARK

Berlin | Bonn | Brezno | Munich | New York

EU Data Protection

technische universität dortmund

Data Protection Practice in Business

SURVEY 2012

2nd EDITION

IMPRINT

2B Advice GmbH
represented by the Directors:
Marcus Belke and Hans Joachim Bickenbach

Wilhelmstraße 40-42
53111 Bonn

Telephone_+49 228 926165-100
Fax_+49 228 926165-109
E-Mail_info@2b-advice.com

Commercial register entry: Bonn HRB 12713

Sales tax ID: DE 228678751

CONTRIBUTORS

Hans Joachim Bickenbach (Managing Director, 2B Advice - the privacy benchmark)
Karsten Neumann (Associate Partner, 2B Advice - the privacy benchmark)
Björn Malinka (Consultant, 2B Advice - the privacy benchmark)
Tobias Mielke (Consultant, 2B Advice - the privacy benchmark)
Kristina Axt (Student, Technische Universität Dortmund)

Table of Contents

Dear reader,

everybody is talking about data protection. Since the German data privacy scandals of 2008, the only partial revisions of the Federal Data Protection Act and the contentions in Europe with corporations acting at the international level, demand has constantly risen - companies at home and abroad seeking to recruit qualified data privacy officers, citizens seeking effective protection of their rights and the press looking for a balanced picture of data protection practice and of policy in respect of data privacy consulting. The possibility of linking together diverse sources of information, meanwhile not only enables new business models, but also allows old fears to resurface. The task of establishing a socially accepted balance here between economic interests and the protection of the privacy of data subjects lies beyond the capabilities of national legislation, owing not least to the international nature of the world wide web. Mistrust on the part of the data subjects, however, threatens to slow down potential further developments. Up to now, the political, legal and social discussion has been characterized by both ignorance of the existing data protection law and by a lack of scientific reevaluation of the experience obtained from practice, to which Germany can point in particular. For these reasons 2B Advice – the privacy benchmark, a leading international data privacy consultancy firm, has undertaken gathering the experiences of in-company data privacy officers in Germany on a statistical basis, in order to add the point of view of practitioners to the existing data on the views of the public and of companies. Performed biennially, this collection of data is intended to provide facts, views and proposals on data privacy practice in companies that can be introduced into policy and into academic discussion. We have also subjected the most recent proposals of the European Commission for unified new data protection regulations with binding effect throughout Europe to critical questioning among the practitioners.

The survey of professional data privacy officers confirms the great need for action by the legislatures at national, European and global levels, but it dispels some of the prejudices. For the debate now emerging about the introduction of this function across Europe, a glimpse of the work of in-company data privacy officers in Germany is very helpful for eliminating unjustified fears and finding practical solutions.

Marcus Belke,
Managing Director

European data protection is facing considerable changes! Following the European Commission's suggestion on 25 January 2012 that a European data protection regulation should be brought in, negotiations in the Parliament and Council of Ministers will soon begin. The aim is to replace the existing national data protection laws with a standardized, Europe-wide data protection regulation, therefore protecting personal data not only in a more targeted and efficient manner, but also in a considerably more manageable and simple manner. At the same time, the plan is to enable digital business to experience a boost in growth, by making the free flow of data across boundaries permissible and legally secure for companies.

Company data protection officers play an important role in this context. I am delighted that we have managed to transfer this "German concept" from the implementation of the 95/46 Directive as a model for the whole of Europe. In return for the waiver of the highly bureaucratic duty to inform placed on supervisory authorities, in future companies will be obligated to appoint a company data protection officer. With this suggestion, all EU member states apart from Germany will be entering new territory and there are numerous reservations regarding training, responsibilities and, quite simply, the usefulness of such a specialist employee.

The present study provides considerable added value at this critical point. It gives both political decision makers and businesses concrete figures on the work of data protection officers. I will continue to fight for a set solution for company data protection officers in Europe, even in companies with less than 250 employees. The figures in the study will be very helpful to me in this quest!

Axel Voss,
Member of the European Parliament

1. Introduction

2B Advice GmbH - the privacy benchmark is a leading data protection management consultant to business within the framework of German and European legislation for practicable data protection regulations in the interest of an effective protection against violation and the creation of relationships of trust. The experts working for 2B Advice GmbH - the privacy benchmark as consultants and external data privacy officers in German companies are also contact partners for lobbying groups and associations for all matters relating to data protection. In the present study we aim to collect, summarize and analyze the experiences of our customers and partners of current data protection law in order to then make this available to legislators, associations and the public in the context of the upcoming debates. Data Protection Practice 2012 in German Companies is not only a statement of the degree of implementation of legal regulations in German companies but also, by its example, a stimulus for their revision in current conditions.

Since the data protection scandals of 2008 the protection of personal data against abuse has become a increasingly central aspect of public attention and political discussion. The alleged data protection scandals resulted in the impression that, as a result of technical developments and the growing commercial exploitability of information, the conception of current data protection as a legal regulation of economic activity and government authority could no longer offer an adequate level of protection.

The call for a fundamental revision of data privacy law poses the question for legislators of whether the evidence of lack of effectiveness of current regulations is accurate and whether suggestions for their redrafting may be drawn from practical implementation. The EU Commission saw the need for action of this kind with the evaluation of the 1995 EU Data Protection Directive and presented extensive proposals for revision in January 2012. In the present study, data privacy officers of primarily Germany businesses that also have international operations were asked to give an extensive statement of their position.

Data privacy officers with 2.335 years of experience gave their views

A total of 375 utilizable completed questionnaires gives an indication of the views on data privacy practice in 375 German companies, including 90 multinational businesses and also the first reactions to the draft by the EU Commission for a comprehensive amendment to data protection legislation. The survey reflects a total of 2335.1 years of experience in professional data protection activity.

2. Overview of Main Outcomes

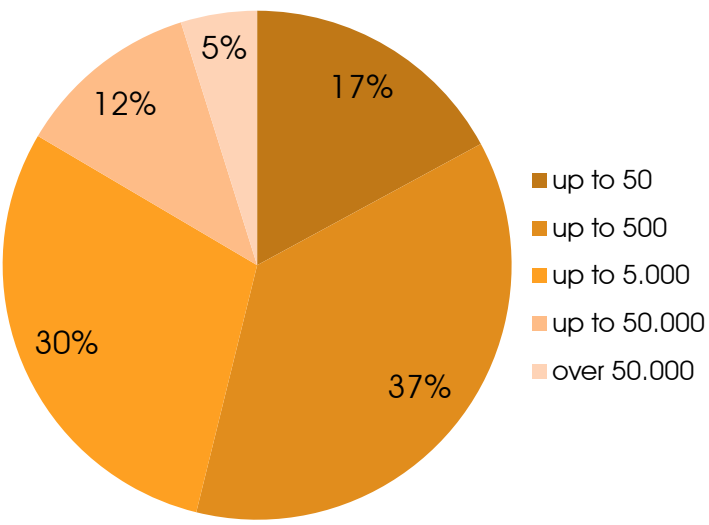
The detailed questioning of up to 375 professional data privacy officers in German companies on their experiences of implementing German data protection law in practice delivers their assessments of the causes of data privacy violations and faults in company organization, and reveals important areas of action for legislators in data privacy law as well as indicating requirements for in-company organization and training. The officers were also asked, for the first time, for their evaluation of the European reform proposals.

Structure of the business surveyed

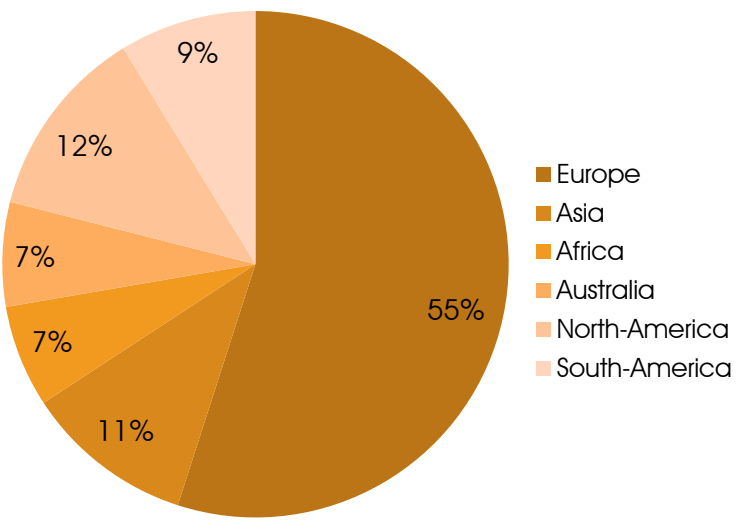
The survey was carried out between February and April 2012 and was aimed at 2751 formally appointed data privacy officers in German businesses who, owing to their practical experience, could provide a clear picture of data protection practice within the company.
Of the sample who participated in the survey, 17% were in companies with up to 50 employees, 37% in companies with 50 to 500 employees, 30% in companies with up to 5000 employees and 17% in companies with over 5000 employees (see 4.1.2). Among them were 29 companies represented with presences worldwide (see 4.1.1) and 36% part of a group (see 4.1.5).

According to the survey, the data privacy officer generally works single-handed - this is the case even for 41% of companies in the category of size between 5000 and 50,000 employees (see 4.1.4). According to the information provided by the data privacy officers, 30% of companies questioned are subject to the special obligation to notify the regulatory authority because they carry out particularly sensitive data processing operations on a commercial basis (section 4d para. 4 BDSG), although they have appointed a data protection officer (see 4.2.6).
The survey reveals that companies with over 50,000 employees have a 7 times greater probability of being audited by the regulatory authority. In this category 35% of respondent data privacy officers reported inspections carried out by their respective regulatory authority. Even in the group of companies with 50 to 500 employees, 9% of data privacy officers reported an inspection by the regulatory authority. An average of 15% of the data privacy officers indicated that they already have experience of an audit by the regulatory authority (see 4.2.7).

Participants by company size:



Company headquarters by continent:



Data protection practice in the company

On average the respondent companies have appointed a data privacy officer for ten years, though in the smallest companies with up to 50 employees the time for which this position has existed was less than five years in 60% of cases (see 4.2.1).
38% of companies with up to 50 employees have made use of the possibility of appointing an external specialist as data privacy officer, whereas in companies with between 500 and 5000 employees this figure is only 8%. In companies that are still larger, however, the proportion of external officers increases again (see 4.2.2).

The typical data privacy officer works single-handed on a part-time basis.

Both internal and external data privacy officers generally do not work solely in this capacity (and are thus 'part time'). Up to a company size of 5000 employees, these predominate at about 80%. Even in the group of companies with between 5000 and 50,000 employees, 46% of data privacy officers are employed only on a part time basis (see 4.2.3).
The respondents employed on a part time basis devote on average 1.3 days per week to carrying out their function as data privacy officer (see 4.2.4). One half of the sample assess the time available to them as sufficient. Here, data privacy officers in small companies with less than 50 employees are very disproportionately satisfied with the time available to them. In this category the figure is 81%, but in the other size categories only 29-39% of the data privacy officers responded to the question of the time available for carrying out their duties with 'sufficient'. Even among data privacy officers who act in this capacity on a full-time basis, between 20 and 40% of respondents still assessed the time available to them as not sufficient (see 4.2.5).
The data privacy officers report regularly to their management, even when they have not been requested to do so (in 49% of companies; see 4.2.8). In about 70% of all companies, employee training on questions of data privacy is carried out at least annually (see 4.2.11). The vast majority of the data privacy officers carry out internal data protection training, while only a small number work with external providers; nevertheless, 35% of the data privacy officers resort at least to the medium of online training. Viewed in relation to the company size categories, in companies with over 50,000 employees 65% of data privacy officers use online training, while the rate of use falls with company size to just 25% among companies with under 50 employees (see 4.2.13).

Data protection violations in the company

For the data privacy officer to carry out his/her duties successfully, information must be available concerning data protection violations. 38.15% of the in-company data privacy officers do not feel sufficiently well informed about data privacy violations within the company. Given that the sample group in question consists primarily of highly experienced data protection officers, this high proportion is alarming. In the company groups of 5000 employees and above, two thirds of the data privacy officers feel sufficiently well informed of data privacy violations in the company; in small companies it is 83% (see 4.3.1).

Since August 2010 section 42a BDSG has postulated an obligation to notify the competent authority in the event of personal data being unlawfully obtained by a third party if this threatens serious harm to the rights or legitimate interests of the data subjects affected. This relatively new regulation in the BDSG has generated a need for clarification. The results of the survey give clear proof to the relevance of such audits where 20.7% of the data privacy officers questioned are already carrying out such an audit (see 4.3.2) and yet already 4.9% of the companies questioned were obliged to notify (see 4.3.3). Most frequently, companies with over 50,000 employees (18% of these companies) had to notify the affected data subjects.

The probability that companies will be audited by the regulatory authority increases once a notification has been given under section 42a BDSG by a factor of three. The most important cause of data privacy violations was named by the data privacy officers questioned as negligence and ignorance on the part of individual employees. Within companies, the "sales and distribution" and "marketing and customer support" departments were the most serious data privacy violation offenders (see 4.3.7).

The result of a cross-comparison between data protection training and data privacy violations gives convincing proof of the effectiveness of regularly provided training. Infringements caused through ignorance are reduced by up to 36% in companies that carry out regular training, according to the data privacy officers questioned (see 4.3.6). In the ranking of the triggers for data privacy infringements, "carelessness with the IT infrastructure" is higher than "documents left lying in printers" and "unencrypted/unsecured IT devices" (see 4.3.6).
In the experience of the data privacy officers questioned, suitable disciplinary action is only instigated for about 51% of the data privacy violations detected (see 4.3.10).

Data protection training (including online) is effective and results in fewer infringements.

The data privacy officer in the company

The external service providers questioned support an average of 6.5 companies in the capacity of data privacy officer (known as external data privacy officers); nine support only one client, 38 support between two and ten clients, seven support between 10 and 20 and three of the external data privacy officers support between 20 and 25 companies (see 4.4.1).

The external data privacy officers have been appointed for an average of 4.3 years and the internal data privacy officers have been in post in the company for 5.9 years (see 4.4.2).

72.5% of the data privacy officers questioned are of the view that they are able to pursue their activity in the company without restrictions. 11% of all data privacy officers have both answered negatively to the question whether they can pursue their activities without restriction and been critical of the support given to them by management, the availability of personnel support and their involvement in projects (see 4.4.4). Similarly, 73% of respondents are of the view that management fulfills its obligations in respect of data protection (see 4.4.5).

Nevertheless, 66% consider the support of management to be sufficient (see 4.4.6), 62.5% regard their annual budget (see 4.4.8) and 58% regard the availability of personnel support (see 4.4.10) as sufficient. The average annual budgets available to data privacy officers in companies with up to 50 employees €1163, in companies with up to 500 employees €2773, up to 5000 employees €13,005, in companies with up to 50,000 employees €46,073 and in companies with over 50,000 employees €666.706.

75% ***...can work without restrictions***

... management recognizes its obligations

The vast majority of data privacy officers experience the technical departments in the company as cooperative. This response clearly reflects the particular situation in the companies questioned, which have often had a data privacy officer in post for many years. In the ranking of the expertise required for fulfilling their own duties, data privacy law is naturally in first place (average score of 2.18 on a scale of 1 to 6), but this is followed closely by issues of IT security (2.82) and knowledge of the organization of operations (2.88). Knowledge of auditing (3.78) and business management (4.31) were given least importance by the respondents.

44.9% of the data privacy officers stated that they are already involved in the planning phase for data privacy law evaluation projects, 17.5% that they are involved in the investment decision at the start of the project and yet still 33% are involved, contrary to the legal regulations, only in live operation (see 4.4.15).

When the data privacy officer is not involved in new projects at an early stage, the main detrimental effect is the discovery of unlawful gathering and processing of personal data. When the data privacy officer is involved at an early stage, the rate of data privacy violations discovered is halved.

The register of procedures

Nevertheless, almost 10% of the data privacy officers questioned stated in the survey that the company does not maintain a register of procedures (see 4.5.1). When asked about the number of individual procedures within one procedure overview, the data privacy officers gave an average of 267 procedures per register of procedures (see 4.5.2). Only 42% of companies stated that they have introduced a regulating process to update the register of procedures (see 4.5.3).

The data privacy officers are additionally responsible as the controller for data processing work outsourced to service providers. Under section 11 BDSG the controller is legally responsible for data protection if he commissions service providers to process personal data. The responses of the data privacy officers indicate that self-monitoring and other control measures continue to have precedence over reference to certifications (22% of all indications) of the outside contractor. Third parties are only consulted for monitoring in rare cases (see 4.5.8).

Data protection certification

The survey proves that data protection certification is still at an early stage (see 4.6.1), but is being increasingly requested, particularly by large organizations (see 4.6.2, 4.6.3).

Regulatory authorities

Asked about their experiences with the activities of the data protection regulatory authorities (see 4.7.1) a slight majority (52%) holds the view that these should monitor less. The respondents were unanimous in the view that the regulatory authorities should act in a consulting capacity (90%) and offer training (75%). 60% also called for certification by the regulatory authorities.

Criticism of the lack of assertiveness of the regulatory authorities was expressed by only 33% of the data privacy officers, who saw the authorities as "toothless tigers" (see 4.7.2). In the experience of 58.5% of the data privacy officers, data privacy violations are sufficiently prosecuted by the regulatory authorities (see 4.7.3) and 56% believe that the penalties imposed were sufficient (see 4.7.4).

Nevertheless, 24.5% of the data privacy officers expressed doubts as to the competence of the regulatory authorities (see 4.7.5). Only 75% of the in-company data privacy officers have the impression that the regulatory authorities are taken seriously in their company (see 4.7.6).

Training of data privacy officers

The Federal Data Protection Act (BDSG) sets personal and material requirements for the appointment of a data privacy officer that have been concretized by a resolution of the supreme regulatory body. To date there exists no vocational training or professional qualification with a legal basis. This lack is an issue of complaint not only for trainers and the professional association but also for 65% of respondents to the survey. A majority among the practitioners argues in favor of a legally regulated training.

51% of the participating data privacy officers stated that they gained their qualifications through continuing professional development measures; 27% rely on the experience they have gained in the course of their work and 12% rely on prior knowledge obtained from a course of study (see 4.9.2). Among a selection of continuing professional development options, specialist conventions were most frequently selected as a possibility for further training (28.8% of responses). The offerings of TÜV (20.5%) and the German Association for Data Protection and Data Security (GDD) (18.8%) received almost equal preference. 33 survey respondents stated that they had participated in training events by both TÜV and GDD.

Only 19 respondents said that they had not made use of any continuing professional development options. Of these, ten have been in post for five or more years (see 4.9.3). 37% of the data privacy officers questioned stated that they attend ongoing training events on a monthly basis, and a total of 83% do so at least once per year (see 4.9.6). Of the training events used by the data privacy officers, 56% also include a final examination on at least some of the training outcome (see 4.9.9).
On closer examination of the results it can be seen that less qualified data privacy officers tend to undertake less continuing training while highly qualified officers undertake training significantly more often, including within their work (see 4.9.8).

EU data protection reform

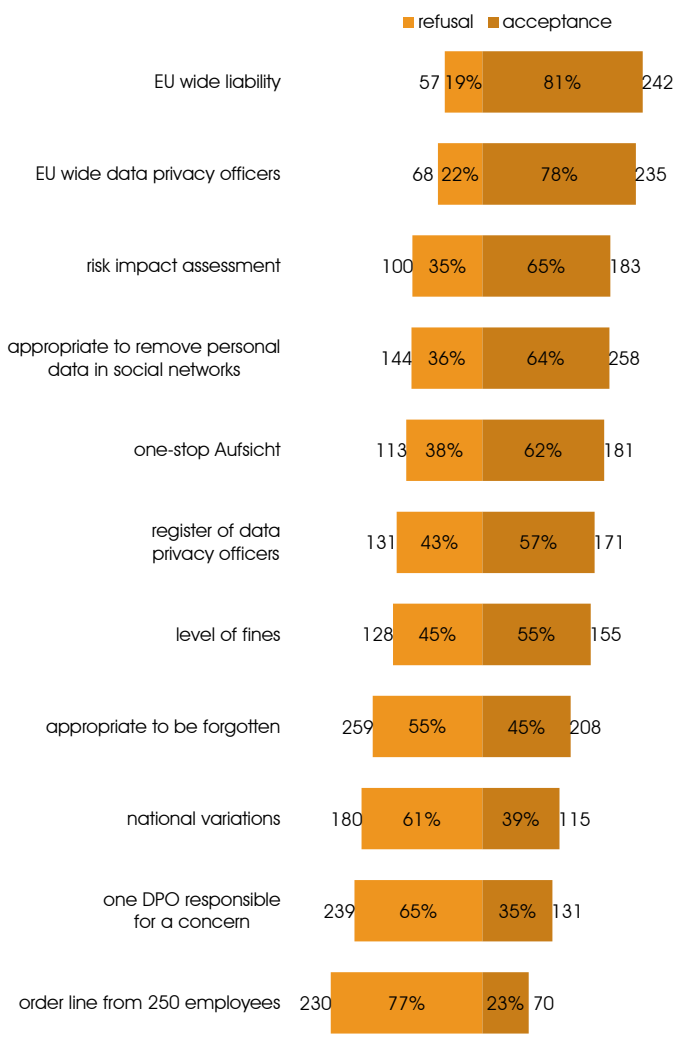
The survey, from the first half of 2012, also contains the first evaluations and opinions on the new EU data protection regulations and thus provides an indication of the disposition of German data privacy practitioners towards the proposed reform, which will also influence German data privacy law. While the data privacy officers do not believe that implementing the proposals will improve the situation for persons affected by violations, they regard the principal innovations in data privacy legislation as fairly positive (see 4.10).

40.6% of the data privacy officers questioned expect an improvement in the level of data protection in Germany, while 59.4% of those questioned anticipate a worsening. The fear that the competent data protection regulatory authority could have an influence through its activities on a company's choice of head office location within Europe, resulting in a "race to the bottom", was shared by 33% of the data privacy officers questioned. A clear majority of 77% of the data privacy officers however regard this fear as "fairly improbable" or "probably not".

Above all, the planned EU-wide liability of the regulation, the proposed level of the fines, the right to remove personal data in social networks and from all data receivers (the right to be forgotten), the establishment of a legal basis for data privacy officers, the proposed risk impact assessment and the one-stop shop for enforcement by a single national regulatory authority for international data transfers were predominantly considered positive.

The German data privacy officers were somewhat critical of the proposed national rights of deviation, the obligation to appoint a data privacy officer only in organizations with over 250 employees and the appointing of only a single data privacy officer within a group of companies. Additionally, the data privacy officers expect a higher level of outlay in the event of grievances, but neither a better level of data protection in Germany nor better possibilities for monitoring by the data subjects through the implementation of the proposals.

The envisaged obligation to notify all data receivers in the event that the data subject intends to erase data (erasure chain) is correct for 56% of the data privacy officers, but at the same time 45.9% of respondents are doubtful about the enforceability of this legislative idea.



3. Methodology and operational processes

The target groups addressed for this survey consisted of data privacy officers from companies in a wide range of industries.

We were supported by the Department of Business and Social Statistics at TU Dortmund University, headed by Prof. Dr. Walter Krämer, in the operational implementation of this market investigation.
From the outset it was necessary that the survey target the persons responsible for data protection within each company. Thus the appointed data privacy officers were addressed directly so that it would be possible to request one appraisal per company.
To be certain that in fact only the actual data privacy officers would respond, only those data privacy officers were directly targeted whose name and work postal address were publicly known. Under these criteria, 1841 requests for participation were sent out. No check was made as to whether the 910 requests sent by e-mail had actually reached the data privacy officer(s) of the company. It must therefore be assumed that some of the requests did not reach their addressee, in part because the addresses had been collected over a period of several years.
It is however impossible to determine the size of this fraction.

A total of 2751 participant invitations were sent

In the case of data privacy officers whose e-mail address for marketing was known, the invitation to participate in the survey was sent by e-mail, with a link to a special online instance of the questionnaire prepared for that individual, which was anonymized immediately it was successfully completed. Respondents to the survey who were contacted by postal mail received a login ID that enabled them to participate online using their e-mail address. Both groups were also able to print the questionnaire and mail it in. Each e-mail address was allowed to participate only once. External data privacy officers could thus take part on behalf of multiple companies by using a different e-mail address for each client, for example, and requested more than one ID. This process gave external data privacy officers the possibility of demonstrating differing conditions in the various companies. All other participants were invited with the paper version of the questionnaire sent to them by mail and returned by them anonymously. If anybody did not wish to participate online, he or she could print out the questionnaire and send it by postal mail. The data from these questionnaires was also made anonymous as quickly as possible.
In order to evaluate the results of the survey, other data such as the size of the company (in terms of number of employees) was also queried.
By comparing these figures with those published by the Institut für Mittelstandsforschung Bonn (IfM) on the basis of the figures of the federal company register for 2009, the following picture emerges:

Company size	Participating DPOs			Number of companies*	
up to 50	65	17.4%		247,358	79.1%
up to 500	152	40.8%		60,241	19.3%
up to 5000	122	32.7%			
up to 50,000	28	7.5%	= 41.8%	5151	1.6%
over 50,000	6	1.6%			
Total	373	100%	100%	312,750	100%

*Institut für Mittelstandsforschung Bonn

In this table all companies with fewer than 10 employees were left out. If one assumes that also in companies with more than 10 employees many do not have to appoint a data privacy officer, the picture is only slightly changed. By leaving out 20% of companies with up to 50 employees, the overall result is as follows:

This is not a surprise, since the officers here are qualified specialists who must represent and deal with the issues of data protection in large and very large organizations. Here the view of cross-company aspects of data protection is probably strongly represented and thus an increased level of willingness can also be expected for such personnel to participate in a survey of this kind.

Company size	Participating DPOs			Number of companies*	
up to 50	65	17.4%		197,886	75.2%
up to 500	152	40.8%		60,241	22.9%
up to 5000	122	32.7%			
up to 50,000	28	7.5%	= 41.8%	5151	2.0%
over 50,000	6	1.6%			
Total	373	100%	100%	263,278	100%

*Institut für Mittelstandsforschung Bonn

The companies with under 50 employees are here considerably under-represented in comparison to the company structure in our survey. This is unsurprising since these companies often do not publish the name of their data privacy officer, and so could not be included in the distribution list for this survey.
The companies with between 50 and 100 employees are under-represented for the opposite reasons. Here the information is far more frequently made public and the data privacy officers tend to be interested in cooperation. Instead of the statistical fraction of about 20%, they appear in the survey roughly twice as frequently. Companies with over 250 are treated as 'large' in accordance with EU statistics and are no longer separately differentiated.
The companies with more than 5000 employees are in relative terms the most strongly represented in this survey: while they only represent about 2% of companies in Germany in general, in terms of participating data privacy officers they make up over 40%.

In summary it may be said that the results substantially reflect the opinions and assessments of data privacy officers of large and larger companies: 40% of respondents are from companies with over 500 employees and almost 10% are from companies with over 5000 employees.

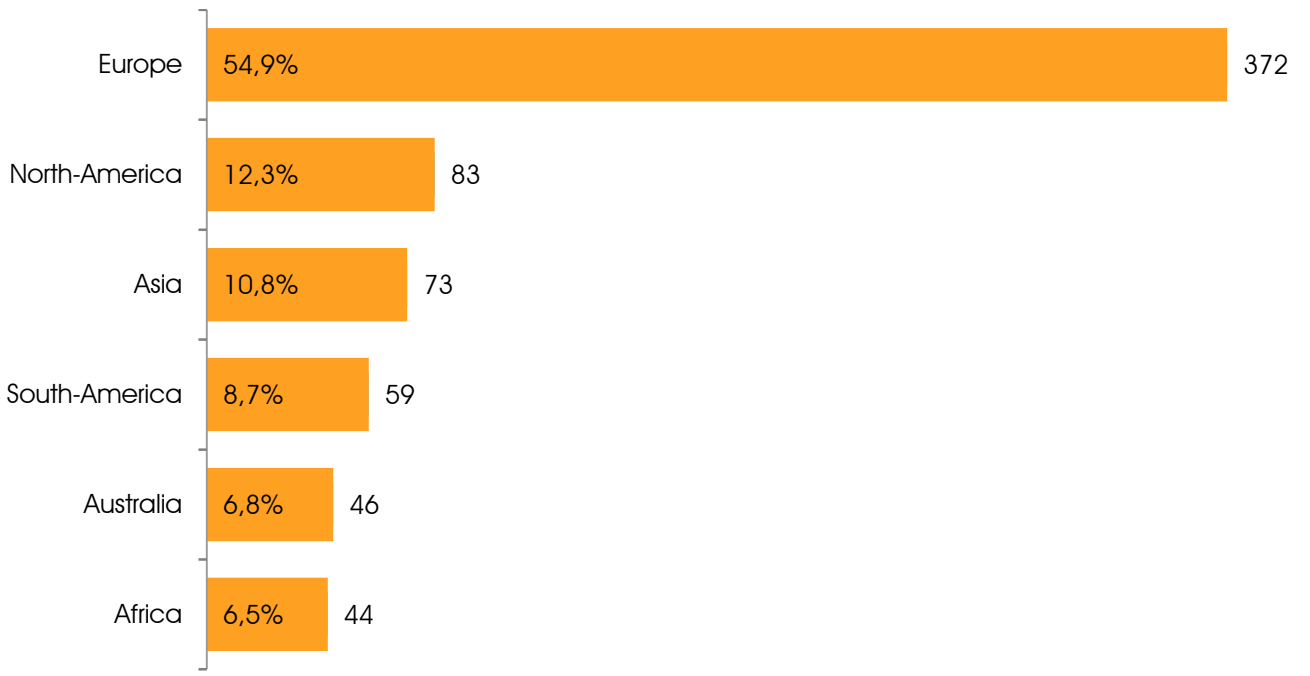
This is underpinned by certain other results, e.g. information on the international nature of the companies, and also information on the frequency of audits by the regulatory authorities. For this survey, however, the representativity in relation to company structure was not decisive, but rather a clear picture of data protection practice in those companies that have already appointed a data privacy officer. It therefore gives emphasis to qualitative evaluations of the practice of implementation of the requirements of data protection law.

Deviations in the totals arise from those questionnaires in which not every question was given an answer.

4. The results in full

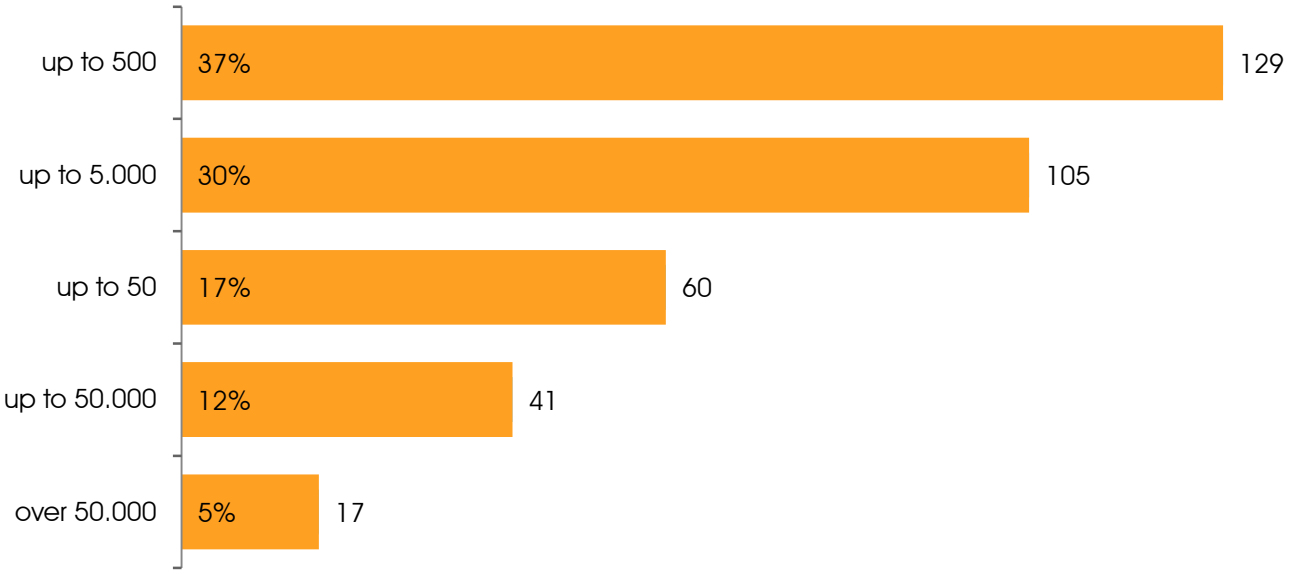
4.1 Structure of the companies surveyed

1. "On which continents is your company represented?"



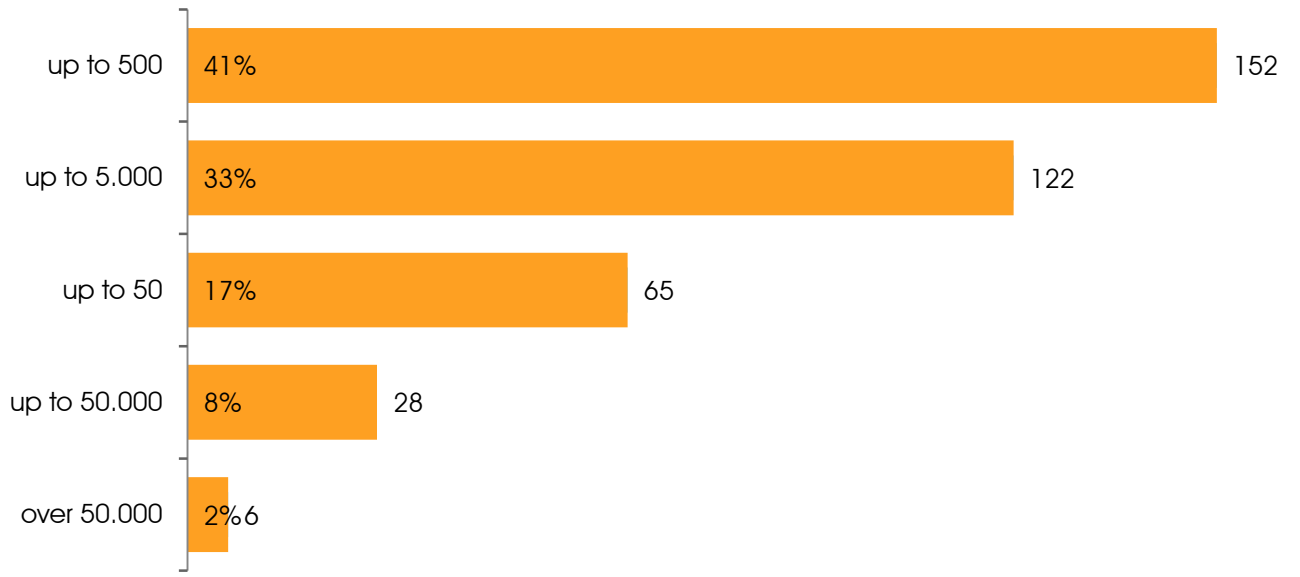
Of the 375 participating companies, 372 (54.9%) are represented in Europe with one branch, 73 (10.8%) also in Asia, 44 (6.5%) also in Africa, 46 (6.8%) also in Australia, 83 (12.3%) also in North America and 59 (8.7%) also in South America. 283 of these companies are represented solely in Europe; eleven on two continents, 17 on three, 18 on four and 15 on five; 29 companies are globally active.
The professional expertise is thus reflected in the results of the survey from both small and medium-sized businesses and also from globally active German corporations.

2. "How many people does your company employ around the world?"



Of a total of 351 participants, 17% stated that they worked as data privacy officers in companies with up to 50 employees, 36.6% in companies with up to 500 employees, 29.8% in companies with up to 5000 employees, 11.6% in companies with up to 50,000 and 4.8% in companies with over 50,000 employees.
It can be seen that officers from large companies made up a disproportionally large number of the participants. This can be attributed to the data collecting methodology (see section 3.). The survey was addressed to 2751 data privacy officers known by name, while companies without a data privacy officer were left out.

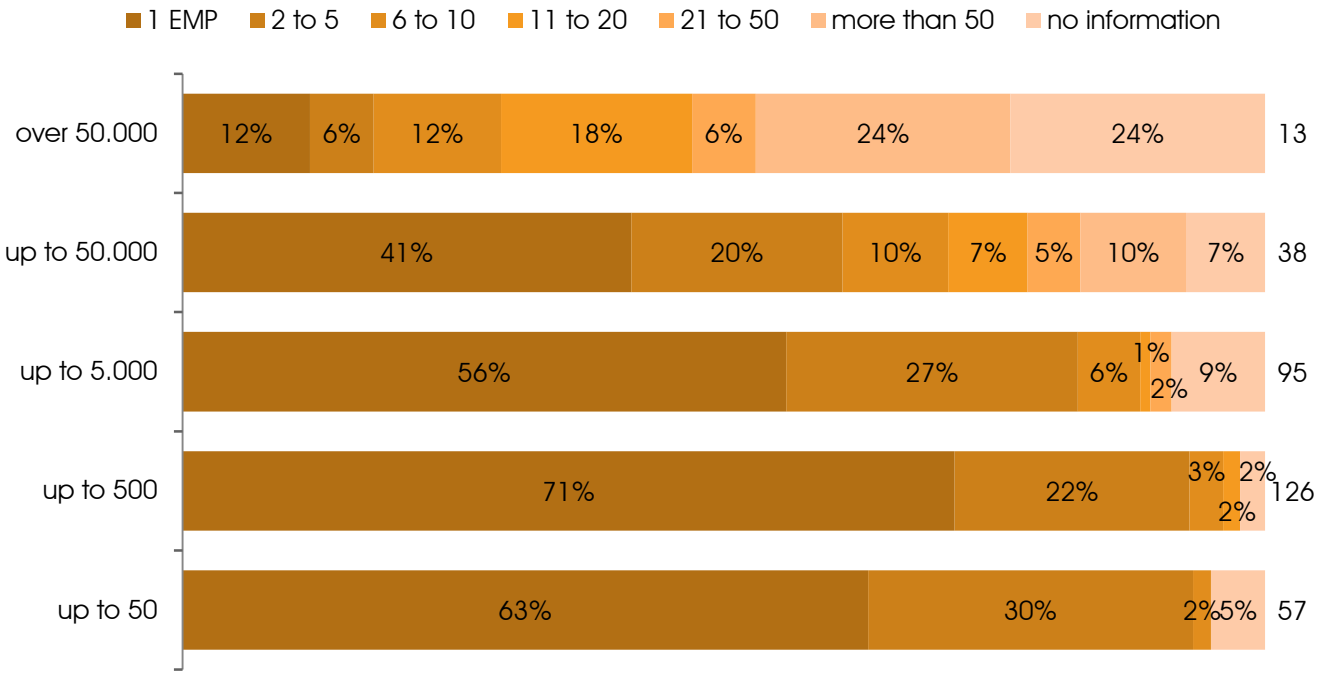
3. "How many people does your company employ across Germany?"



Across Germany, 17.4% of the participating companies employ up to 50 employees, 40.8% up to 500, 32.7% up to 5000, 7.5% up to 50,000 and 1.6 % over 50,000.

4. "How many employees in your company work directly with data privacy?"

From the 353 useable responses it was found that a total of 1754 employees worldwide, of whom 1311 are in Germany, work directly with data privacy in the participating companies - thus on average 5 or 3.7 employees per company, respectively. However, 229 respondents gave only one employee worldwide and 202 only one employee in Germany, and 48 and 71 respectively stated that two employees worked with data protection in their company. In terms of the company size classifications, the distribution appears as follows:



Even in the group of companies with up to 50,000 employees worldwide, a single data privacy officer is the usual case in 41% of these companies. It is clear from this that in Germany the data privacy officer generally works single-handedly and only in about 30% of companies with up to 5000 employees is a second employee also involved.

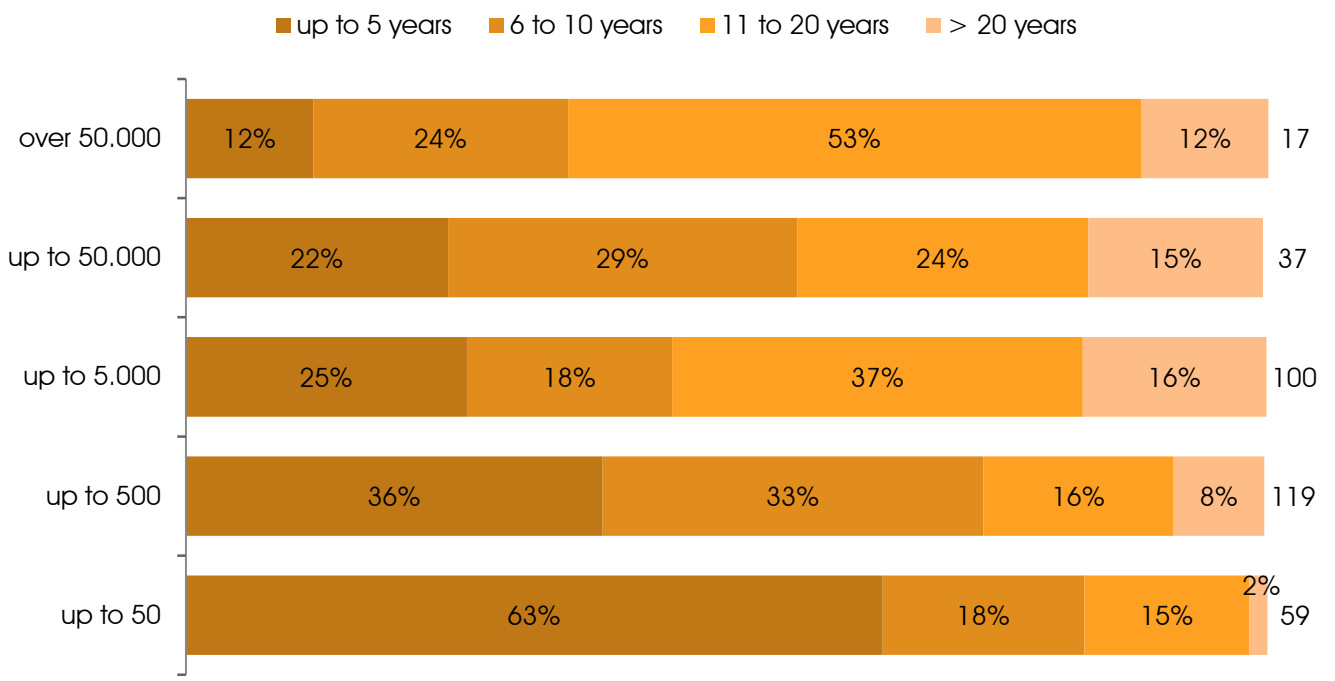
5. "Is your company a subsidiary of a parent company?"

64.6% of all companies surveyed are not affiliated to a parent company.
This unusually high number of subsidiary companies as the subject of the survey can also be explained by the means by which the addresses were generated (see section 3). The survey was directed only towards data privacy officers who were already publicly known, and so an above-average number of corporations could be included in the survey.

4.2 Data protection practice in the company

1. "For how many years has there been a data privacy officer appointed in your company?"

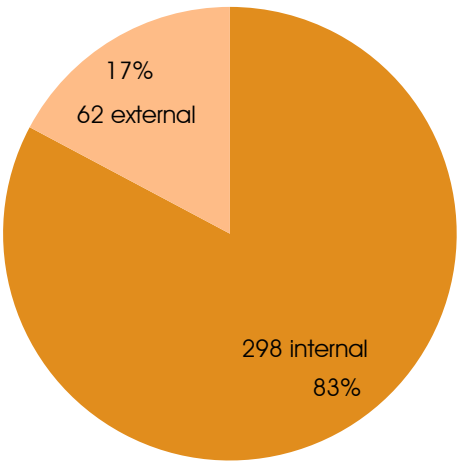
The average length of appointment in the company of the data privacy officers involved was given by the survey results as 10.4 years.
The data privacy officer, whose appointment was obligatory, was established in German data privacy law as early as 1977 in the BDSG as a means of internal self-monitoring. The 2009 revisions extended the regulations to protection against unfair dismissal, so that the prolonged periods of employment of the appointed data privacy officers was not only justified on a technical basis but also had a legal explanation.



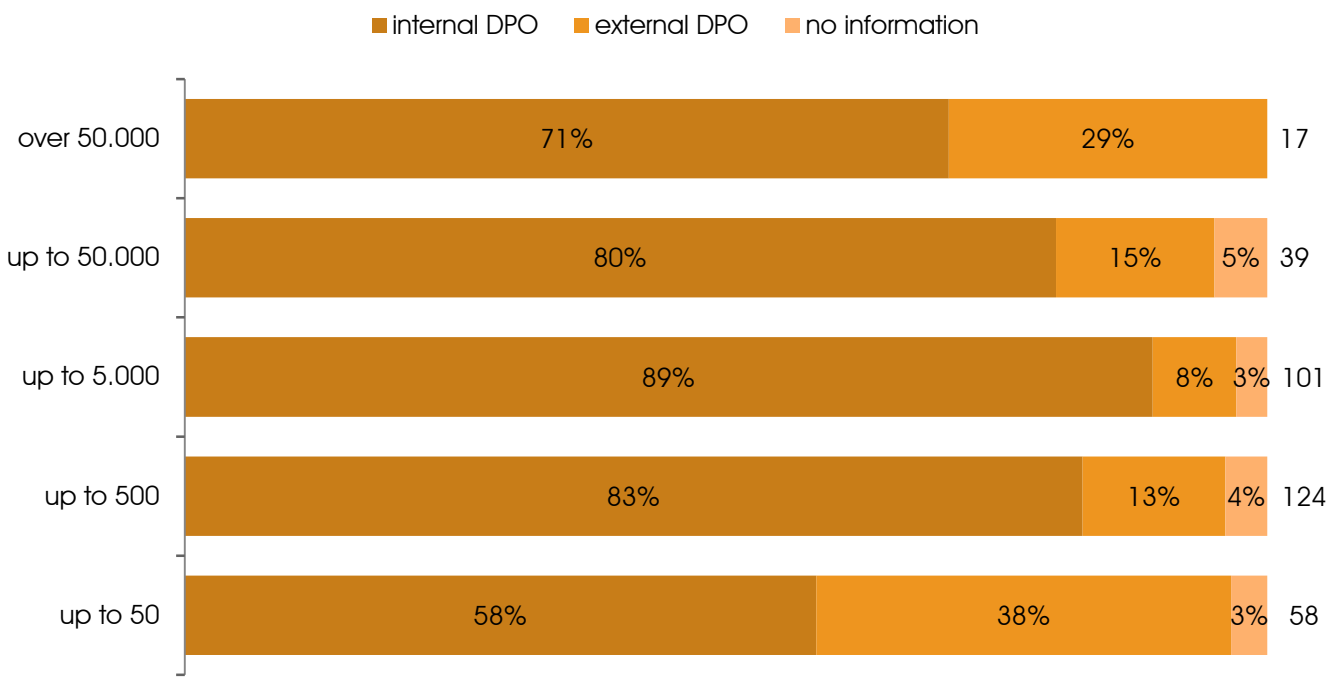
If one compares the size categories of the companies with the various periods of appointment, it can be seen that in companies with up to 50 employees, efforts have been made in the last five years to catch up with the obligation to appoint an officer; the large companies, meanwhile, have already employed data privacy officers for considerably longer. The larger the company, the longer have data privacy officers already been working there.

2. "Have you been appointed as an internal or an external data privacy officer?"

The BDSG offers the possibility of satisfying the general legal requirement of appointing an employee as an (internal) data privacy officer by appointing an external data privacy officer (section 4 para. 2 sentence 3 BDSG). This may be any person outside the data controller - thus either external specialist providers or other (internal) data privacy officers of related companies. The number of internal and external data privacy officers in our survey did not however give a representative picture of the distribution among the totality of German businesses but rather the composition of the group of respondents.



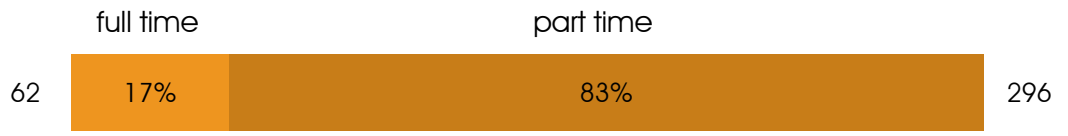
Information from the data privacy officers by company size:



The internal data privacy officer is the general rule in practice; 58% of the companies with up to 50 employees and 71% of those with over 50,000 employees have appointed their own employees as data privacy officers. The companies that have made greater use of the opportunity to appoint external data privacy officers are those with up to 50 employees and those with over 50,000; the motivation in the two categories is however different. While the small companies certainly opt for external data privacy officers for reasons of capacity and qualifications, in the very large companies the reason for appointing an external officer is rather the possibilities for specialization.

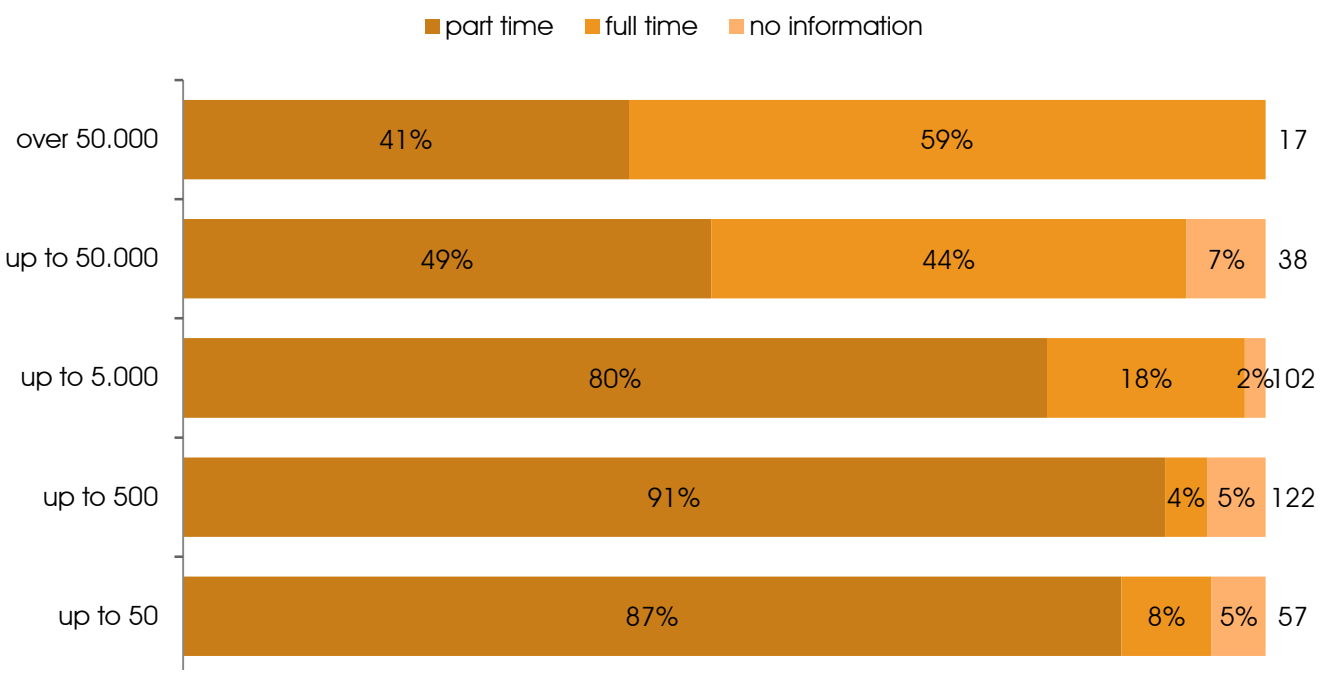
This distribution would seem to suggest that companies in the range of 5000 employees appoint an external data privacy officer least frequently. However, the increase above this order of magnitude is covered by far fewer cases than is that below it, and therefore we request a cautious approach on methodological grounds.

3. "To what extent do you devote yourself specifically to the function of data privacy officer?"

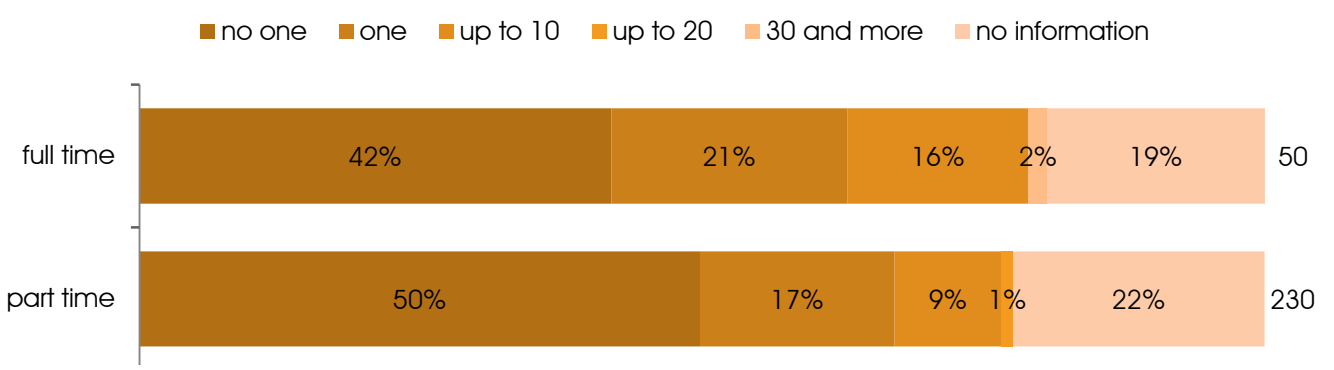


The legal prerequisite for the lawfulness of the appointment is the aptitude of the data privacy officer for fulfilling his/her duties. This also includes the granting of sufficient work time. With the decision of the Düsseldorfer Kreis of 24-25 November 2010 the highest regulatory authorities in Germany formulated minimum requirements in respect of the expertise and independence of data privacy officers under section 4f paras 2 and 3 BDSG but did not concretize them further here. The utilization and workload of the data privacy officer is principally influenced by the size of the controller, the number of controllers to be supported, the particularities of data processing in the particular industry and the level of protection required for the personal data to be processed.

Information from the data privacy officers by company size:



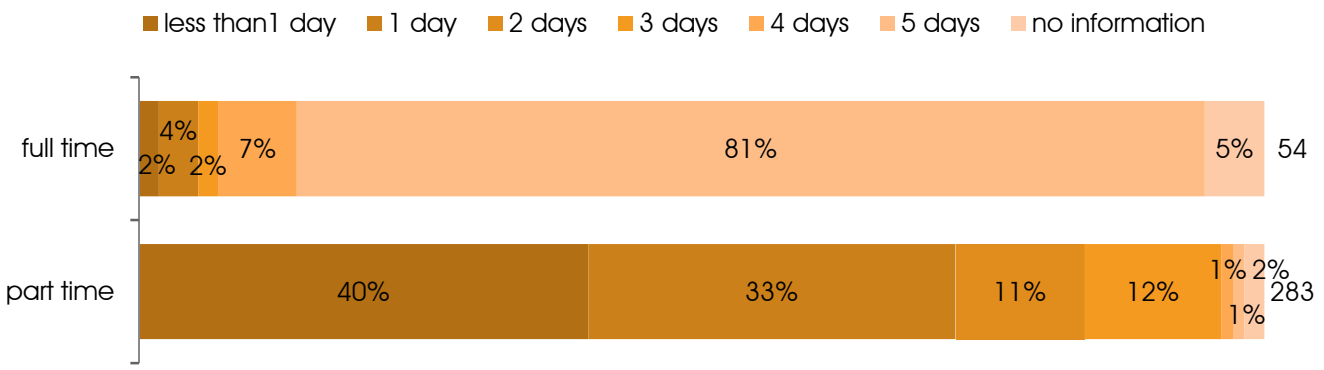
According to the results of the survey, as a rule the data privacy officer in small and medium-sized companies is appointed on a part-time basis and even in organizations with over 50,000 employees worldwide the officer still works part-time in 46% of cases.



When it comes to providing additional employees it clearly makes little difference whether the data protection officer himself acts on a full-time basis or whether this function only occupies a part of his work time.

4. "Roughly how many days is that per week?"

On average the data privacy officers questioned have 1.9 days per working week available for performing their duties. The average for data protection work among only the part-time officers is 1.33 days per week.

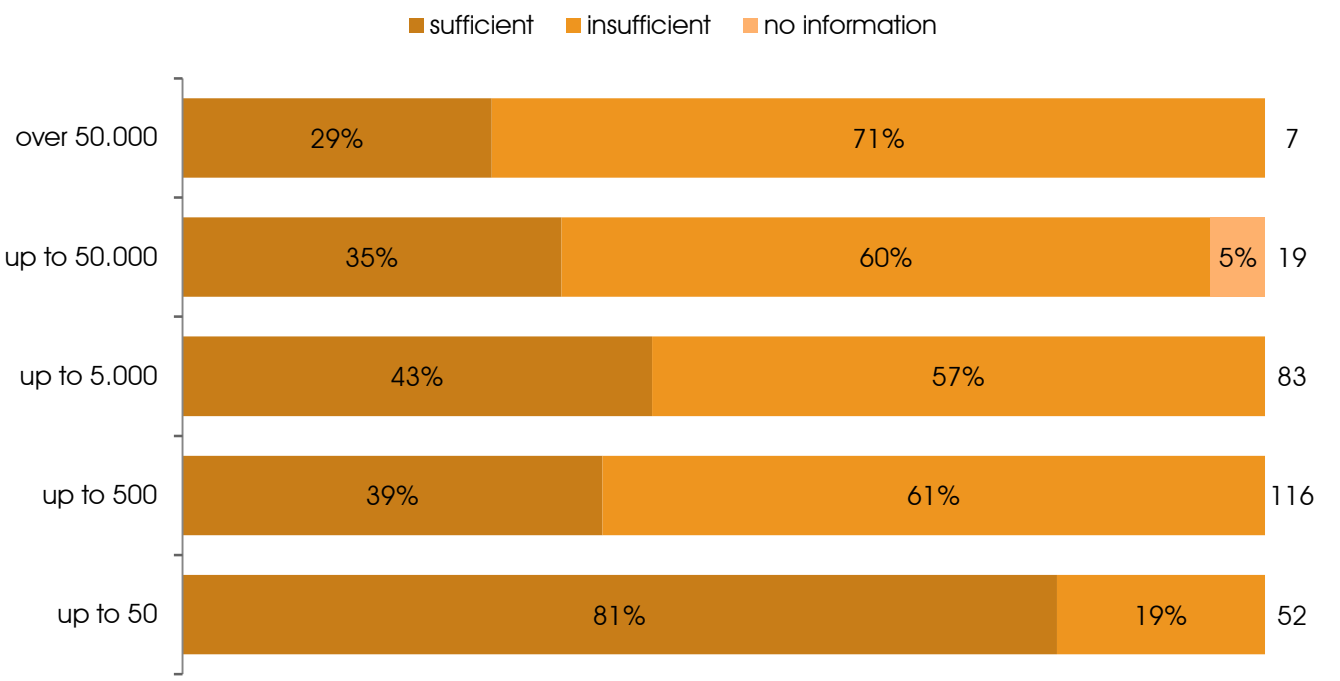


40% of those only partially appointed as data privacy officers spend less than one day per week performing their duties.

5. "Do you consider the amount of time available to you for carrying out your duties to be sufficient?"

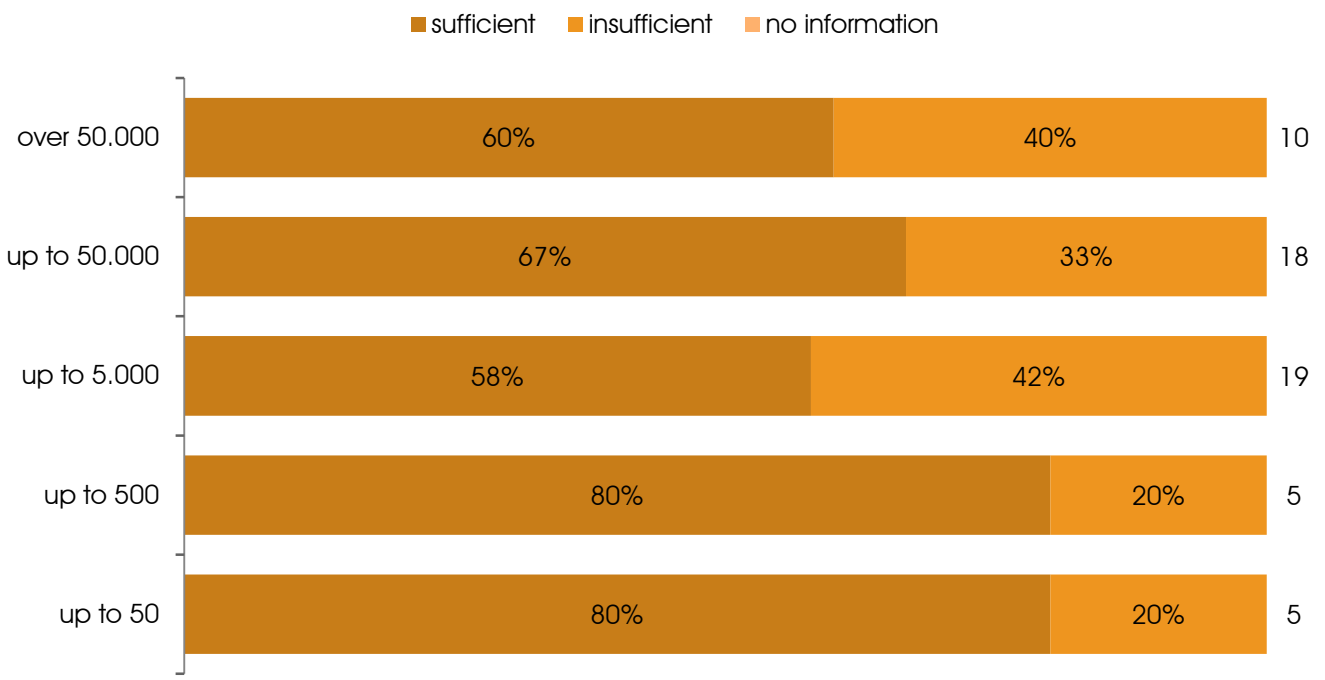
Half of the data privacy officers questioned consider the time available to them to be sufficient.
Of the 296 data privacy officers who work part time, 139 (47%) consider this time to be sufficient; of the 62 full-time officers, 39 (63%) consider it sufficient. The "overworked" data privacy officers have on average 3.9 additional employees available to them who are engaged on data protection functions (c.f. 2.4). The data privacy officers who have sufficient time have an average of 3.04 staff available to them. The response appears as follows in terms of the size of the company.

Opinions of the data protection officers by company size:



If only the responses of those data privacy officers that work full-time are used to analyze the question, still 20% of those in companies with up to 500 employees respond with "not sufficient" and in companies with over 500 employees this figure still averages 38%. This finding from practice confirms the view that it is not the number of employees but the type of processing of personal data that must determine the qualifications of the data privacy officer and the level of resources (personnel and funding) required.

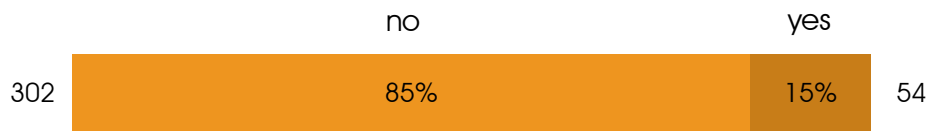
Opinions of full-time data privacy officers by company size:



6. "Is your company subject to the obligation to notify?"

The 30% positive responses to the question of the obligation to notify in special cases of the commercial processing of data reveals what is at first glance a surprising picture. Under section 4 BDSG the obligation to notify the regulatory authority of automated data processing activities does not apply so long as the company has appointed a data privacy officer. If such an officer has been appointed, only one exception applies: under section 4d para 4 BDSG the competent authority must be notified of the processes even if a data privacy officer has been appointed if they concern automated processing operations in which personal data is stored on a commercial basis for the purposes of transfer, transfer in anonymous form or for market or opinion research purposes. These notifications are held in registers by the appropriate regulatory authorities. Unfortunately, up to now only a few regulatory authorities have published the number of processes notified to them: for example the Bavarian state agency (Landesamt) registered 138 entries in 2009, according to its activities report, while 51 entries were recorded in Hamburg. Here it appears that an important condition for the notification of such processes is the appointment of a data privacy officer who is in a position to undertake the legal requirements in the company.

7. "Has your company had an audit from the regulatory authority?"

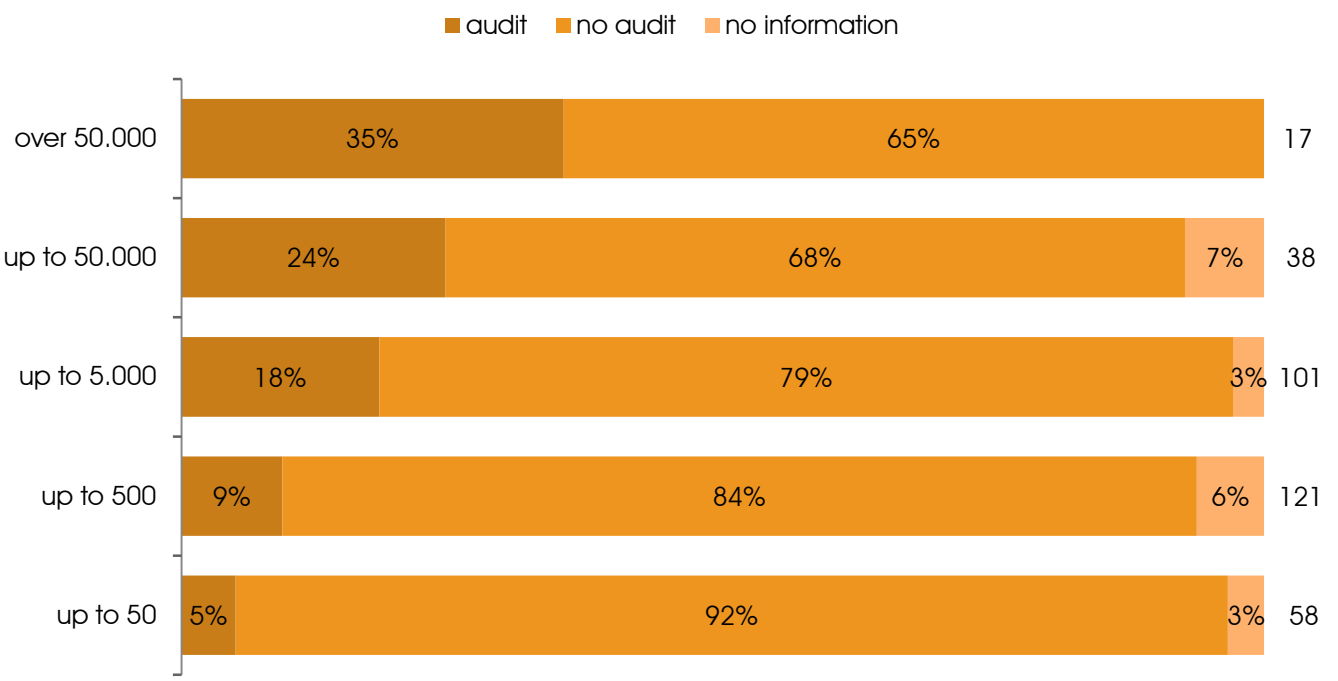


The quantitative discrepancy between the numbers of employees in the regulatory authorities to the number of companies is such that the response can be expected to be minimal. This would certainly also be the case in a representative survey of all companies. Within the present survey, however, the responses have been primarily from appointed data privacy officers in larger companies, which seems to increase the probability of experience with an audit by the regulatory authority.

The listing by company size reveals a sevenfold higher probability of being audited for companies with more than 50,000 employees. In this category 35% of respondent data privacy officers reported audits carried out by their respective regulatory authority. Even in the group of companies with 50 to 500 employees, 9% of data privacy officers reported an audit by the regulatory authority.

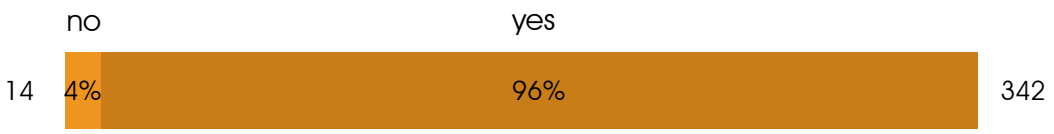
It is possible that the notion of the "audit" was not understood by all respondents in the same way. Actions such as questioning on certain legally prescribed features in a large number of companies by individual regulatory authorities may in itself be regarded by some of the individuals questioned as auditing.

Regulatory authority audits by company size:



The larger the company, the more frequently it is audited by the regulatory authority. Overall, 15% of the companies questioned have already been audited by a regulatory authority.

8. "As the data privacy officer, do you report direct to the directors?"

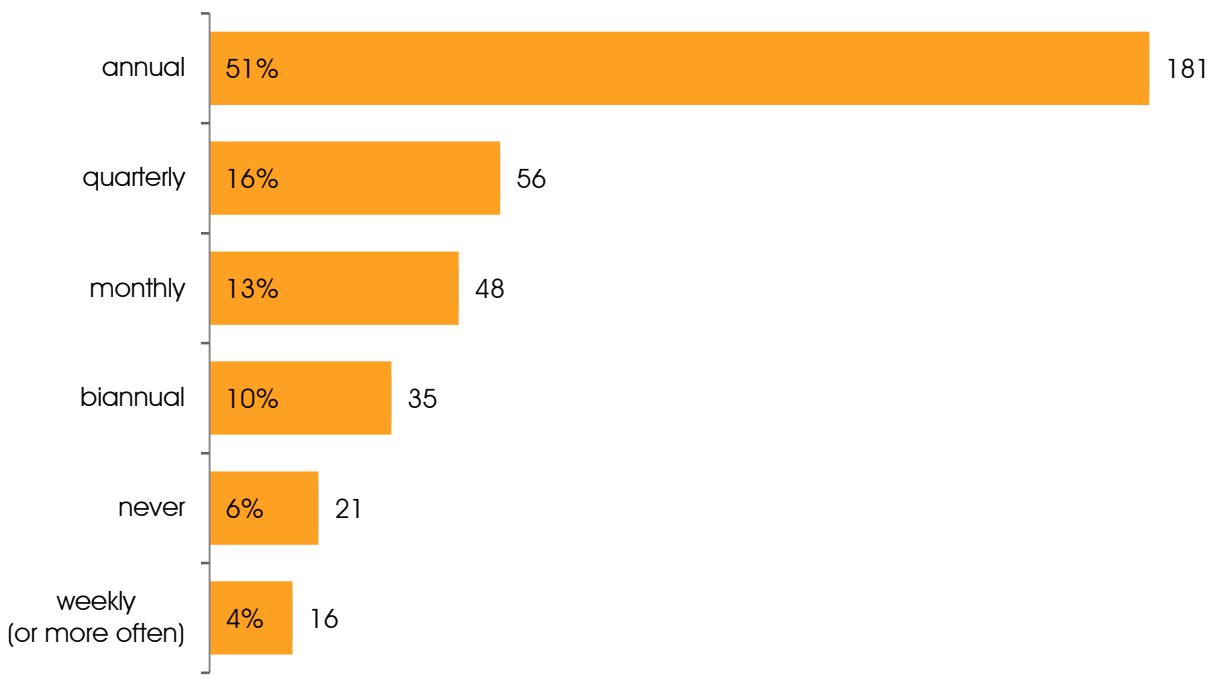


The subordination of the data privacy officer to the head of the controller is a mandatory legal requirement, section 4f para 3 BDSG. Nevertheless, 4% of the data privacy officers questioned answered this question with No. Two of these were in a company with over 50,000 employees worldwide, five in companies with up to 5000 employees worldwide and two in companies with up to 50 employees.

9. "Does your management require an activities report from you?"

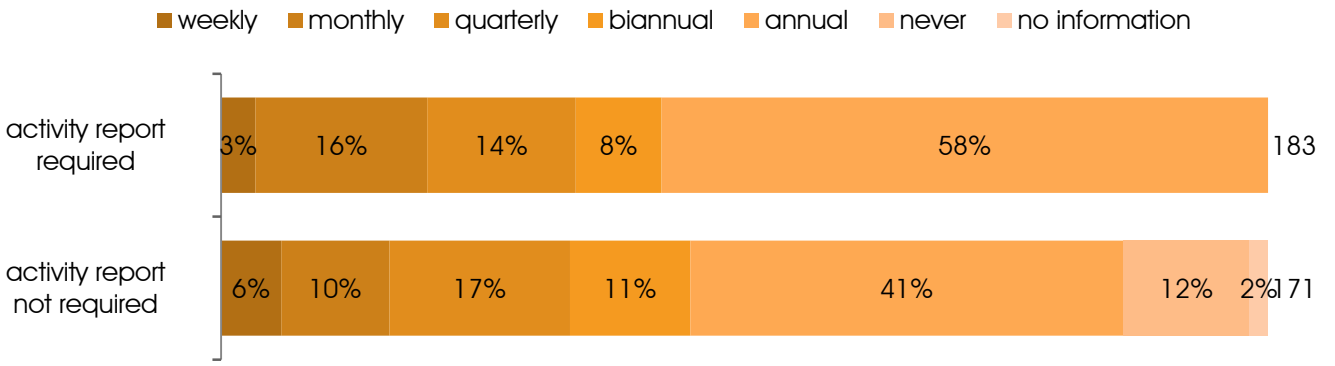
Unlike the case for public data privacy officers, obligated to Parliament as heads of the regulatory bodies, an activities report is not legally required of a data privacy officer in a private business. It has however proved itself as a reliable tool for governing the implementation of data protection regulations along reporting lines. Despite having appointed a data privacy officer, the management retains its full responsibility even in this area. 51.3% of management require a report of this type.

10. "How frequently do you report to management?"



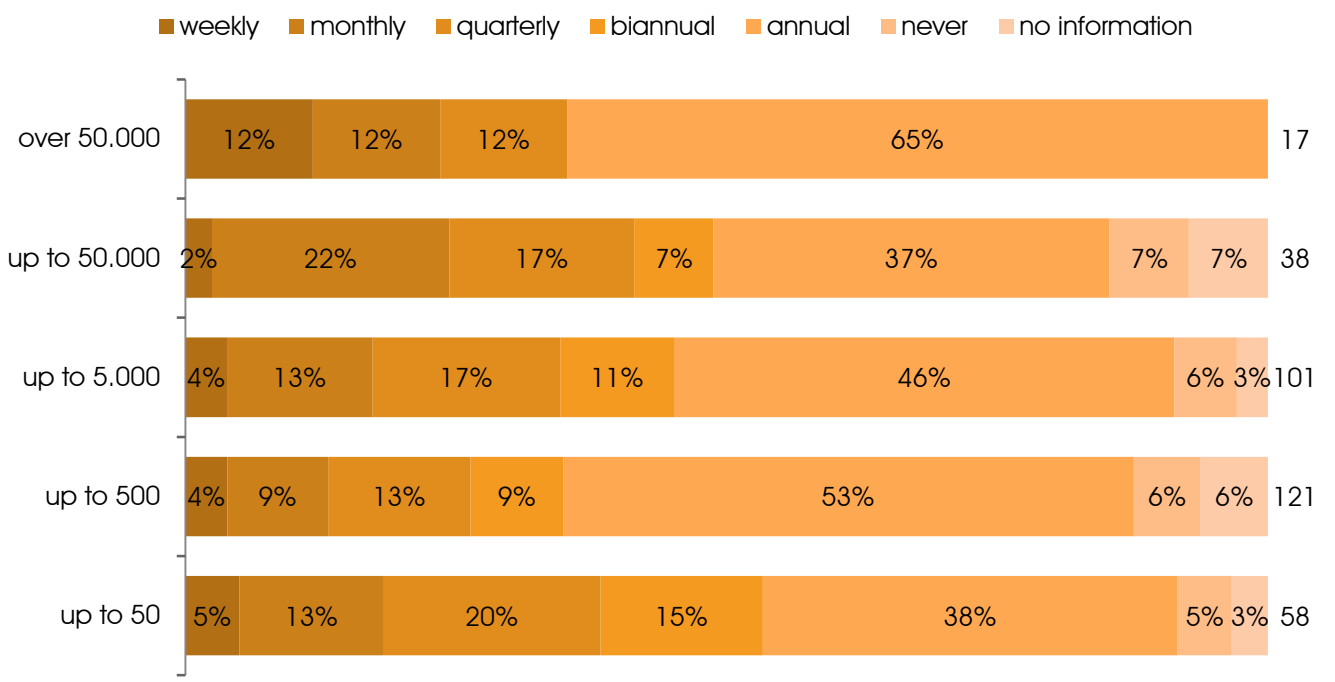
All 21 data privacy officers who responded to the question of the reporting obligation with 'Never' are also never required to report to their management. In the other 153 cases the data privacy officers produce a report though are not required to do so. Here it can be seen that the data privacy officers have realized that without a form of documentation of their own work and regular information delivered to management, it can be very difficult to pursue their own responsibilities in the company.

"What is the effect on the frequency of activities reporting when the management request this?"



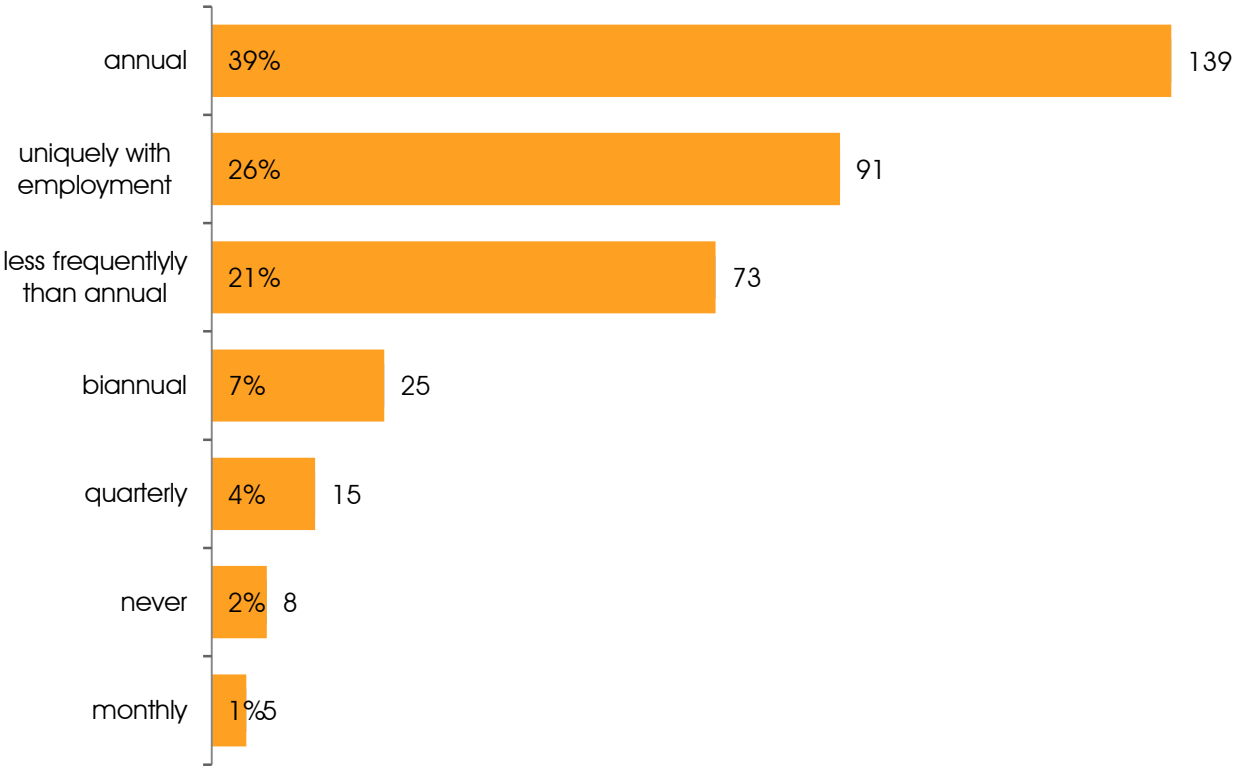
The frequency of reporting changes only slightly when the management requests it. It is clear that operational practices and the other internal reporting systems determine the frequency of reporting.

Frequency by company size:



The size of the company also does not appear to have a significant effect on the frequency of reporting.

11. "How often, generally, are your employees given training in data protection?"

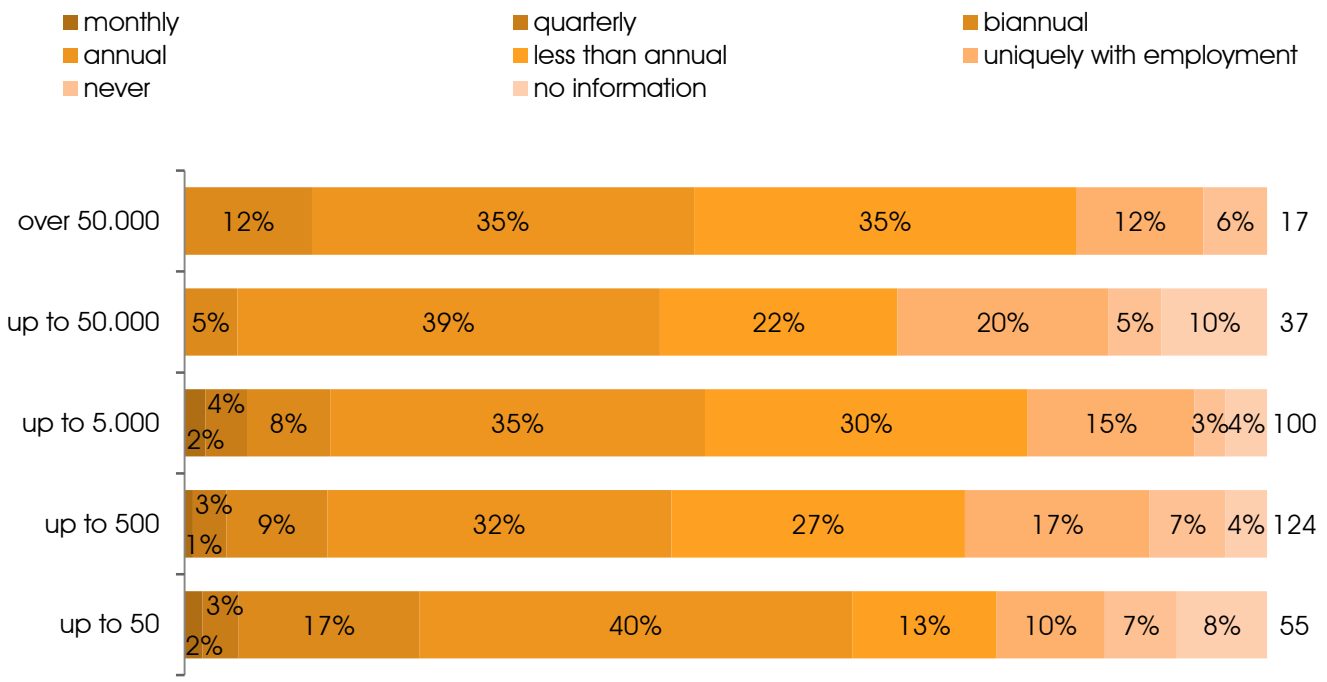


The core legal tasks of the data privacy officer include familiarizing the employees with the data protection provisions and with the various special requirements of data protection, section 4g para 1 point 2 BDSG. The manner and extent of this training depends on the particular conditions of the company in question and the particular area of activity. The extent, frequency and type of such training is decided by the data privacy officer in his own capacity.

26% of the companies train their employees only once in data protection, during their induction. This may be in conformity with the law in areas in which the processing of personal data takes place only occasionally and not electronically. An annual training, as stated by 40% of the practitioners, is the commonest practice, given the changing content of the work and the technical and organizational requirements placed on them. A shorter frequency of training may be necessary in sensitive areas and is practiced in 17% of the companies.

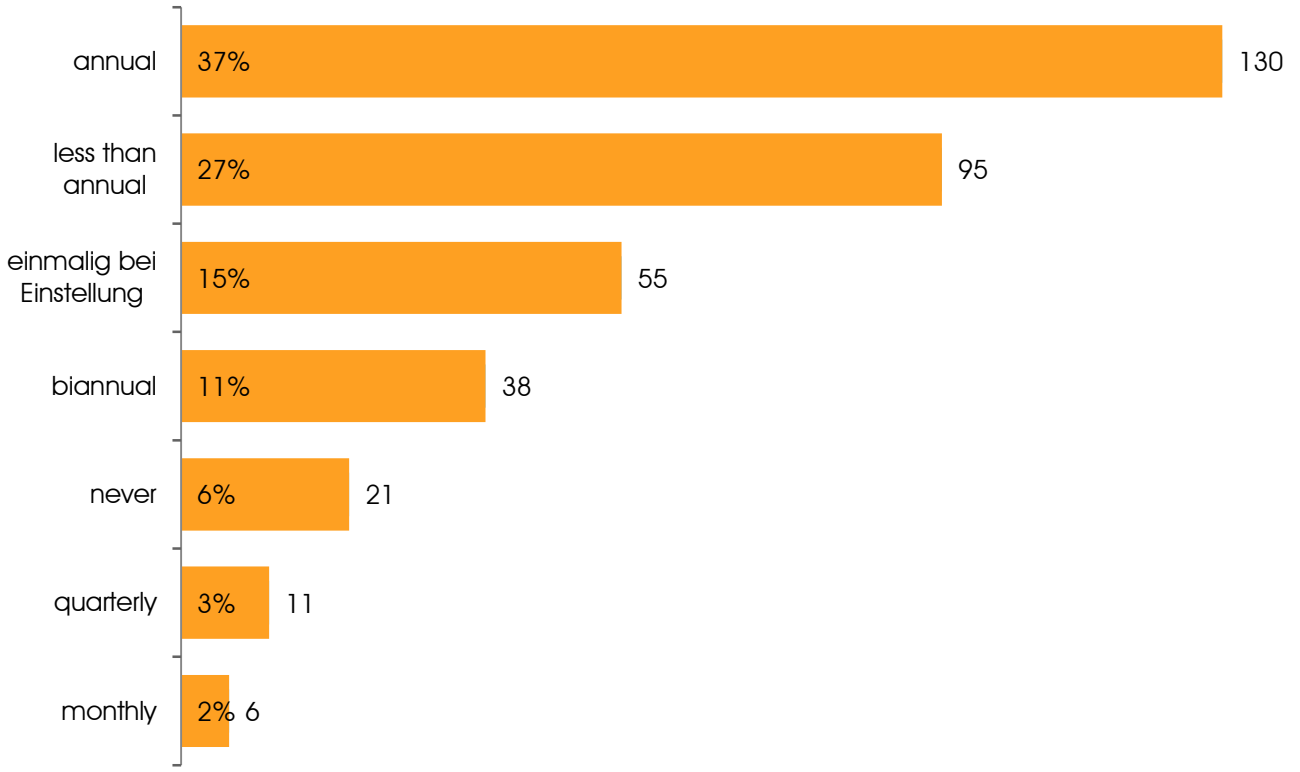
The result of a cross-comparison between data protection training events and data privacy violations demonstrates convincingly the effectiveness of training performed on a regular basis. In the estimation of the data privacy officers, monthly training can reduce the level of infringements caused by ignorance by 36% (c.f. 4.3.6).

Training rhythm by company size:



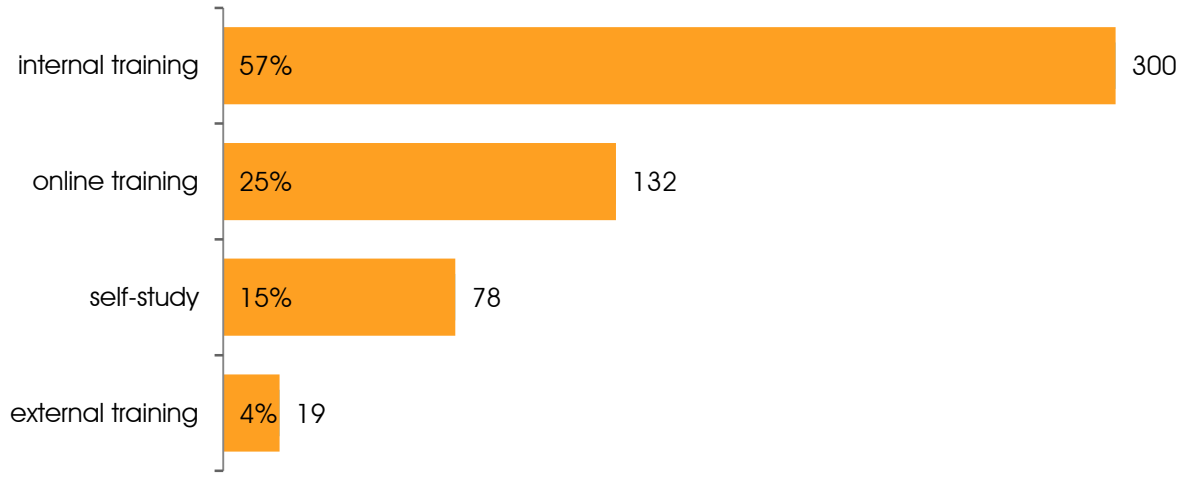
The size of the company makes no significant difference to the rhythm of data protection training. In the companies with less than 50 employees alone annual training is given more frequently than in the other size categories.

12. "How often are your employees given data protection training with reference to their own specialty (personnel, marketing etc.)?"



In addition to general instruction in data protection law, one of the core legal tasks of the data privacy officer is to familiarize the employees "with the various special requirements of data protection", section 4g para 1 point 2 BDSG. There were found to be only slight differences as regards the number of training events between general training (section 4.2.11) and that specific to particular professions.

13. "What methods do you use to train your employees?"



One of the core duties of the data privacy officer is to train the employees. The overwhelming majority of data privacy officers run internal training, while only 19 work with external providers; nevertheless, 132 or 25% of the data privacy officers resort at least on occasion to the medium of online training. In comparison to the company size, 65% of the data privacy officers questioned in companies with over 50,000 employees use online training, while this rate falls together with company size. In companies with less than 50 employees, 25% of the data privacy officers questioned also use online training.

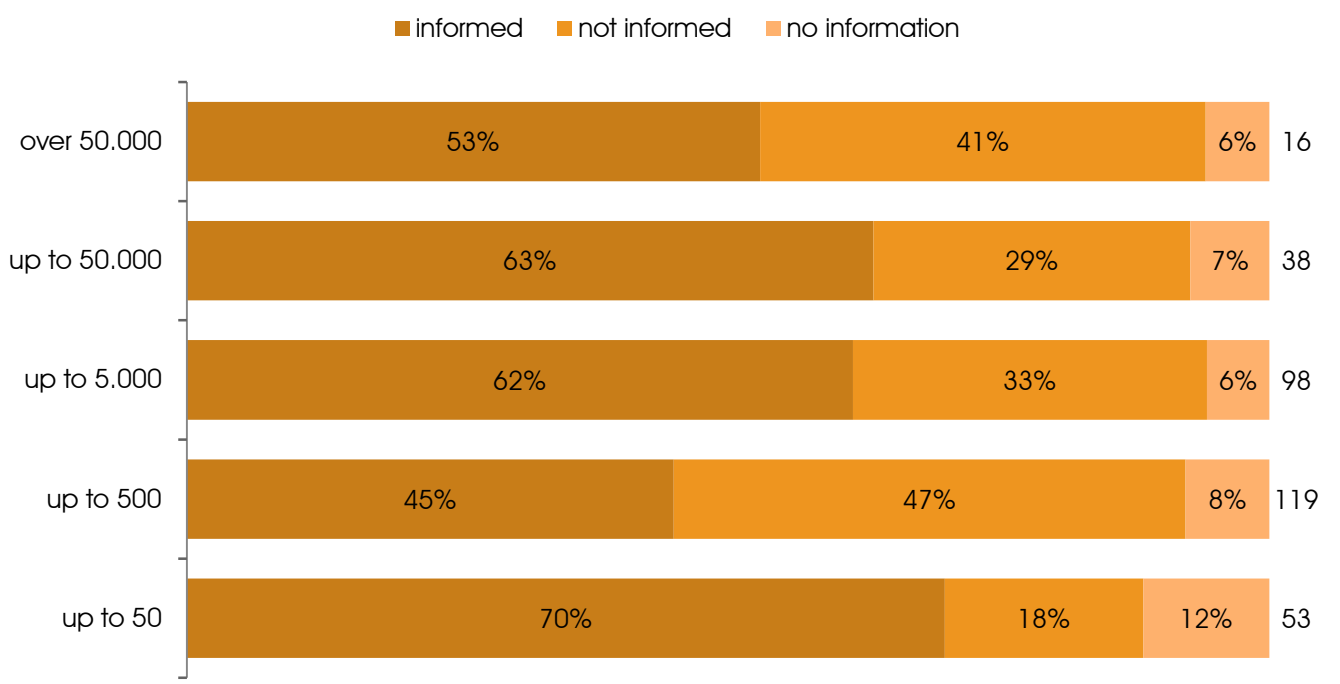
4.3 Data privacy violations in the company

1. "Do you feel well informed about data privacy violations in your company?"

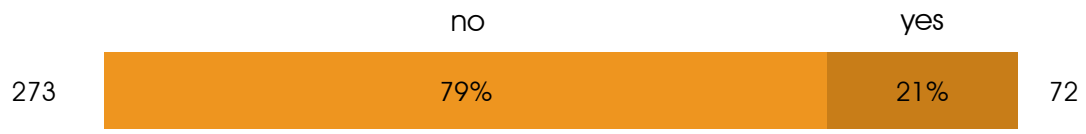
Not only do data privacy violations in a company damage its image and result in information obligations and claims for damages by the affected data subjects. In certain cases they must also be notified to the responsible regulatory authority, section 42a BDSG. At the same time, such violations form an important source of information for the data privacy officer in maintaining his obligations to the implementation of data protection legislation. In any event, violations count among the information that must be communicated to the data privacy officer; the latter must also be involved in the resolution of such violations.

38.1% of the in-company data privacy officers feel insufficiently informed of data privacy violations in their company. Given that the sample group in question consists primarily of highly experienced data protection officers, this high proportion is alarming. Above a company size of 5000 employees, two thirds of the data privacy officers feel sufficiently well informed about data privacy violations; in small companies only 17% feel not sufficiently informed.

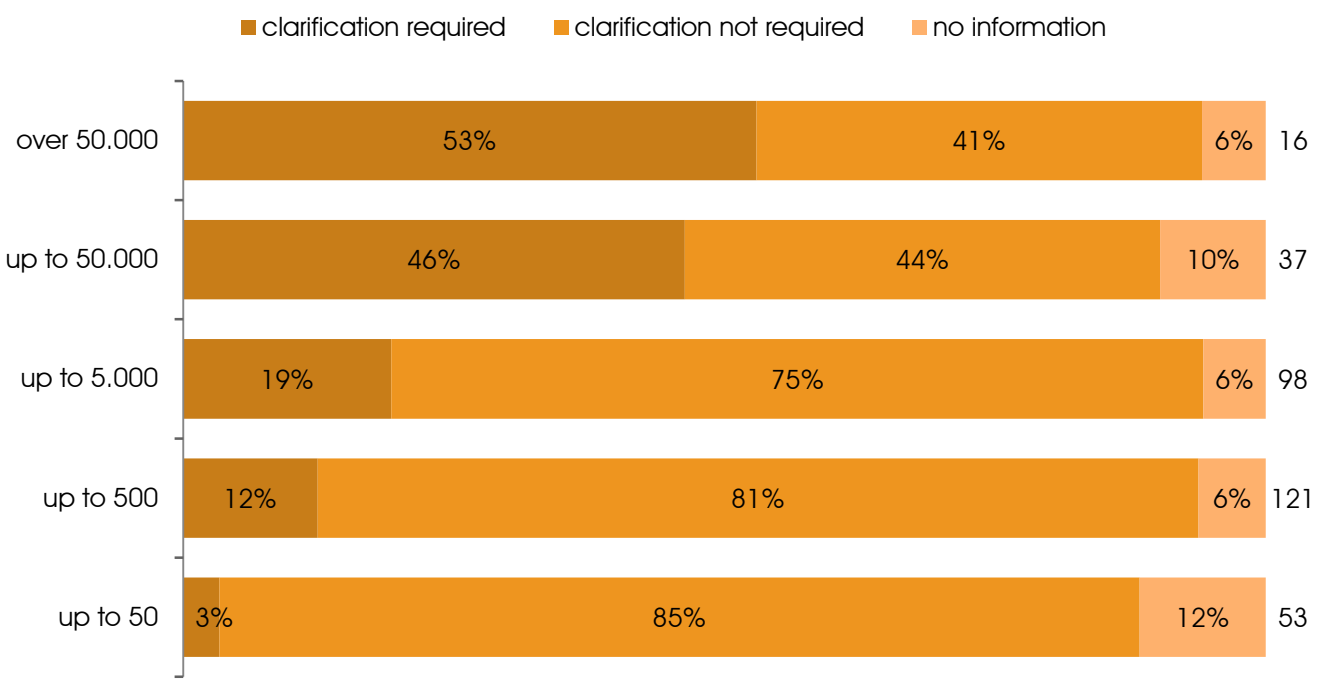
Opinions of data privacy officers by company size:



2. "Have you ever had to clarify whether a notification was necessary under section 42a BDSG"?

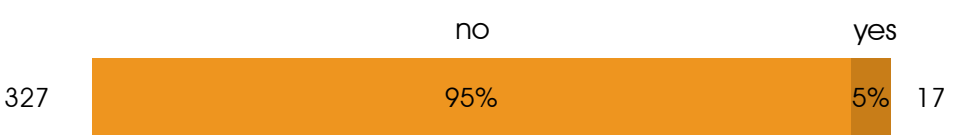


Section 42a BDSG postulates an obligation to notify the competent authority in the event of personal data being unlawfully obtained by a third party if this threatens serious harm to the rights or legitimate interests of the data subjects affected. This relatively new regulation in the BDSG has caused much uncertainty in the practice and the need for clarification. The results of the survey give clear proof to the relevance of such audits where on average 20.9% of the data privacy officers questioned have already had to carry out such an audit.



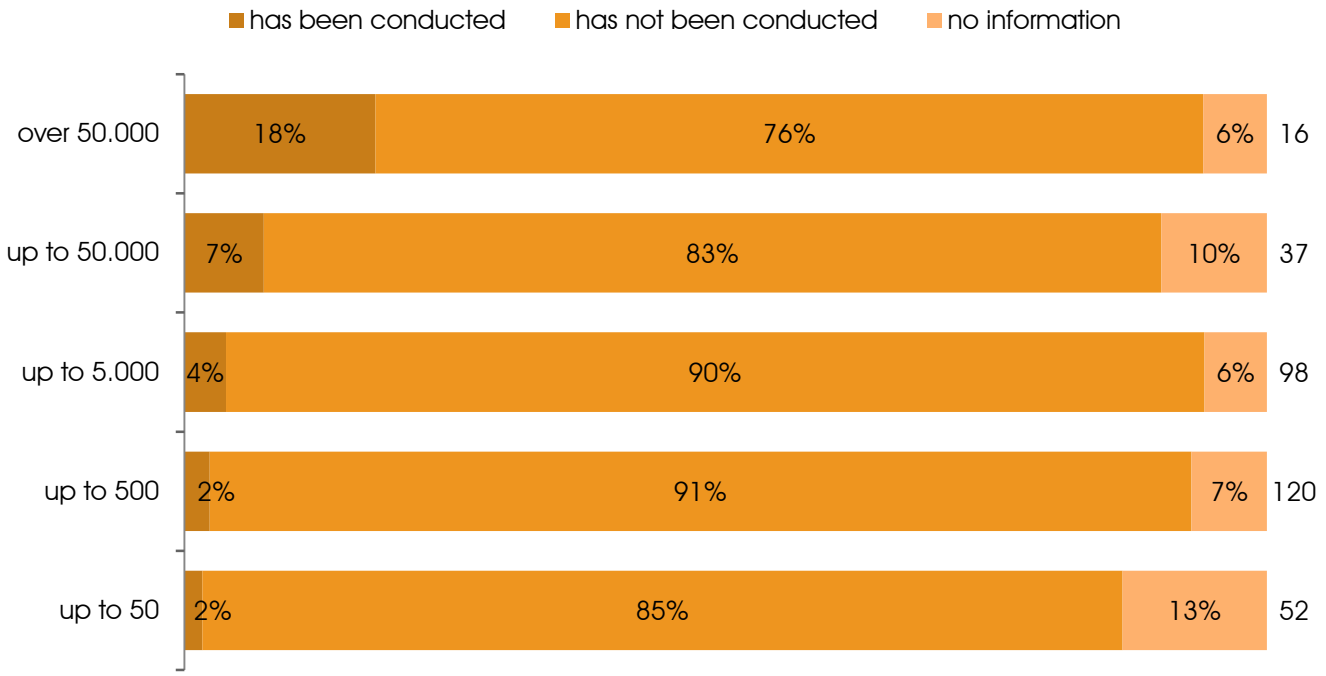
Here the frequency of clarification of alleged data privacy violations differs strongly by company size. The frequency constantly increases with the number of employees. In the companies with over 5000 employees every second data privacy officer has already had occasion to resolve a data privacy violation. In companies with up to 50 employees only 3% of the data privacy officers were confronted with such a question.

3. "Have you had to make a notification under section 42a BDSG?"



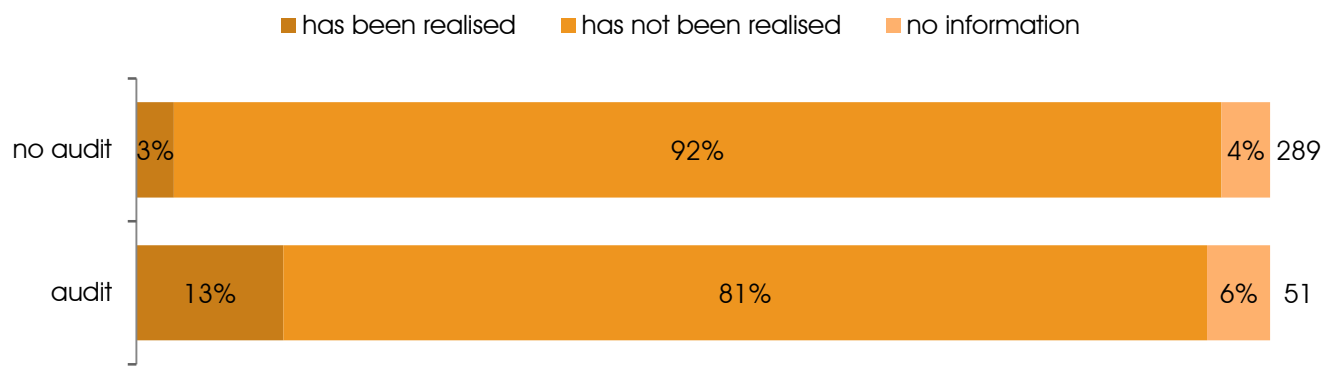
Under section 42a BDSG there is an obligation to notify the competent authority in the event of personal data being unlawfully obtained by a third party if this threatens serious harm to the rights or legitimate interests of the data subjects affected. When such a risk is detected, the affected data subjects must be informed, with a description of the nature of the unlawful disclosure and recommendations of measures to minimize possible harm. Such a notification have been made by the data privacy officers questioned or the data controllers in 17 companies; this is however already 4.9% of the companies in the survey.

Relation by company size:



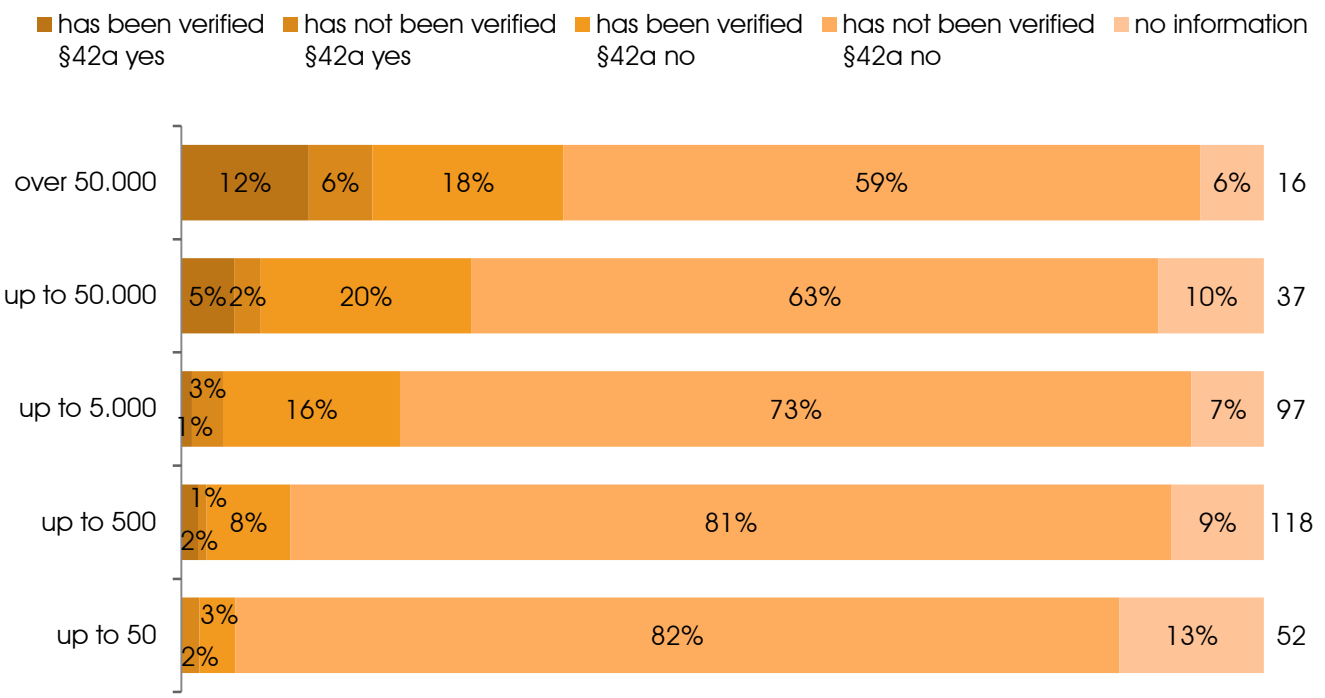
Here again it can be seen – as also with the audits of data privacy violations – an increasing number of notifications with increasing employee numbers. In companies with over 50,000 employees, 18% of respondents have already had to initiate such a notification, while the figure for companies with less than 50 employees was only 2%.

"Are companies that have already had to make a notification under section 42a audited more frequently by the regulatory authorities?"



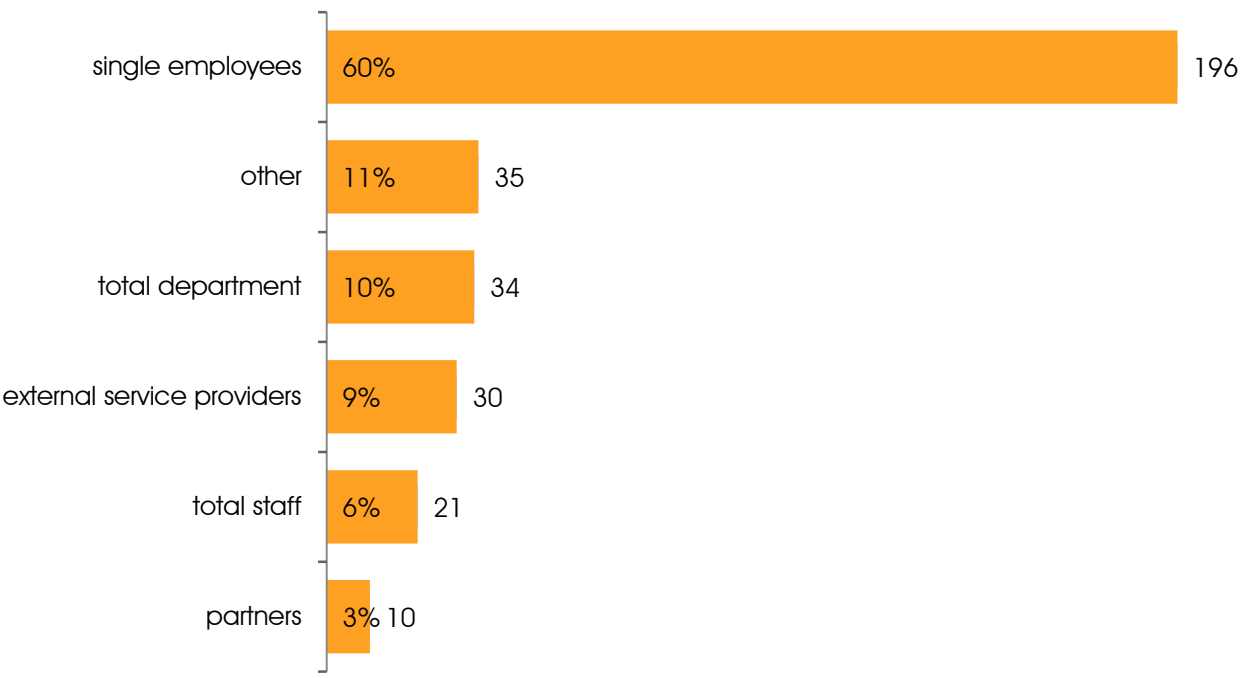
The probability that companies will be audited by the regulatory authority increases in the event of a notification under section 42a by a factor of three, since after such a notification the public awareness and the readiness of the affected parties to request the regulatory authorities to perform an audit and instigate disciplinary action increases.

Response of data privacy officers by company size:



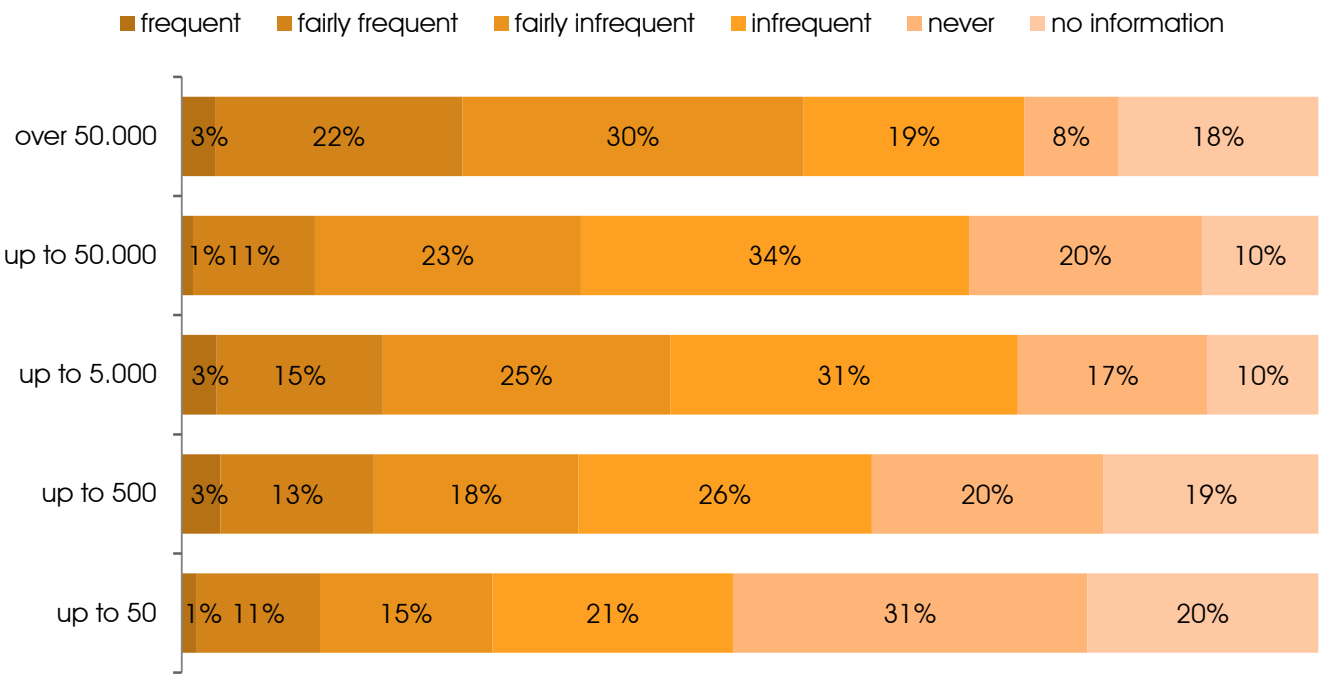
In a comparison between notifications and regulatory authority audits, the emphasis is again seen to be on companies with over 5000 employees, which have a significantly higher risk of being audited.

4. "Which group, in your view, commits the most data privacy violations?"



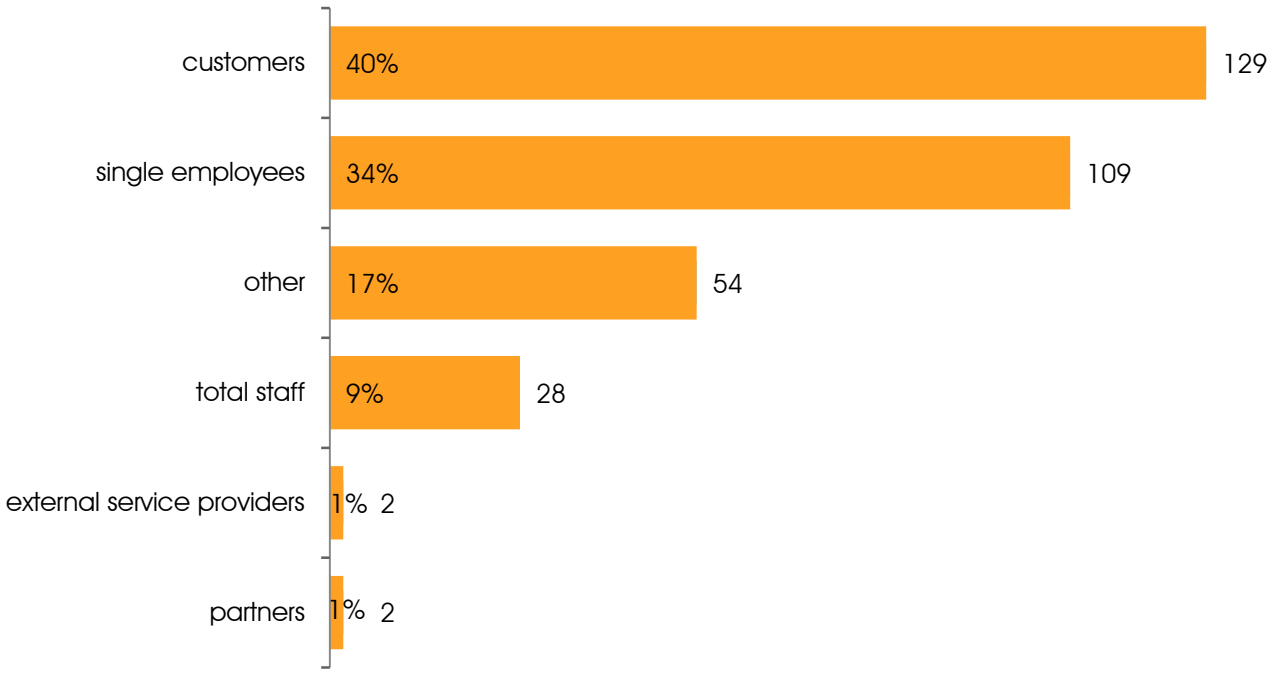
Data protection law regulates the protection of personal data from misuse by unauthorized parties. In the experience of the data privacy officers, the most serious cause of data privacy violations is misconduct on the part of individual employees (60.1% of responses), but 10.4% of responses refer to total departments. Only 3% of the responses implicate business partners, 9% external service providers and 11% other perpetrators. In the view of the practitioners the emphasis is significantly on internal perpetrators.

Frequency of data privacy violations by company size:



The average value of less than 20% "fairly frequent" or "frequent" data privacy violations are exceeded only by the companies with over 50,000 employees by a significant 5%. Here again a substantially higher workload for data privacy officers than in the smaller organizations.

5. "Which group, in your view, is the most frequent victim of data privacy violations in your company?"



Victims of data privacy violations are the affected data subjects whose data has been processed unlawfully. In a company this could be either customers or the company's own employees. Unsurprisingly, the most frequent victim of data privacy violations is the customer as data subject, with 39.8% of responses, but this is closely followed by employees with 33.6%. These figures suggest an equal weighting of self monitoring under data protection law in favor of external victims (customers) and internal victims (employees).

6. "Assess the frequency of the various causes of data privacy breaches in your company"

Cause	frequent	fairly frequent	fairly rare	rare	never
Negligence	14.94%	35.06%	21.34%	20.73%	7.93%
	50%		50%		
Ignorance	11.28%	31.40%	27.44%	23.48%	6.40%
	42.68%		57.32%		
Technology	2.47%	10.67%	26.83%	43.29%	16.46%
	13.41%		86.59%		
Corporate guidelines	2.82%	8.78%	14.42%	31.35%	42.63%
	11.60%		88.40%		

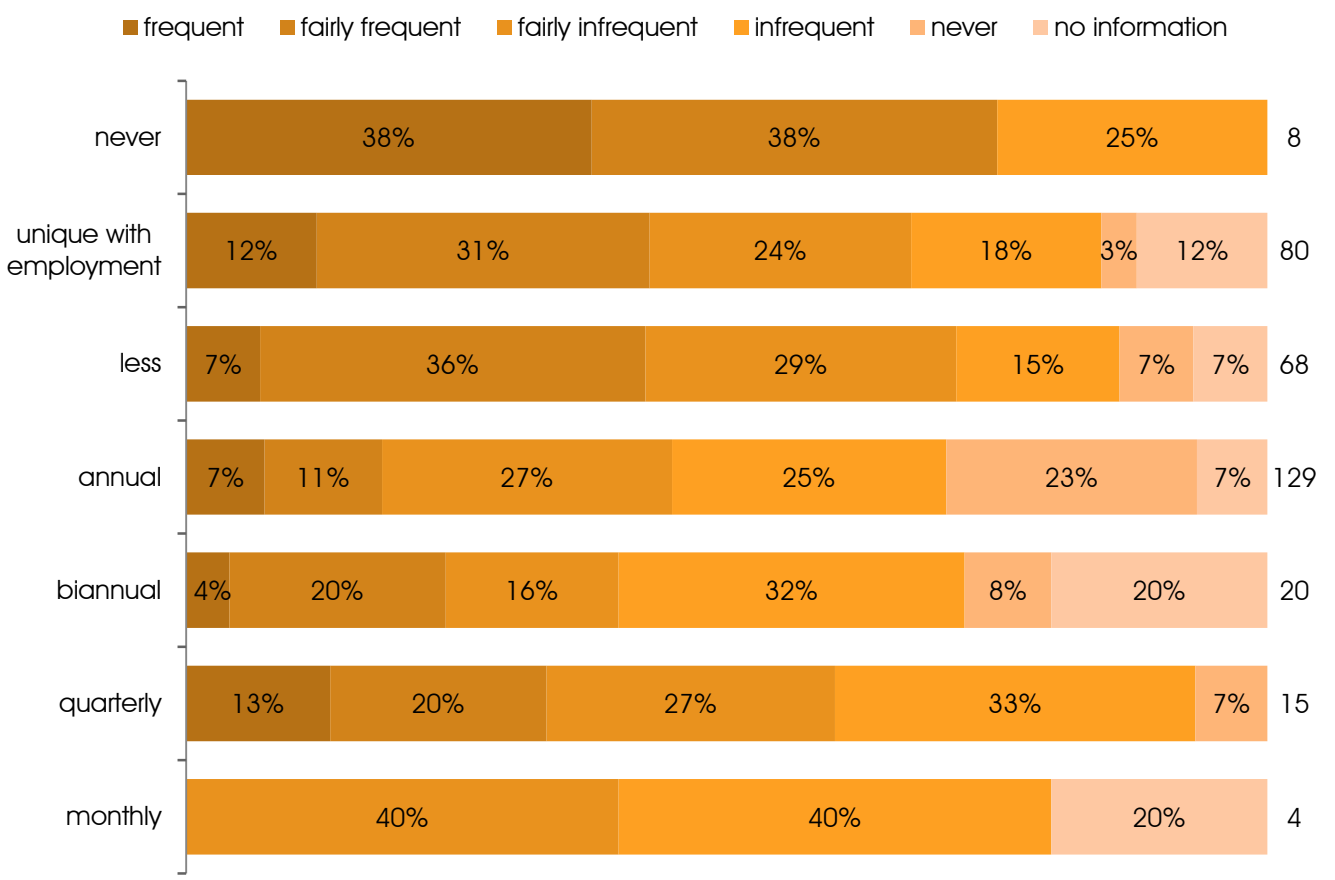
The survey presented the following as potential causes of data privacy violations: negligence, ignorance, technology and corporate guidelines. The data privacy officers questioned are however divided over the importance of negligence as a cause: while 50% experience this "frequently" or "fairly frequently", the other 50% rated this cause as between "rare" and "never". "Ignorance" comes out only 7% more clearly as a cause: here roughly 43% of the data privacy officers considered it a frequent occurrence, while 57% evaluated it between fairly rare and never. The picture becomes clearer only with "Technology" and "Corporate guidelines" as potential causes. These were experienced by 86.59% and 88.40% of all respondents, respectively, as either "rarely" or "never" a cause for data privacy violations.

If the response to "Corporate guidelines" is examined solely among those data privacy officers who work in subsidiary companies, the following picture emerges:

	frequent	fairly frequent	fairly rare	rare	never
Corporate guidelines	4.07%	13.07%	19.51%	37.40%	26.02%
	17.07%		82.93%		

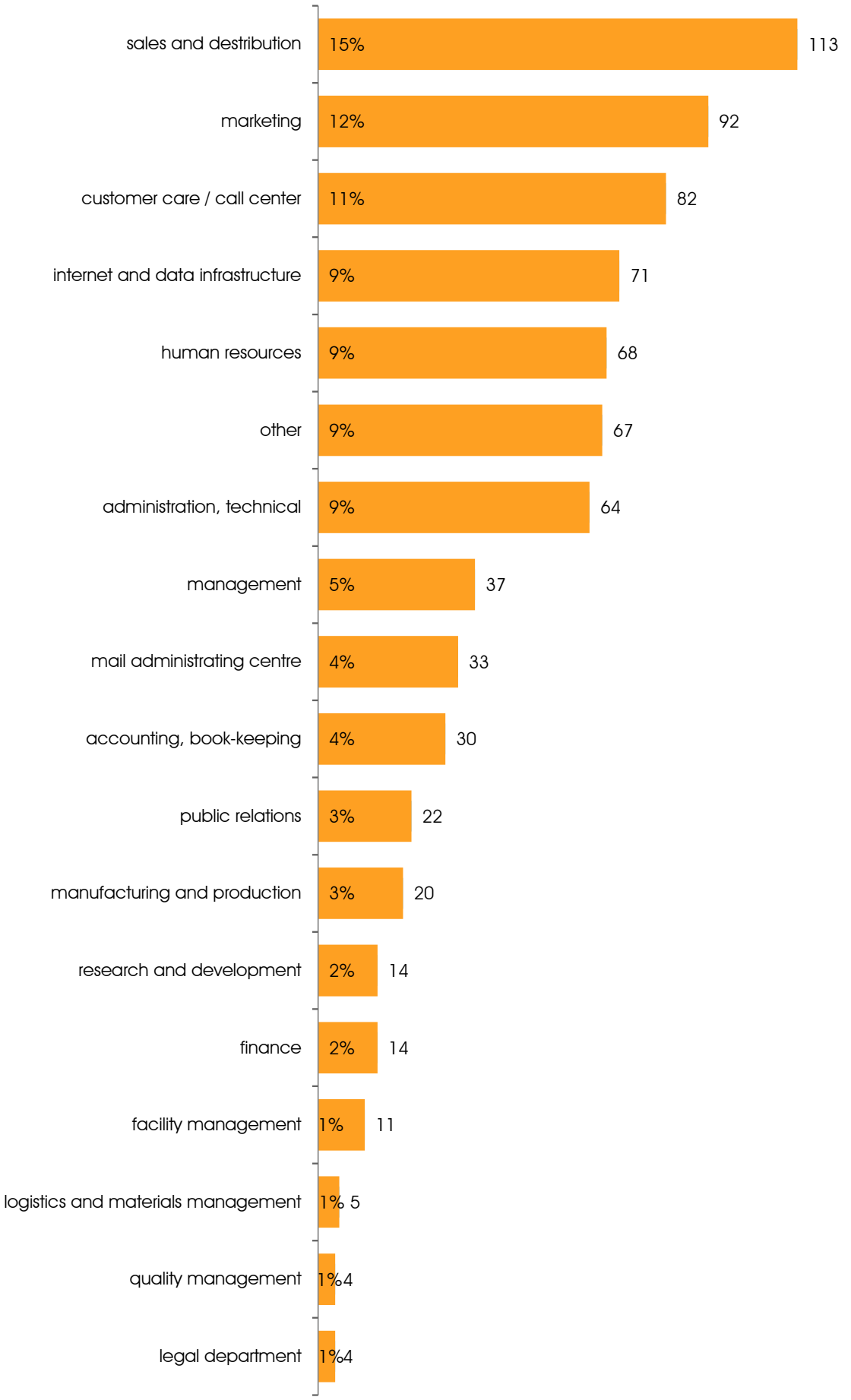
If only the data privacy officers of subsidiary companies are questioned, the number of negative responses towards corporate guidelines increases only marginally. Corporate guidelines as a cause of data privacy violations remain here as "rare" to "never" for 83% of respondents.

"Does regular training help to reduce the violations caused by ignorance?"



The result of a cross-comparison between data protection training events and data privacy violations demonstrates convincingly the effectiveness of training performed on a regular basis. The violations caused by ignorance fall, in the assessment of the data privacy officers, if regular training is given.

7. "In which departments do you detect the most data privacy violations?"

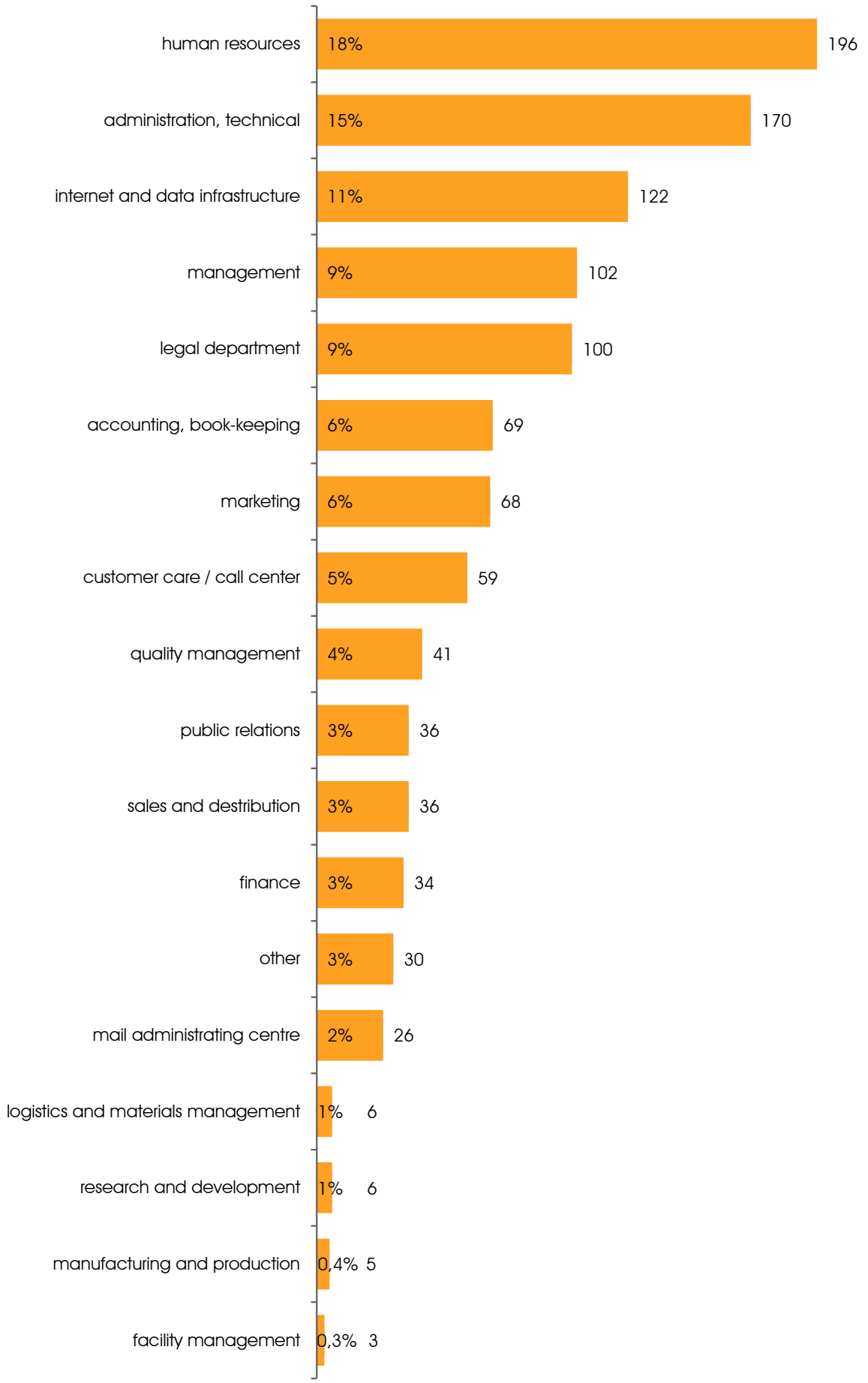


A ranking of data privacy violations by department in % of all responses appears as follows:

Ranking by violations	Department	Responses in per cent
1.	Sales and distribution	15.05
2.	Marketing	12.25
3.	Customer support, call center (if applicable)	10.92
4.	Internet and data infrastructure	9.45
5.	Human resources	9.05
6.	Other	8.92
7.	Administration, technical	8.52
8.	Management	4.93
9.	Mail administering center	4.39
10.	Accounting, book-keeping	3.99
11.	Public relations	2.93
12.	Manufacturing, production	2.66
13.	Finance	1.86
14.	Research and development	1.86
15.	Facility management	1.46
16.	Logistics and materials management	0.67
17.	Quality management	0.53
18.	Legal department	0.53

Sales, distribution, marketing and customer support are not only the departments that handle the most personal data but are also thus highest on the list for data privacy violations. Here the evident accuracy of the efforts of the legislators can be seen, as it is exactly these areas that are being re-regulated in the greatest detail - not least in the wake of the 2009 data protection scandals.

8. "In which departments, in your view, is data protection dealt with seriously?"



Sorted by the ranking of data privacy violations, the results in percent of responses for adjustment efforts appears as follows:

Ranking by violations	Department	Ranking by engagement with data protection
1.	Sales and distribution	10.*
2.	Marketing	7.
3.	Customer support, call center (if applicable)	8.
4.	Internet and data infrastructure	3.
5.	Human resources	1.
6.	Other	12.
7.	Administration, technical	2.
8.	Management	4.
9.	Mail administering center	13.
10.	Accounting, book-keeping	6.
11.	Public relations	10.*
12.	Manufacturing, production	16.
13.	Finance	11.
14.	Research and development	15.
15.	Facility management	17.
16.	Logistics and materials management	14.
17.	Quality management	9.
18.	Legal department	5.

* identical number of responses

A highly differentiated level of awareness of the problem in the different departments can be seen from the results of the survey: while the personnel departments are most concerned with data protection issues, they are still fifth on the list for violations. The worst offenders for data privacy violations are the sales, distribution and marketing departments. These same departments also come last when it comes to engagement with data protection issues. Here the expected relationship between ignorance of the legal regulations and data privacy violations can be clearly seen.

9. "How often do you observe the data privacy violations listed below in your company?"

Data privacy violations in a company are as diverse as their possible causes. The law differentiates in administrative offenses between more formal violations, which can be fined by up to €50,000 and substantive violations that involve an infringement of the rights to informational self-determination of the data subjects and may be fined by up to €300,000. Where the violations are committed with a deliberate intent for financial gain or to cause harm, the offenses are such that they may be punished with up to two years imprisonment.
The survey questioned the data privacy officers about typical data privacy infringements in their practical experiences. These related both to typical misconduct by employees (carelessness, unauthorized use, improper storage, documents left lying about) and also to insufficient implementation of the legally prescribed organizational measures (unlawful collection, processing, transfer and processing of personal data) and technical issues (unencrypted or unsecured IT and electronic data processing equipment).

In order of frequency of responses, careless use of IT infrastructure, documents left in printers and unencrypted, unsecured IT and EDP equipment were the commonest data privacy violations in the companies questioned; the processing of personal data in violation of contract, on the other hand, was the least frequent violation.

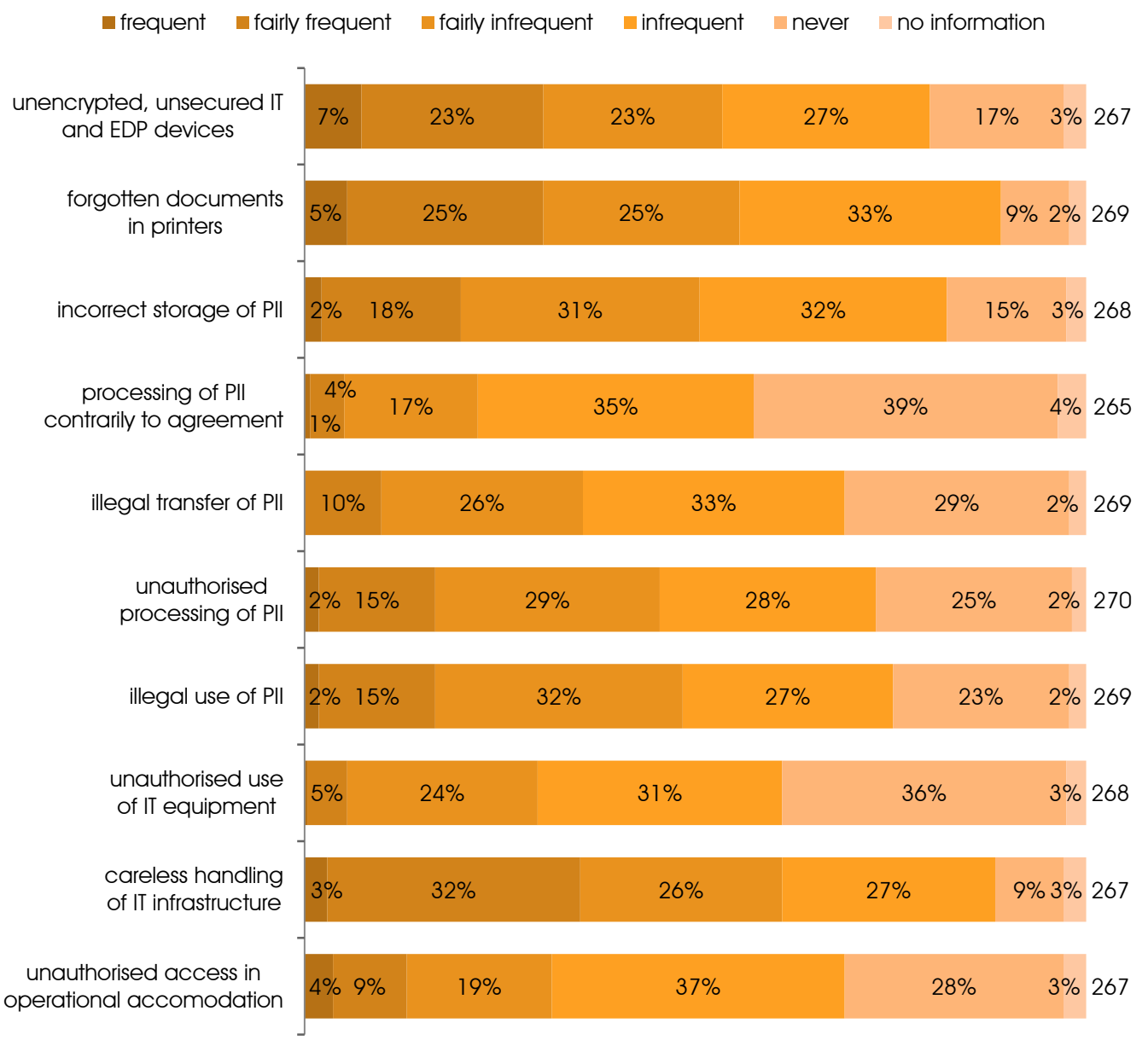
Ranking of established causes of data privacy violations:

Place	Causes of data privacy violations	Percentages of "frequent" and "fairly frequent" responses
1.	Careless handling of IT infrastructure	36.28
2.	Documents left in printers	31.97
3.	Unencrypted, unsecured IT and EDP equipment	30.38
4.	Improper storage of personal data	21.2
5.	Unauthorized processing of personal data	17.19
6.	Unlawful collection of personal data	16.98
7.	Unauthorized entry into operational work areas	12.3
8.	Unlawful transfer of personal data	11.29
9.	Unauthorized use of EDP equipment	6.6
10.	Data processing in violation of contract	4.76

"Does the keeping of a register of procedures result in a reduction in data privacy violations (particularly in relation to technical and organizational measures)?"

The register of all procedures used in automated data processing in the company (overview as per section 4g para 2 BDSG) forms one of the most important tools for effective data protection management and is also legally prescribed. This register must be made available to any person on request and to the regulatory authority on demand. When creating a register of procedures it should be checked and determined within the company which data may be processed legally in which manner and which technical and organizational protective measures should be taken under section 9 BDSG.

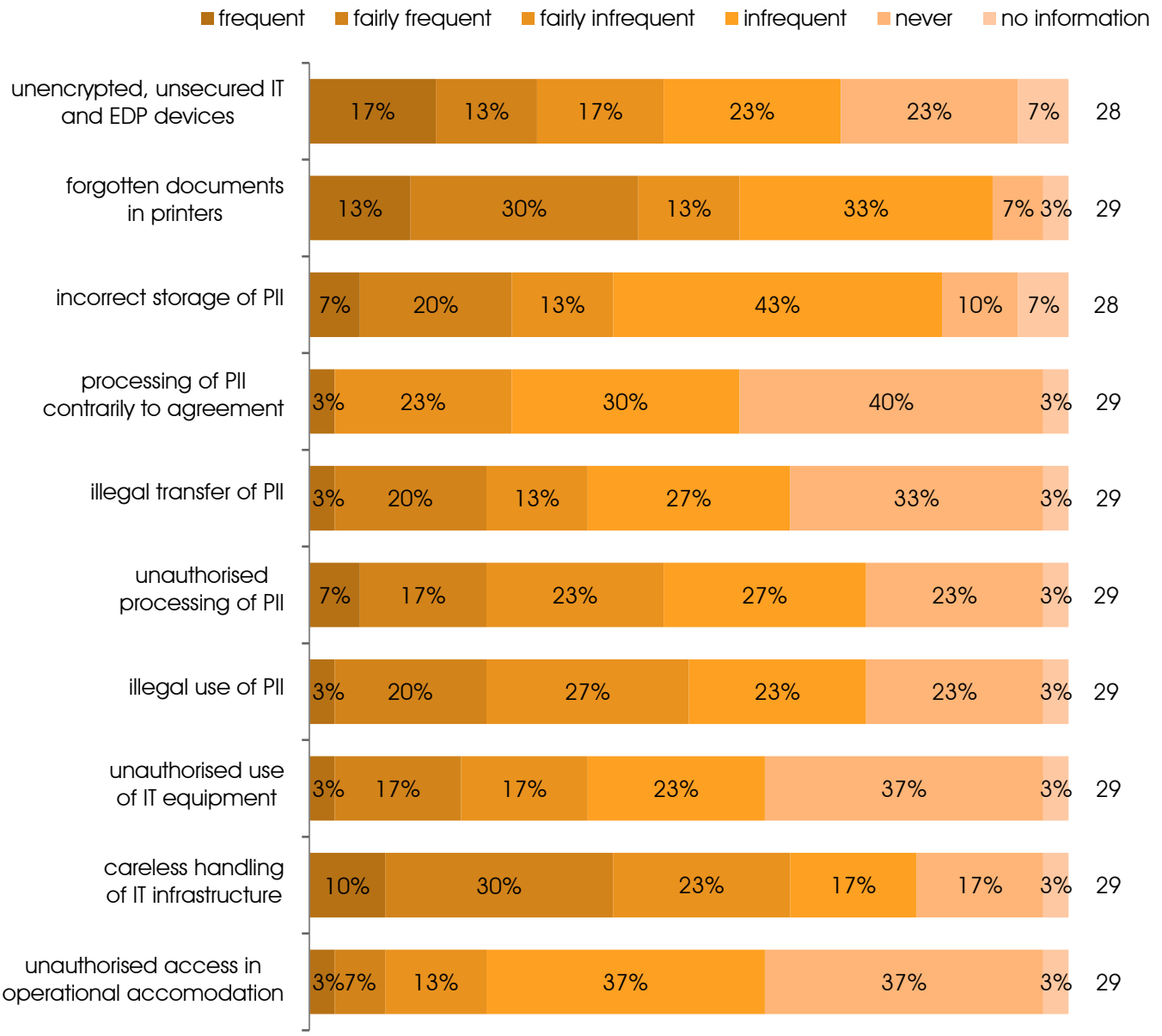
Companies with a register of procedures:



*PII: personally identifiable information

Overall the frequency of data privacy violations is reduced by an average of 8% of "frequent" and "fairly frequent" responses when the company has a register of procedures in use. In companies that have reviewed their organizational management on the basis of data protection law when setting up a register of procedures, unlawful transfers (-13%), unauthorized processing (-16%) and unauthorized use of EDP equipment (- 14%) have fallen significantly as causes of data privacy violations. It is thus above all the technical and organizational measures that are made more effective in companies that use a register of procedures than in those that do not.

Companies without a register of procedures:

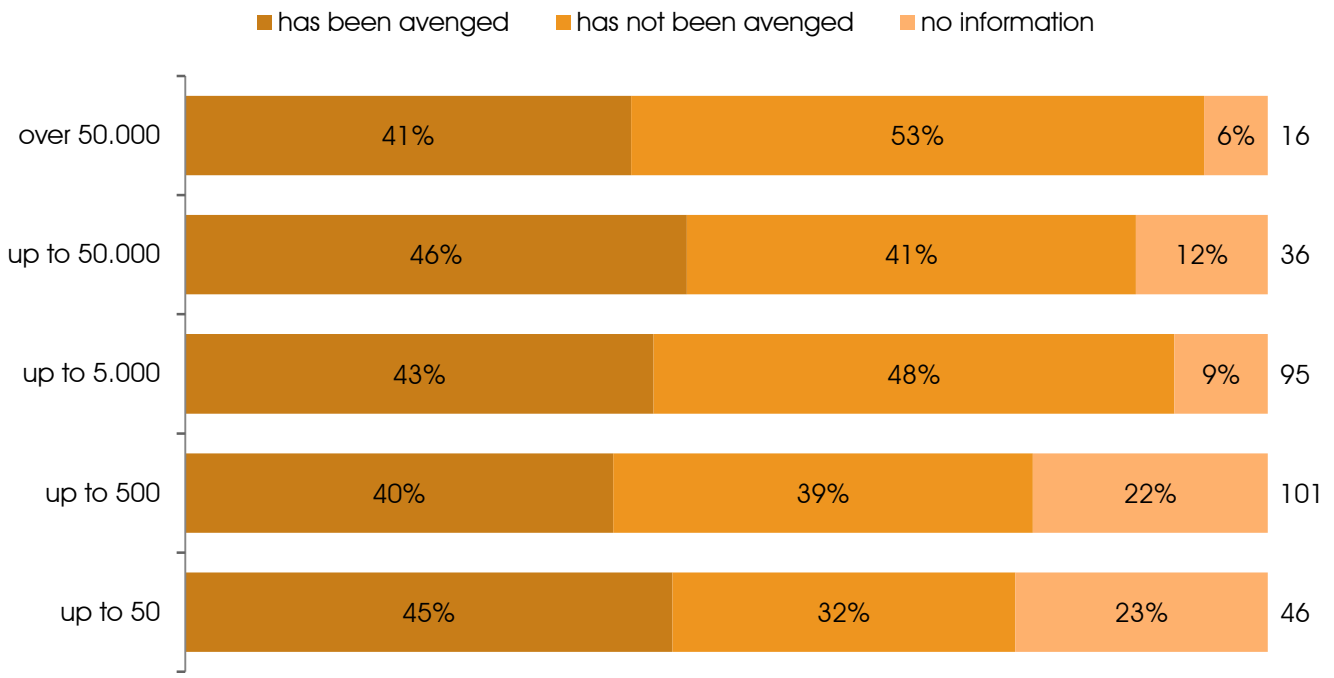


*PII: personally identifiable information

10. "Are all registered data privacy violations appropriately punished?"

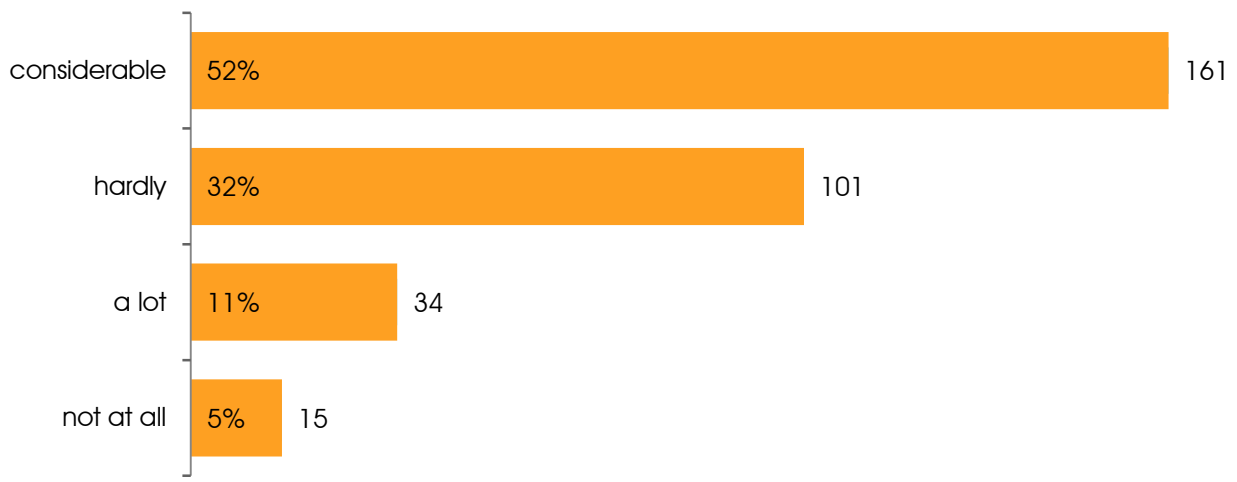
In the experience of the data privacy officers questioned, suitable disciplinary action is only instigated for about 51% of the data privacy violations detected.

"Are data privacy violations disciplined differently depending on company size?"



An examination by company size shows no significant variation in the disciplinary action practice.

11. "How satisfied are you with the consequences?"



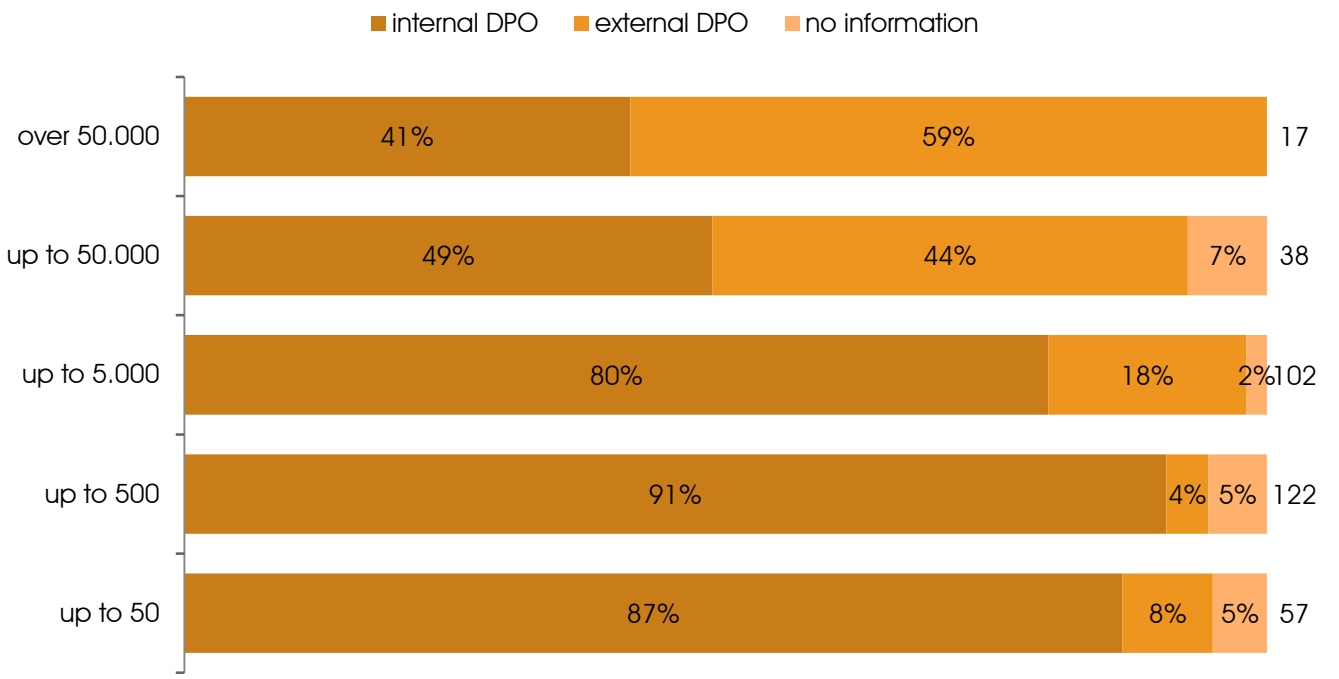
In-company data privacy officers have no competence of their own to take disciplinary action against data privacy violations, nor do they have any obligation to report violations to the competent regulatory authority. Here they are more reliant on the company management and its willingness to draw lessons from violations and misconduct. In those cases in which established data privacy violations are punished, the data privacy officers questioned responded by 63% with "fairly" or "very" satisfied.

4.4 The data privacy officer in the company

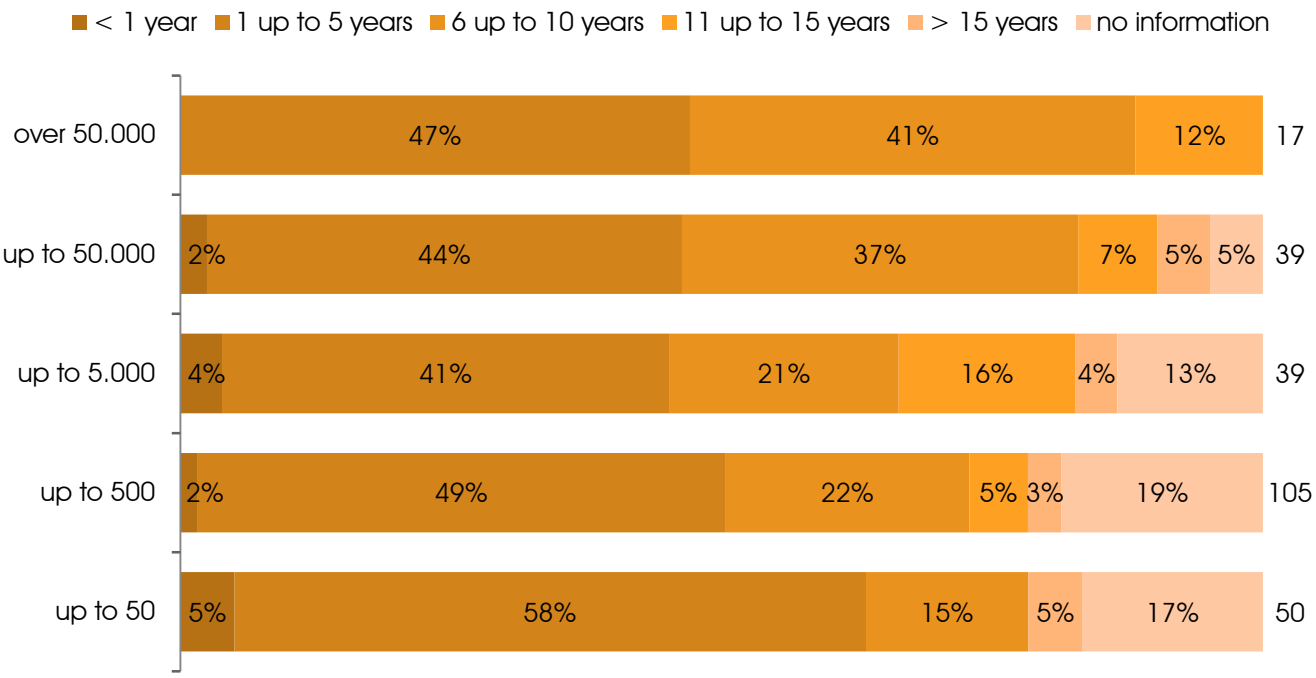
1. "How many clients do you support as an external data privacy officer?"

Of the 63 external data privacy officers who participated in the survey, 9 support only one client, 38 support between 2 and 10, 7 support between 10 and 20 and 3 external data privacy officers support between 20 and 25 companies (seven officers gave no response to this question).

"How are external data privacy officers distributed in terms of company size?"



2. "How long have you been appointed in your company as a data privacy officer?"

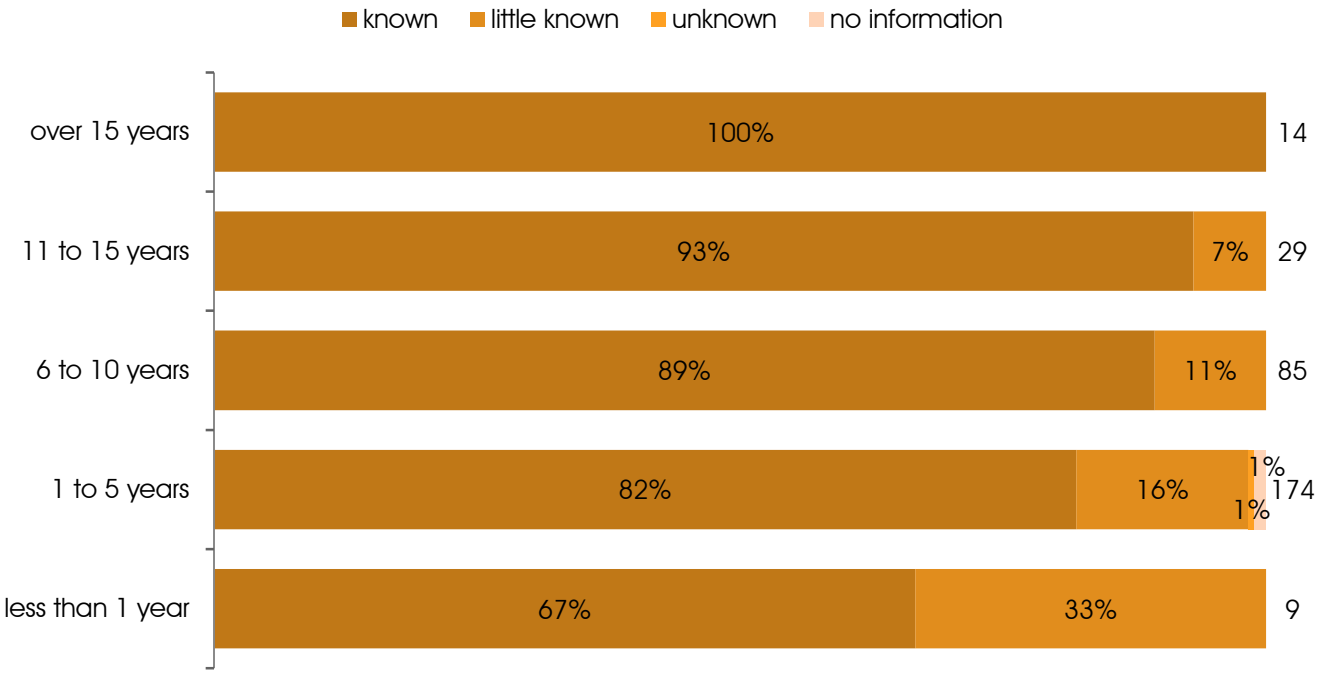


In total the 317 data privacy officers who responded to this question have worked for 1794 years in the same company, i.e. an average time in position of 5.7 years. Taken alone, the internal data privacy officers have been in post for an average of 5.9 years. This is evidence of a low level of fluctuation and thus a developed culture of data protection in the participating companies. Among the external data privacy officers in isolation the figure is a little lower at 4.3 years.

3. "Are you known to the employees in your company as the data privacy officer?"

Because of the data privacy officer's function on the one hand as a technical advisor and on the other as an appeals authority for employees in the event of data privacy violations, his or her being known as such in the company is in most cases a matter of course. The negative response related to one data privacy officer who has worked for less than one year in the company and thus, appropriately, can describe only a temporary situation.

"Does the level of awareness of the data privacy officer increase with length of post in the company?"



In their self-evaluation as data privacy officers the level of awareness in the company of this position increases with the length of appointment.

4. "Can you pursue your work as a data privacy officer without restrictions?"

72.5% of the data privacy officers estimate that they are able to pursue their activity without restrictions. The possible causes of restrictions, drawn from the evaluation of the results to questions 4.4.4/4.4.6/4.4.10/4.4.14, give the following picture: 11% of all data privacy officers have both answered negatively to this question and been critical of the support given to them by management, the availability of personnel support and their involvement in projects.

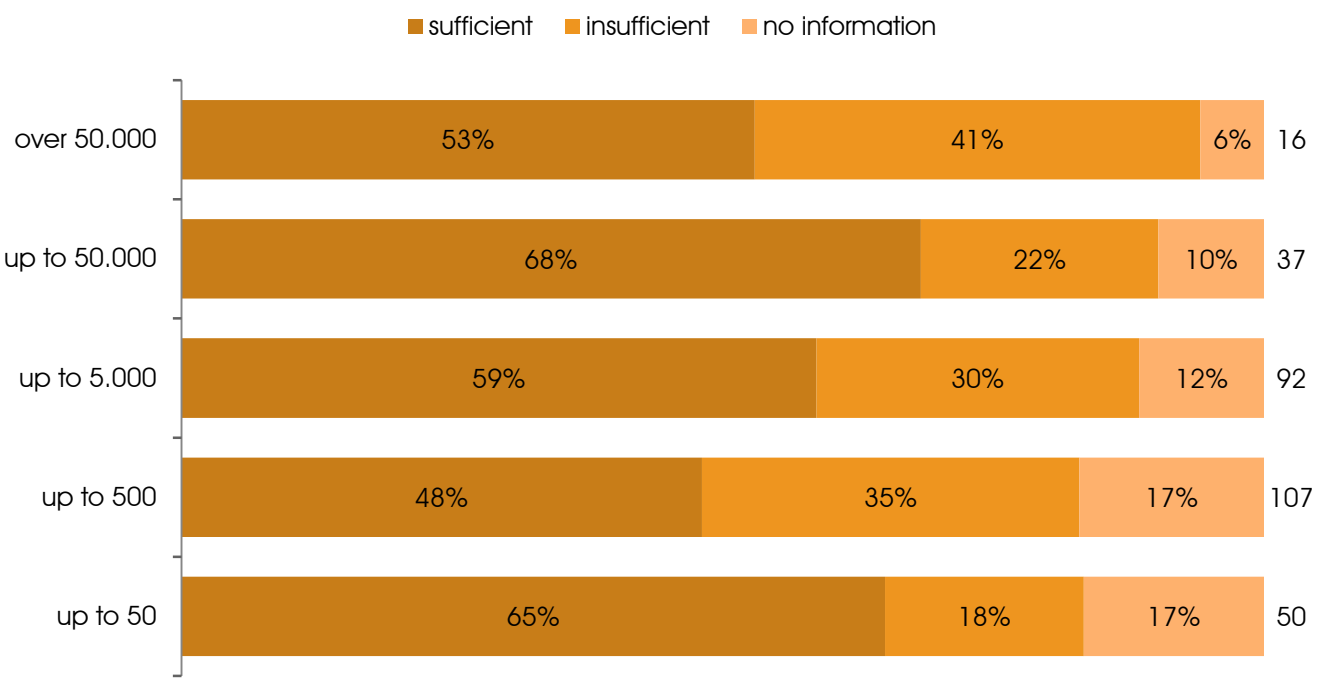
5. "Do you consider that the management meets its obligations?"

Even with ordering a data privacy officer the management has the obligation to enforce the data protection requirements. In the opinion of 315 data privacy officers, who answered this question, this duty is also met by 73% of the management.

6. "Do you consider the support given by management to be sufficient?"

Nevertheless 33% of the data privacy officers questioned complained of a lack of support for their work by management.

Opinions of the data privacy officers by company size:

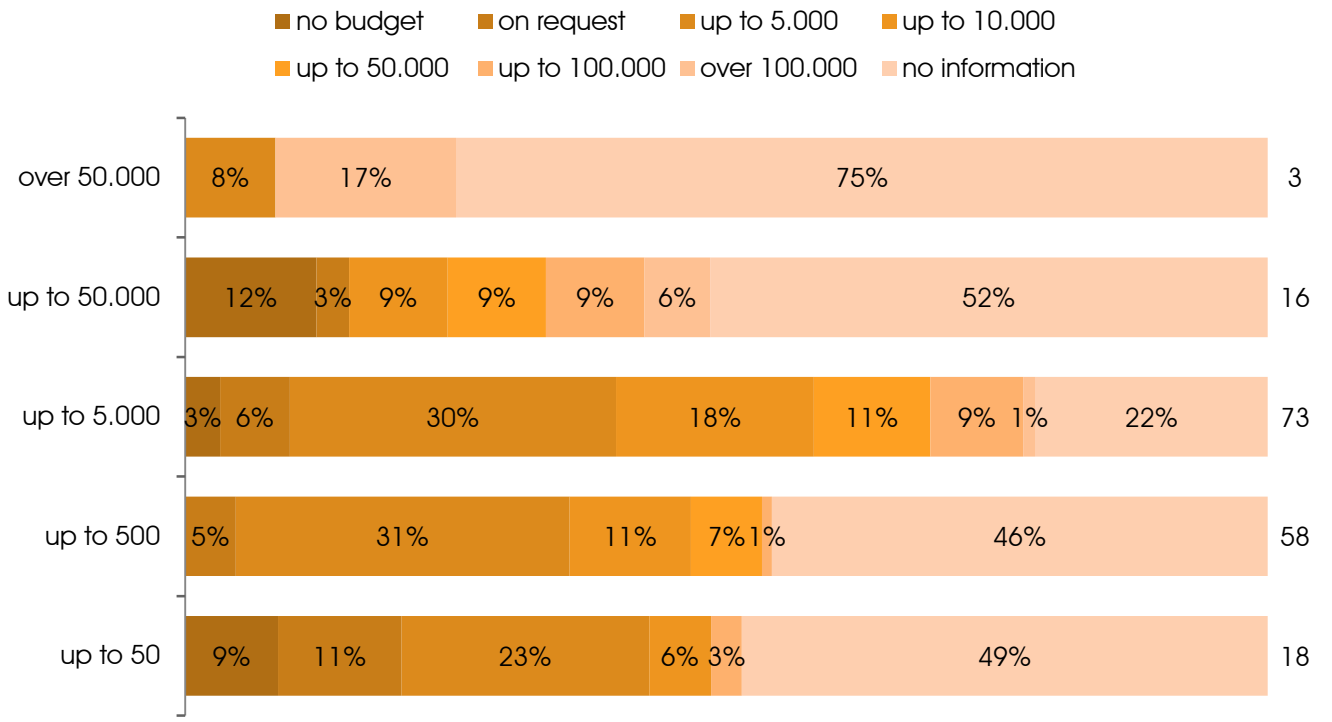


The study showed no significant differences in the support given to the data privacy officers in relation to company size. A slight majority of all management provide sufficient support.

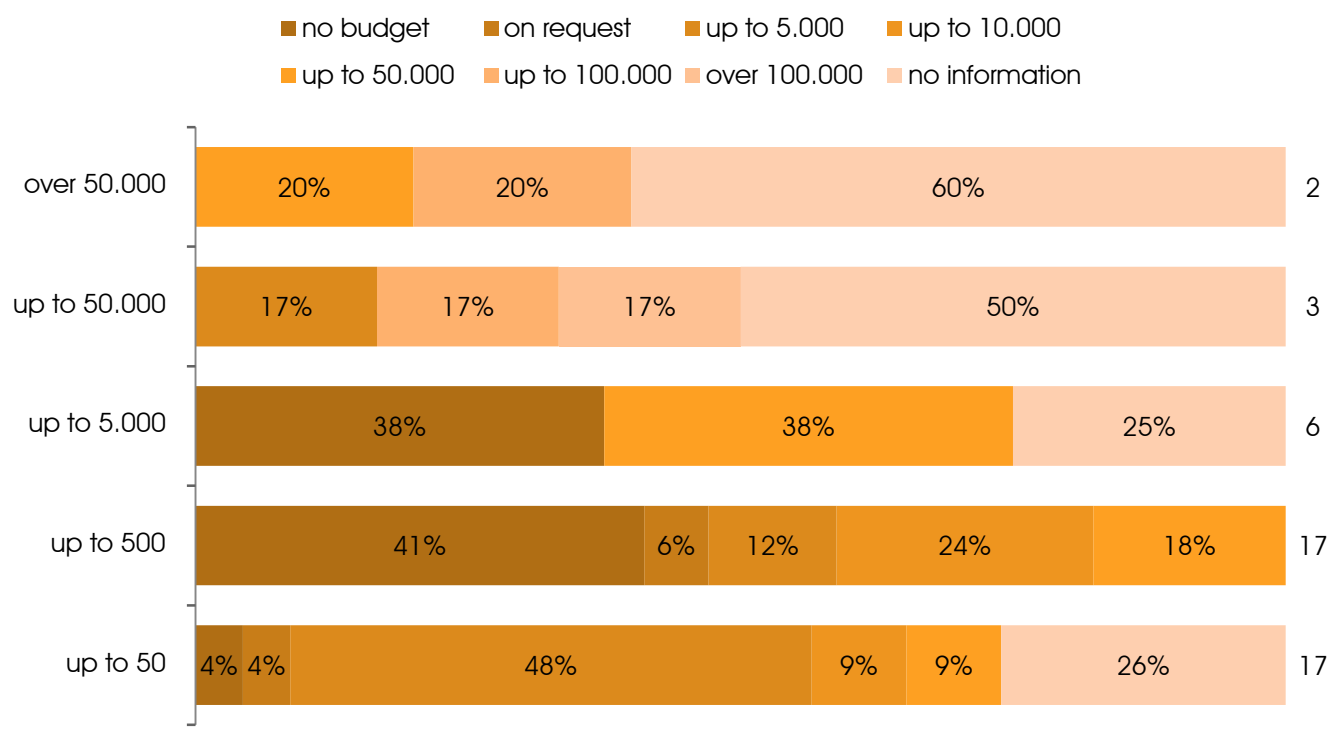
7. "How big is the budget available to you annually for your work as a data privacy officer?"

The average annual budget of the respondents is €70,596. 37 of the data privacy officers questioned stated that no budget was available to them; the question was answered in total by only 215 officers. Of these, companies with up to 50 employees provide an average budget of €1163 annually; companies with up to 500 provide on average €2773, those with up to 5000 employees €13,005, those with up to 50,000 employees €46,073 and companies with above 50,000 employees provide an average annual budget of €666,706. The large differences do not only result from the company size but also from different practices in in-house resource planning.

"How large is the budget by company size for an internal ..."



"... and for an external data privacy officer?"



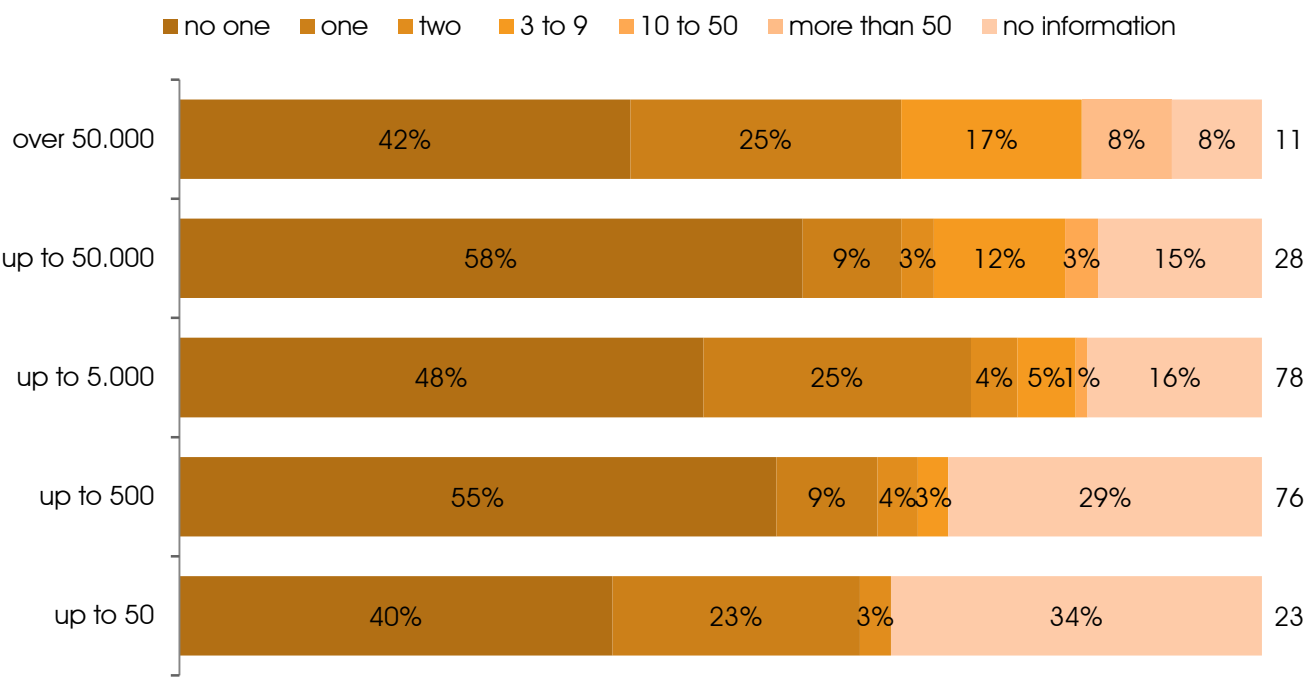
8. "Do you consider the amount of this budget to be sufficient?"

Of the 282 data privacy officers who answered this question, 62.5% considered their budget to be sufficient. Of the 41 data privacy officers who have no budget of their own, five nevertheless answered "yes".

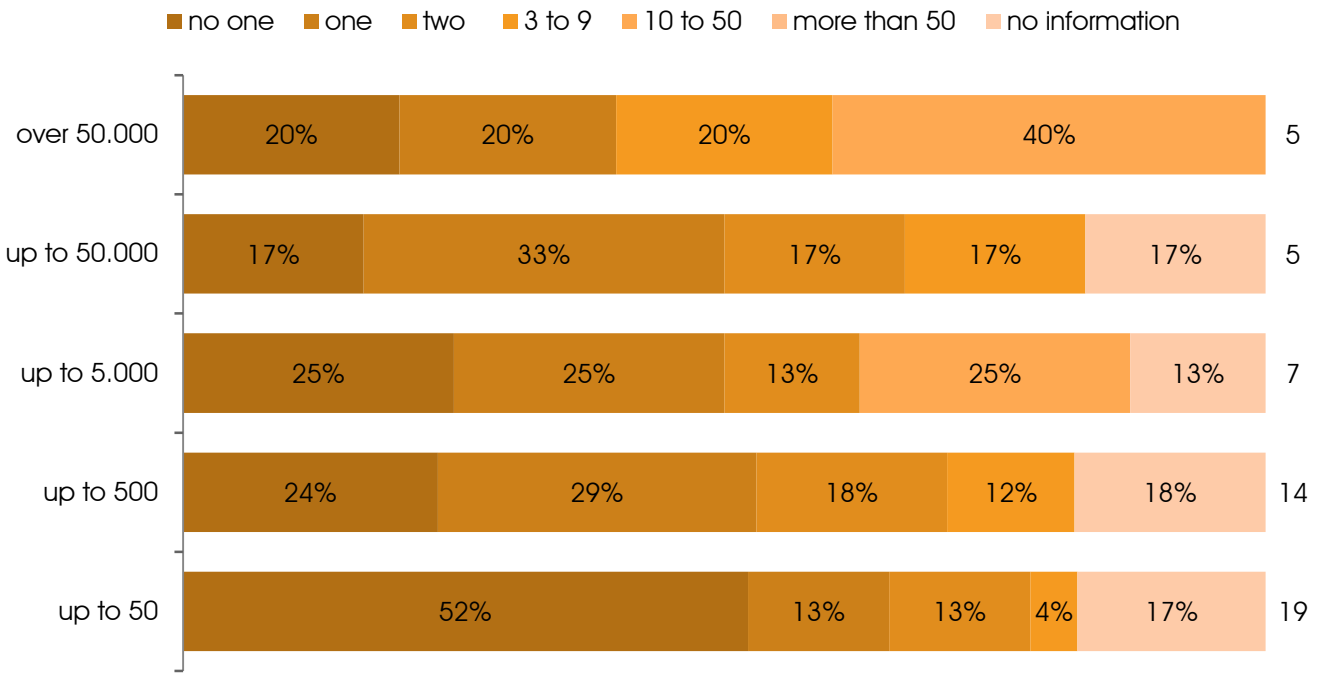
9. "How many employees are available to you directly in performing their duties?"

289 data privacy officers questioned stated that on average 1.3 employees were available to them directly in performing their duties. Here the picture of the data privacy officer as acting single-handed in the company is confirmed once more.

"How many employees directly support the internal data privacy officer by company size?"



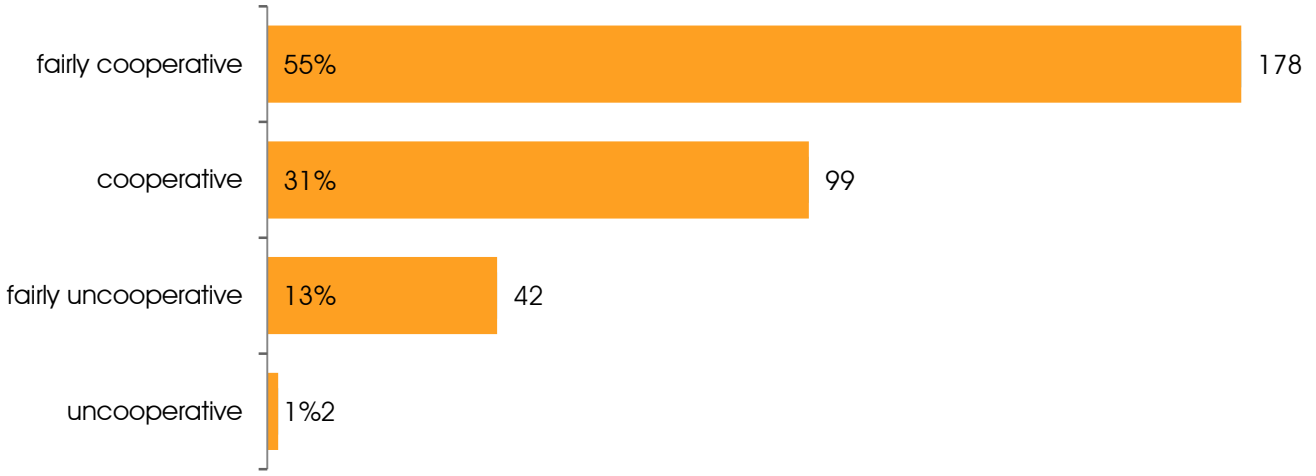
"...and how many directly support the external data privacy officer?"



10. "Do you consider the personnel support available to be sufficient?"

58% of the data privacy officers consider the support of available personnel sufficient for the fulfillment of their duties. However, 42% of the data privacy officers are not satisfied.
Looking at these results more closely, it can be seen that internally appointed data privacy officers are more dissatisfied with the personnel support available to them (43.7%) than are externally appointed data privacy officers, of whom only 33.3% share this view.

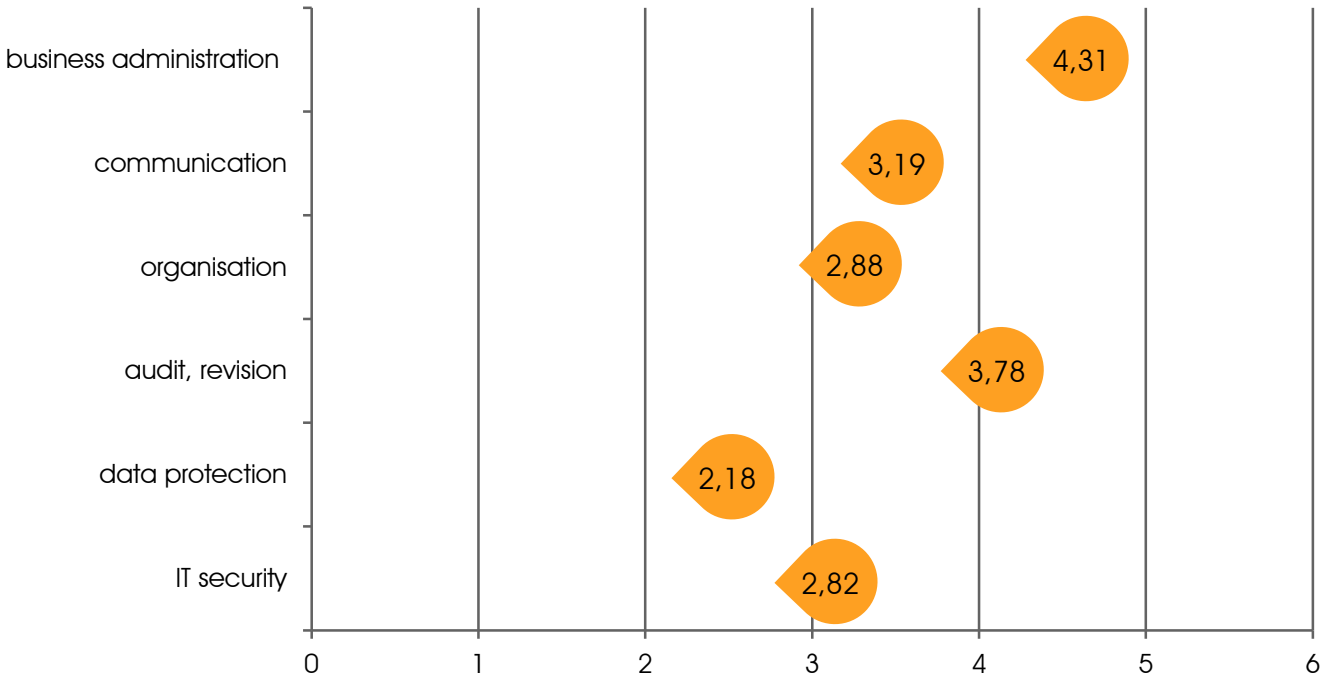
11. "How cooperative do you consider the company departments in working with data protection?"



The vast majority of data privacy officers experience the technical departments in the company as cooperative. This response also reflects the particular situation in the companies questioned, which have often had a data privacy officer in post for many years.

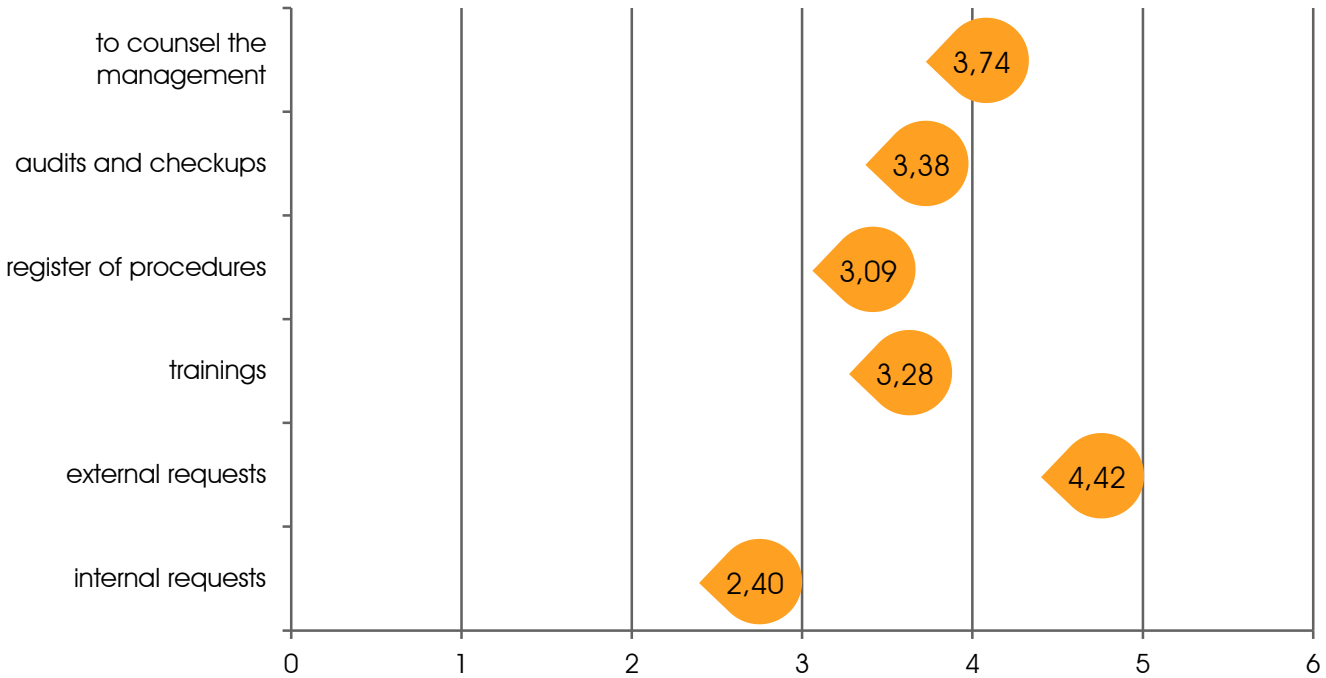
12. "Please list the main elements of your work by your areas of expertise."

(1: most - 6: least)



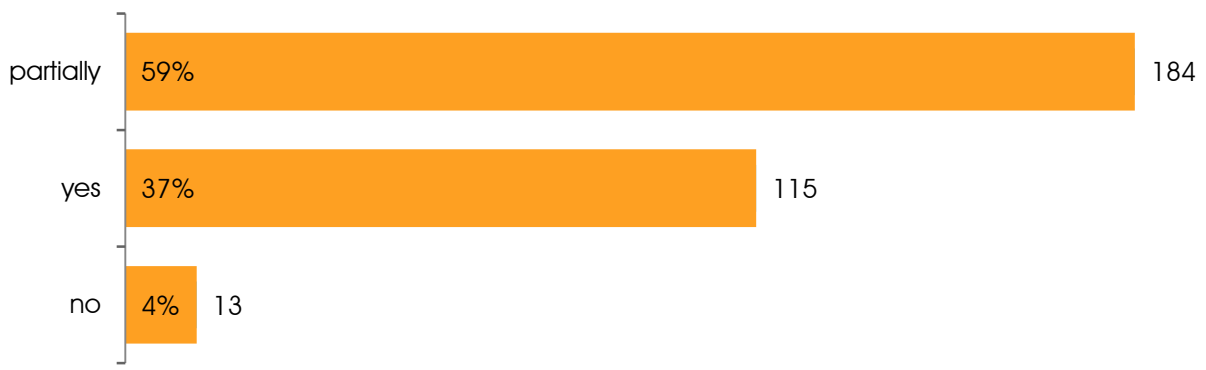
In the ranking of the expertise required for the function of data privacy officer, data privacy law is naturally in first place (average score of 2.18 on a scale of 1 to 6), but this is followed closely by issues of IT security (2.82), knowledge of the organization of operations (2.88) and communication (3.19). Knowledge of auditing (3.78) and business management (4.31) were given least weighting by the respondents.

13. "Please place the following tasks in order of how much time they take you." (1: most - 6: least)



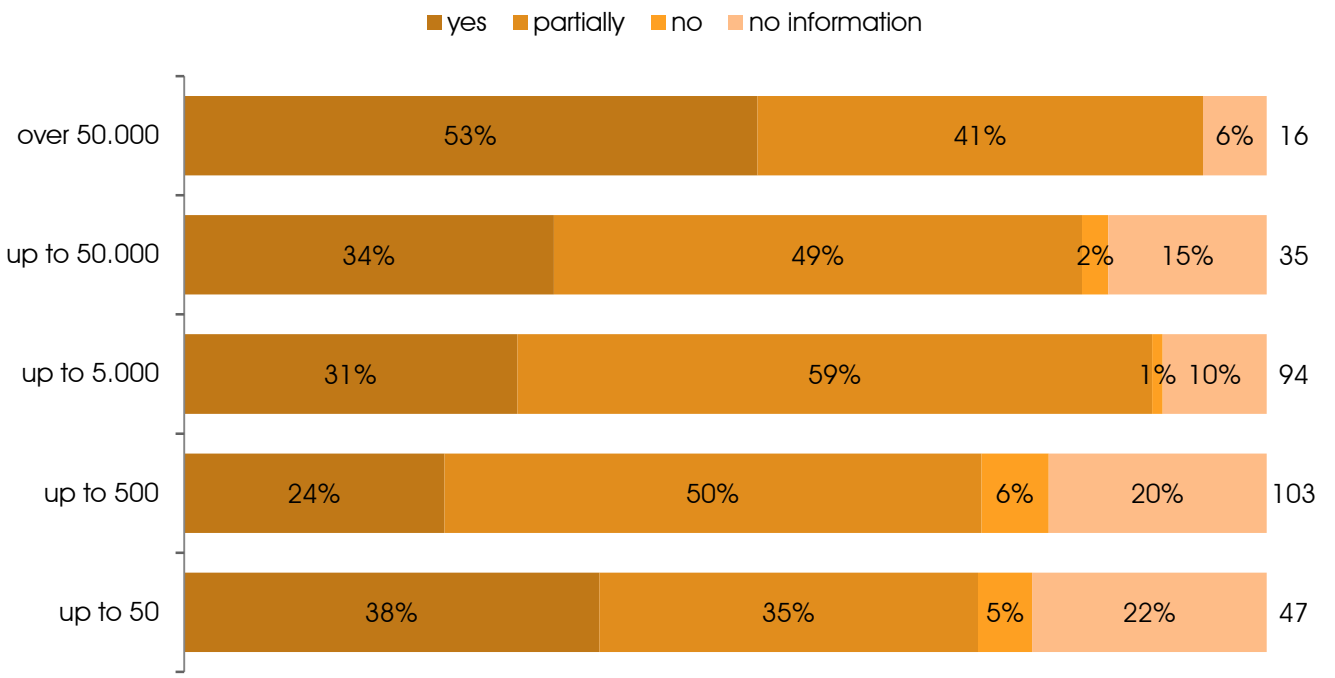
The ranking of time demands on the data privacy officer includes the categories of internal inquiries before the design of the register of procedures, training, audits and monitoring and consultancy to the management. The least time is taken up by external inquiries. This result lets it be assumed that the possibility of affected data subjects outside the company lodging complaints with the in-company data privacy officer is little known and certainly little used.

14. "Are you involved in projects so that you can evaluate them in terms of data protection law?"

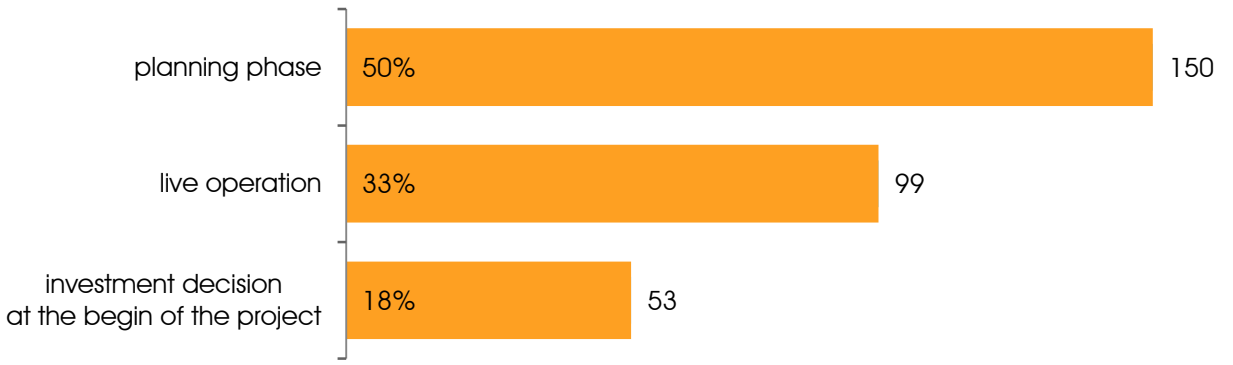


The effectiveness of legal consulting on data protection as a preventive measure seems to be penetrating only slowly in the companies. 96% of the data privacy officers questioned are always, or at least sometimes, involved in projects in order to appraise them in terms of data privacy law. In this matter the size of the company makes only a slight difference. In the companies with over 50,000 employees, 94% of respondents answered "yes" or "sometimes", while 6% gave no answer. Nevertheless, 53% of respondents in this group answered "yes" to this question, while only 24% of data privacy officers in companies with less than 500 employees gave this response.

"How are data privacy officers involved in projects for legal consultancy by company size?"



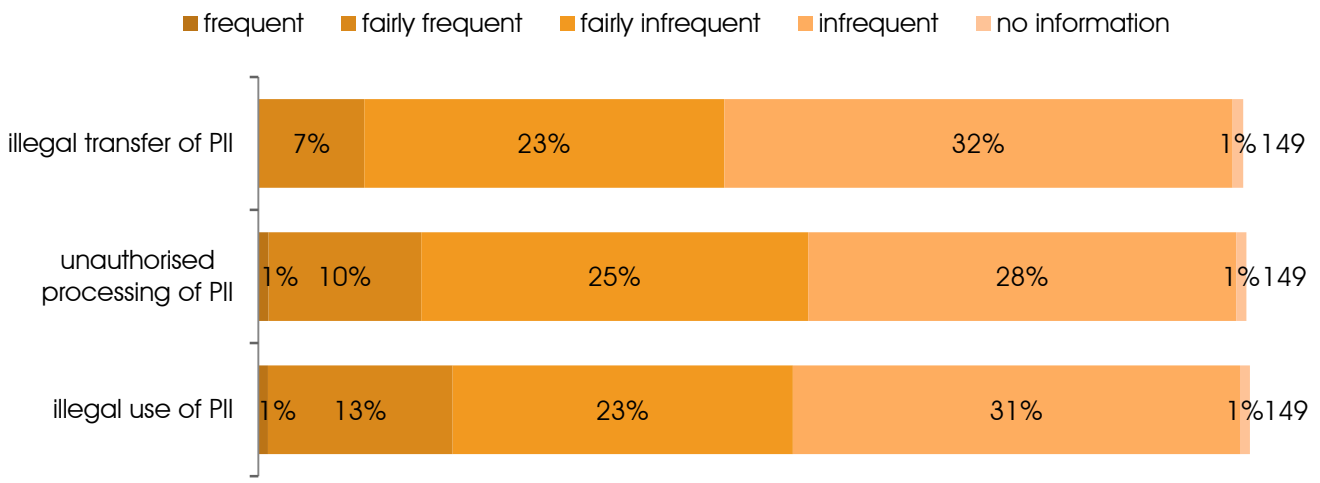
15. "In what phase are you usually included in projects?"



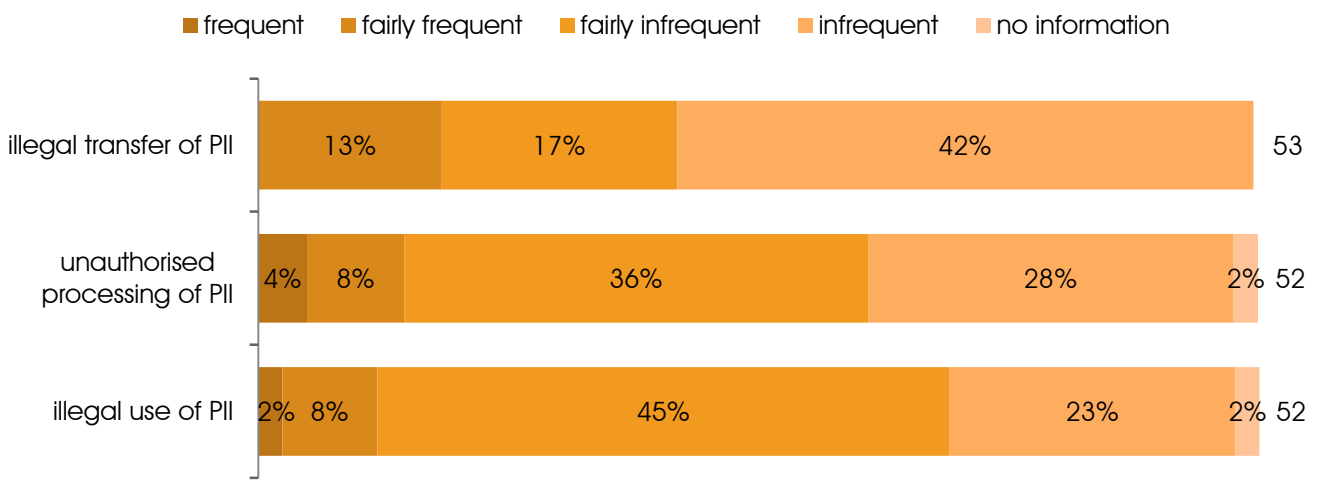
Only involvement at an early stage can prevent wrong decisions and bad investments. It is therefore important to include the data privacy officer at an early stage. 50% of data privacy officers stated that they are engaged for data protection legal appraisal in projects from the planning phase; 18% are involved in the investment decision at the start of the project and only 33% only when the project under way.

"What influence on the frequency of data privacy violations does the involvement of a data privacy officer have...

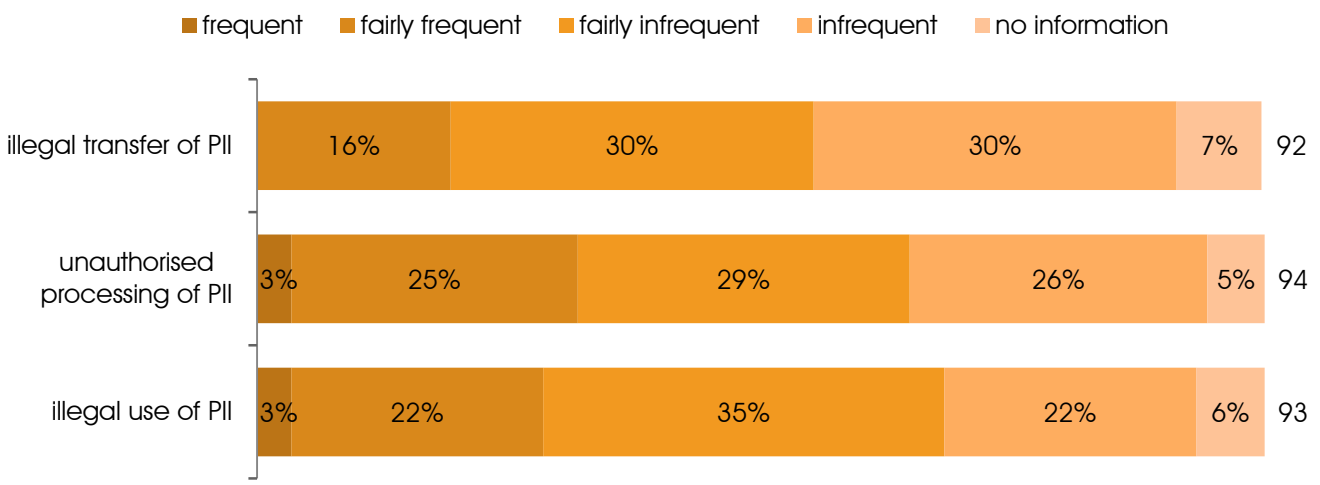
... in the planning phase?"



"...at the start of the project?"



"...only once the project is under way?"

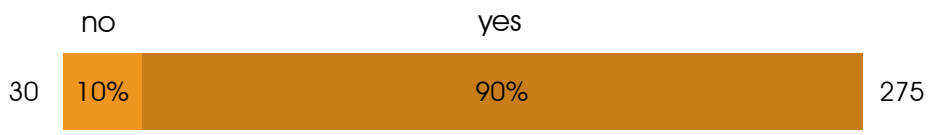


*PII: personally identifiable information (personal data)

When the data privacy officer is not involved in new projects at an early stage, the main detrimental effect is the discovery of unlawful gathering and processing of personal data. When the data privacy officer is involved at an early stage, the rate of data privacy violations discovered is halved.

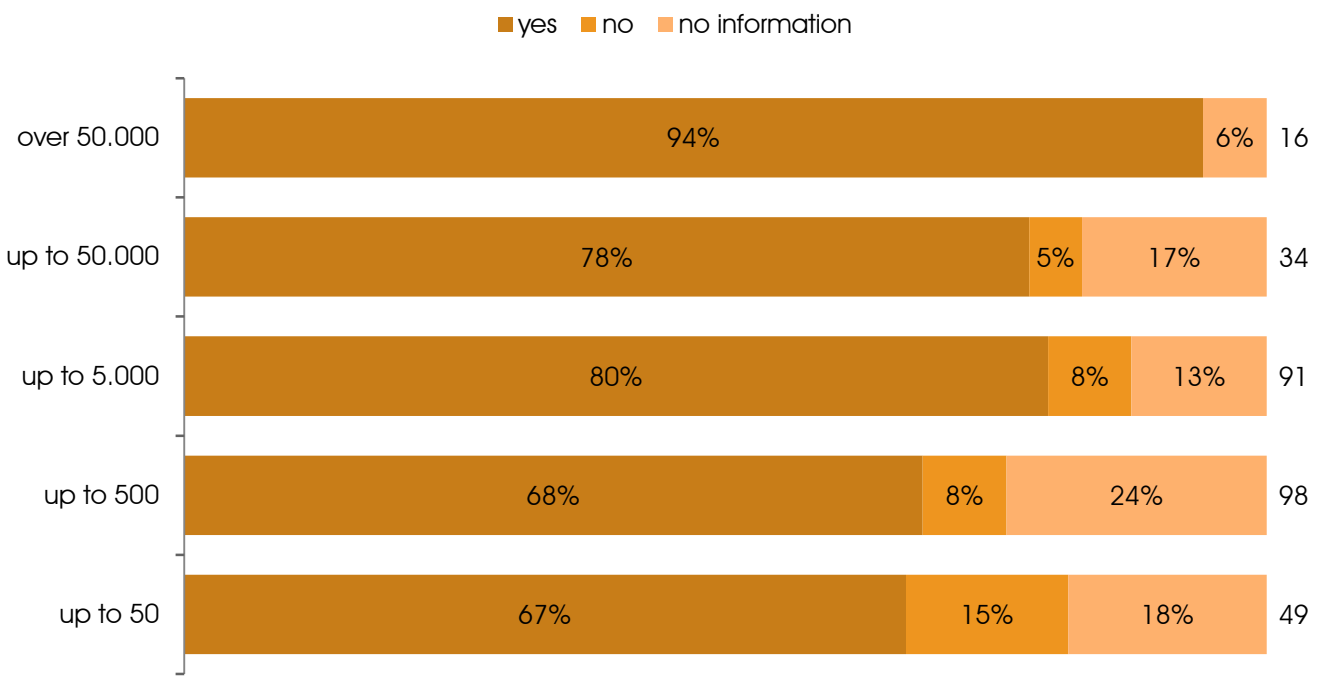
4.5 The register of procedures

1. "Is a register of procedures used in your company?"



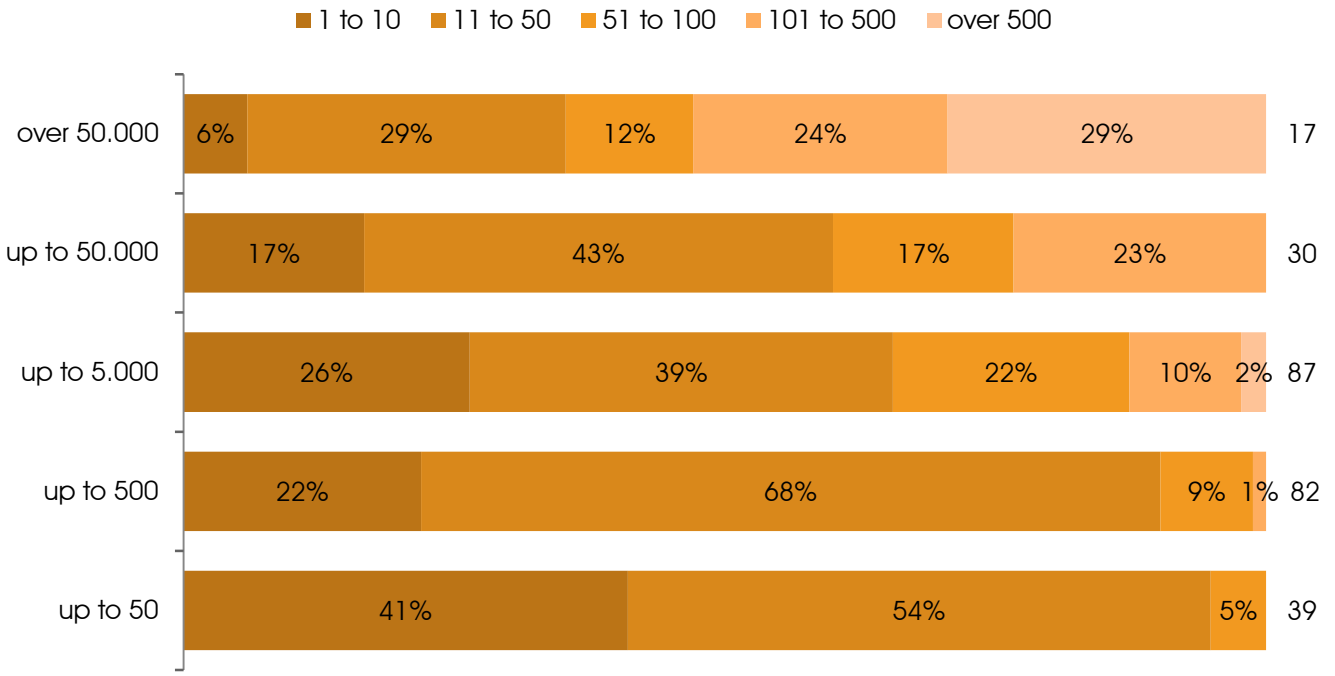
Almost 10% of the data privacy officers questioned still stated in the survey that the company does not maintain a register of procedures. Since with the current state of use of automated data processing systems it is highly unlikely that companies will not automatically process personal data in some form, the absence of a register of procedures under section 4g para. 2 BDSG constitutes an infringement of the company's obligations to make this register available to the data privacy officer. Simultaneously, the absence constitutes an infringement by the data privacy officer against his obligation to make this overview available to any person on request.

"Do large companies keep a register of procedures more frequently than smaller ones?"



The larger the company, the more frequently a register of procedures is maintained.

2. "How many processes are kept in your register of procedures?"



In the overview of all processes of automated processes, the responsibility, legal basis and safety arrangements of all automated data processes must be recorded and documented When asked about the number of individual procedures within one procedure overview, the data privacy officers gave an average of 267 procedures. This number varies considerably with the size of company. Thus, 29% of the data privacy officers in companies with over 50,000 employees stated that their register of procedures covered more than 500 individual processes. These figures make it clear that this is a substantial piece of work in organizational terms that requires significant resources. In the group of companies with under 50 employees, by contrast, more than 90% of the register of procedures contain not more than 50 different processes.

3. "Is there a regulating process that ensures that the register of procedures is kept updated?"

The register of procedures is subject to continual change through every modification within the processes it describes and also as a result of changes to the technical and organizational procedures in the company. To ensure that the register is kept up to date, an internal process in the company is required. According to the responses of the data privacy officers, 130 out of 306 companies (42.5%) have introduced such a process.

4. "Does your company make available a processing overview, as required by law?"

Under the BDSG regulations it is the duty of the company to make the overview of automated data processing procedures (processing overview) available to the data privacy officer. In practice, however, it is often the case that when a data privacy officer is first appointed, he or she must create the register of procedures him/herself. This question was answered negatively by 28% of the data privacy officers, which makes clear, in comparison to the response to question 4.5.1, that here it is not the company that has created the register of procedures and made it available to the data privacy officer – as the law proposes – but rather it is the data privacy officer who prepares the register of procedures. Because of the high demands on the process overviews it may however turn out to be advantageous for the data privacy officer to be closely involved in the process.

5. "Are the company departments involved in creating and updating the register of procedures?"

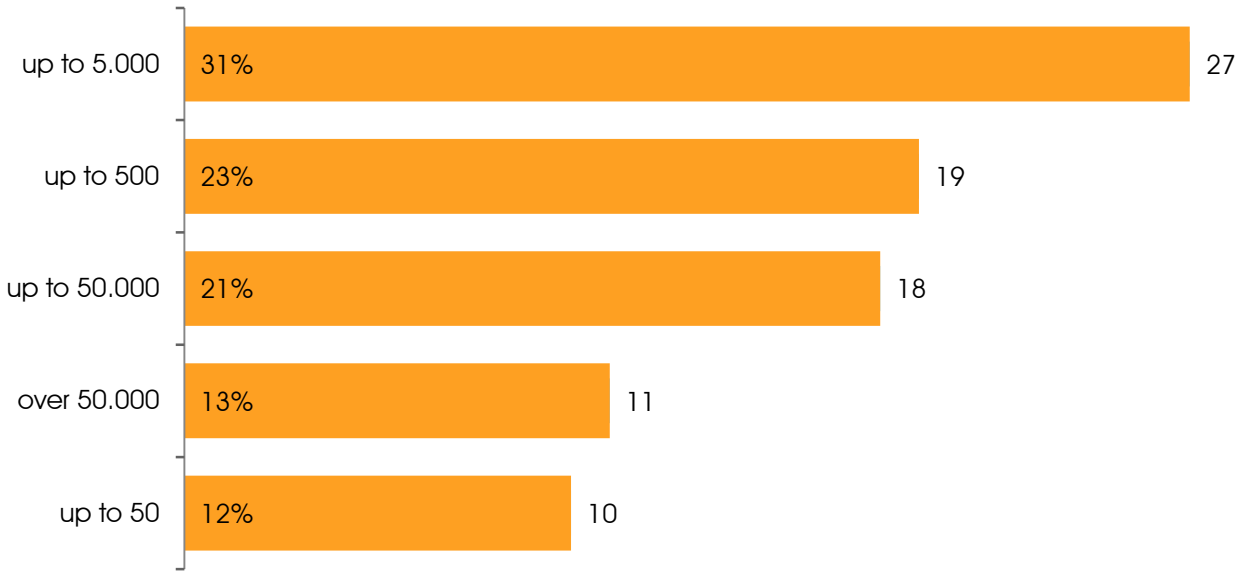
In only 73% of the companies are the departments involved in the creating and updating of the register of procedures.

6. "Do you prefer to compile the register of procedures yourself?"

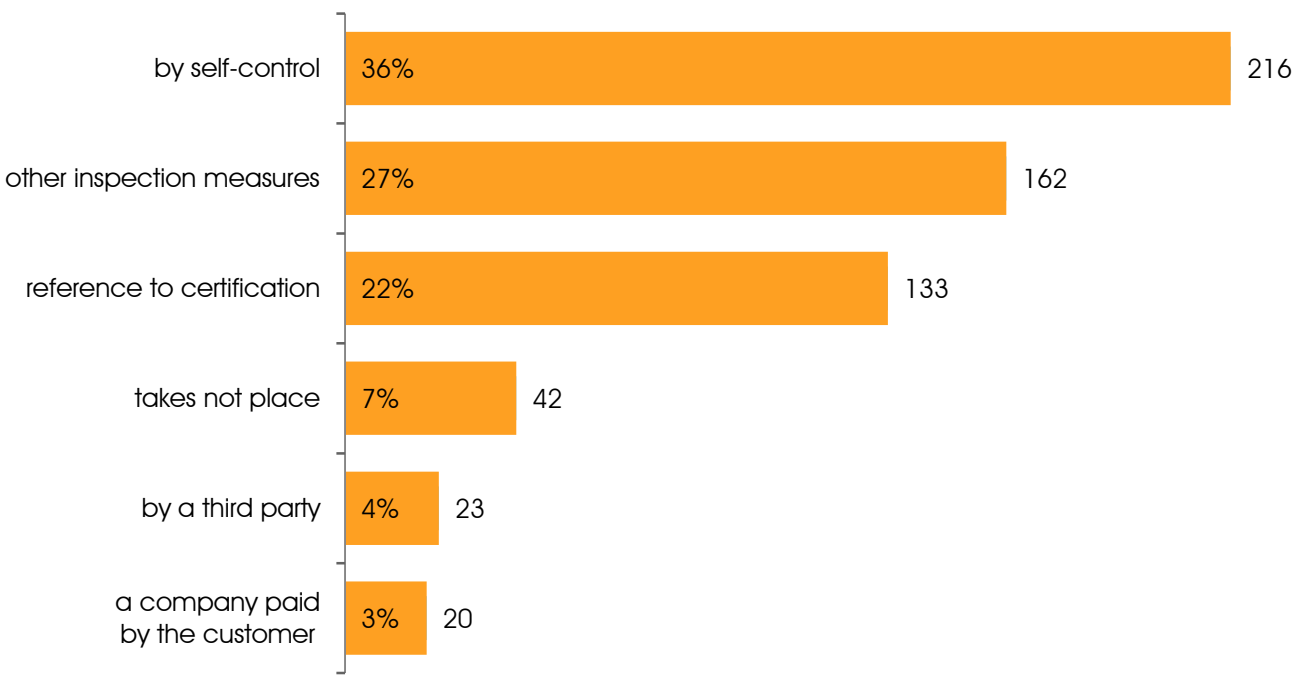
The data privacy officers questioned, who mostly have long experience in applying data privacy law, prefer in 60% of cases to prepare the register of procedures themselves over giving the task to the company departments alone. This indicates the difficulties confronted by employees with an expertise in data protection law when they are required to prepare a processing description themselves.

7. "Are there nominated employees in the company departments who act as multipliers for data protection?"

As company size increases it becomes increasingly difficult for data privacy officers to maintain contact with the various departments. The appointment of data privacy coordinators has in this respect proved successful. This confirms a comparison with company size:



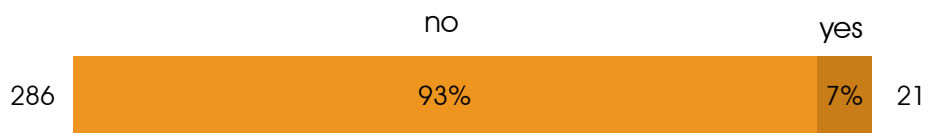
8. "How do you exercise the monitoring required when it comes to processing data on behalf of another client?"



Under section 11 BDSG the client remains responsible under data protection law when he commissions third parties to process personal data. He has extensive control obligations which, however, he may exercise autonomously. No specific form of control is legally prescribed. The responses of the data privacy officers indicate that self-monitoring (37%) and other control measures (27%) continue to have precedence over reference to certifications of the outside contractor, such as EuroPrise, ISO 27001 or BSI IT Grundschutz (23% of all responses) and third parties are only consulted in 7% of cases. Despite the clear unlawfulness of the situation, 7% of respondents still stated that no monitoring takes place.

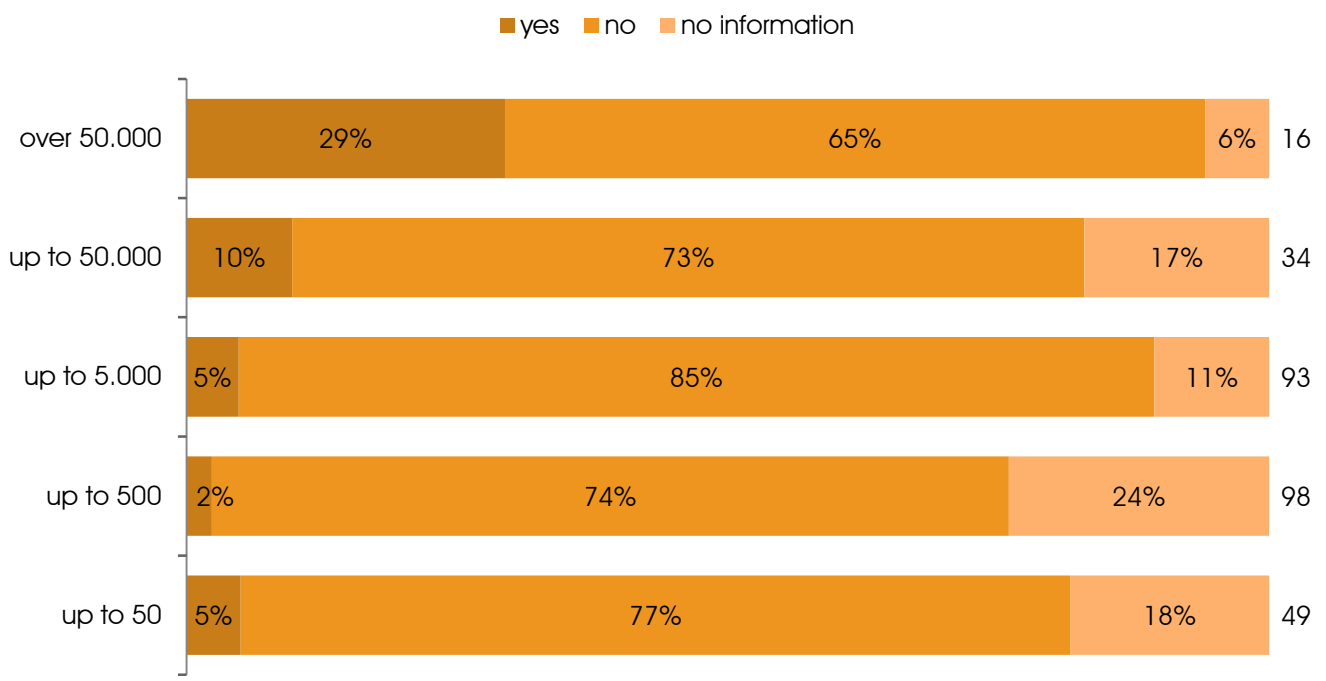
4.6 Certification

1. "Has your company ever received data protection certification (e.g. EuroPrise, ULD or similar) for products or services, procedures or company processes?"



Up to now 21 companies from the participants' group have gained experience of data protection certification.

Opinions of the data protection officers by company size:



Even where certification has already been granted, the percentage share in large companies is significantly higher at 30%. For smaller companies certification has thus far been of only limited importance. Only an average of 5% of companies from under 50 to up to 5000 employees have yet had experience of data protection certification.

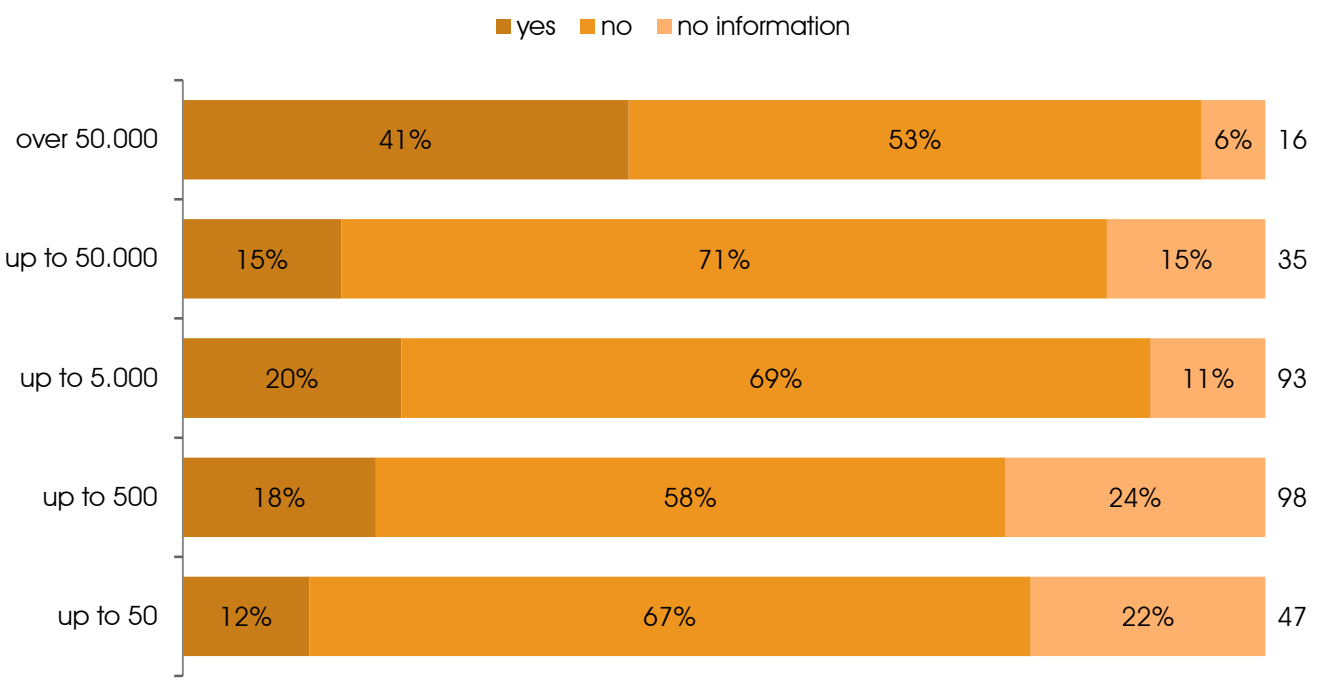
2. "Is your company interested in data protection certification?"

Almost 21% of the data privacy officers see an interest by their company in obtaining data protection certification.

3. "Do you consider data protection certification to be useful for your company?"

Almost 46% of the data privacy officers questioned would regard data protection certification of their company as useful.

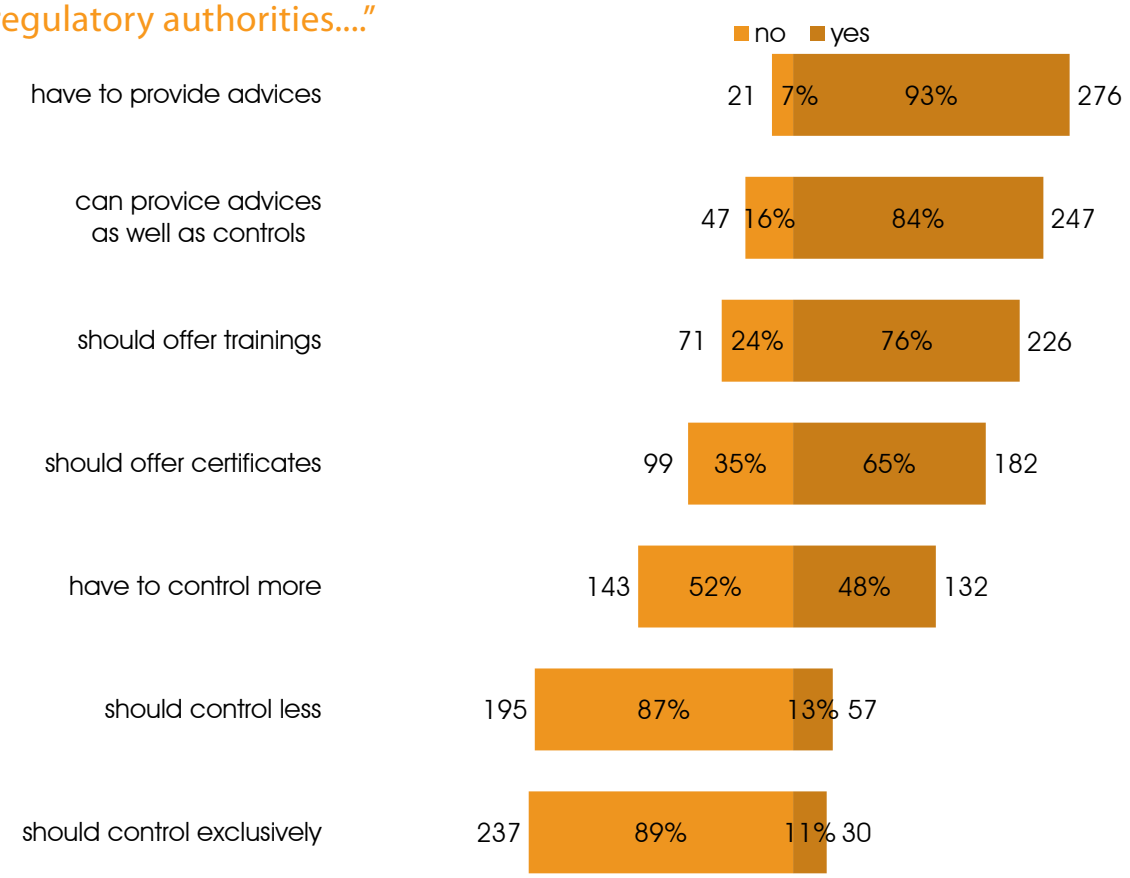
Opinions of data privacy officers by company size:



Interest in certification increases significantly with company size, but only with companies with over 50,000 employees does it cross the 20% threshold.

4.7 Regulatory authorities

1. "Please indicate your position on the following statements about regulatory authorities: The regulatory authorities...."



Enthusiasm among data privacy officers for regulatory authorities is still within limits; nevertheless, 43.3% of respondents would like more checks. In almost complete agreement with this, the data privacy officers (90.5%) demand more consultancy activity on the part of the regulatory authorities and for them to offer training (75%). Nearly 60% of the data privacy officers also demanded certification through the regulatory authorities.

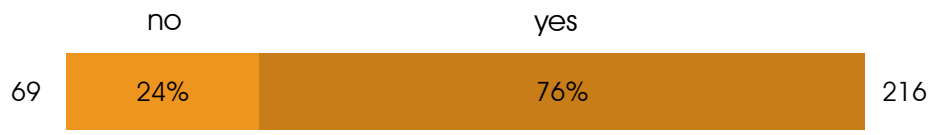
2. "Are the regulatory authorities 'toothless tigers', i.e. do they express criticism but then take no action?"

Criticism of the lack of assertiveness of the regulatory authorities is expressed by only 33% of the data privacy officers, who see the authorities as "toothless tigers".

3. "Are data privacy violations sufficiently prosecuted by the regulatory authorities?"

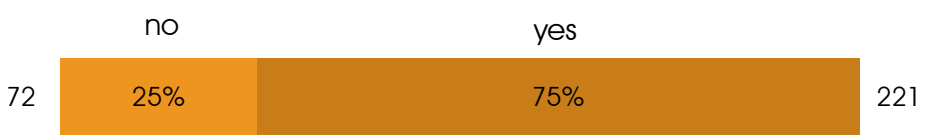
In the experience of 51.6% of the data privacy officers, data privacy violations are sufficiently prosecuted by the supervisory authorities.

4. "Do you regard the punishments that result from this as sufficient?"



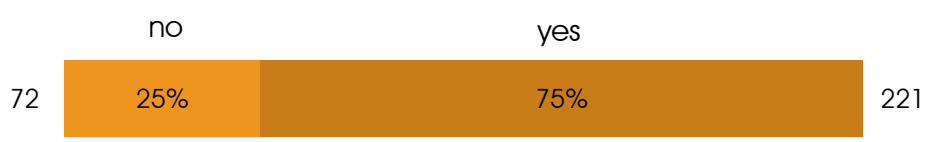
The penalties imposed by the regulatory authorities for data privacy violations in companies are considered by 56% of the data privacy officers as sufficient.

5. "Do you regard the regulatory authorities as sufficiently competent?"



24.5% of the data privacy officers questioned still have doubts as to the competence of the regulatory authorities.

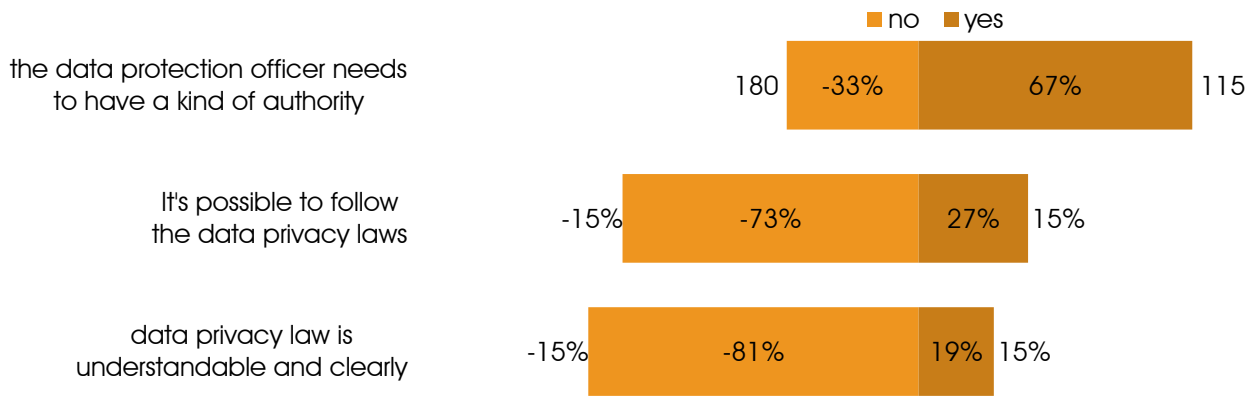
6. "Is the data protection regulatory authority taken seriously in your company?"



Only 75% of the data privacy officers have the impression that the regulatory authorities are taken seriously in their companies.

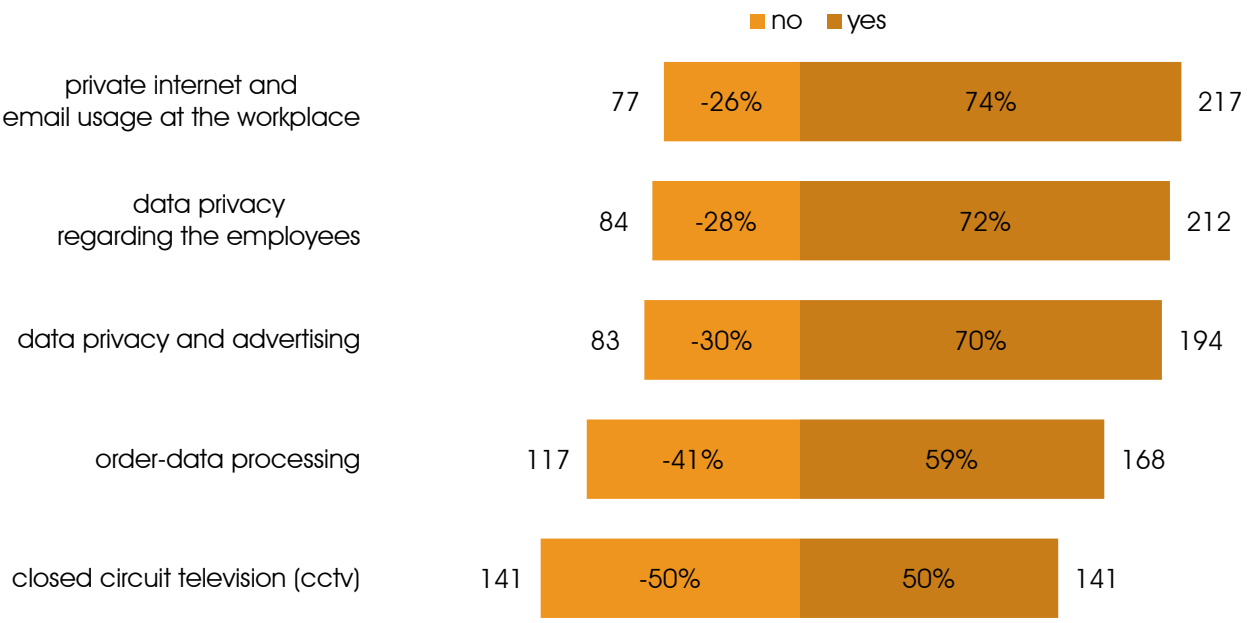
4.8 Legal issues

1. "Please indicate your position on the following statements:"



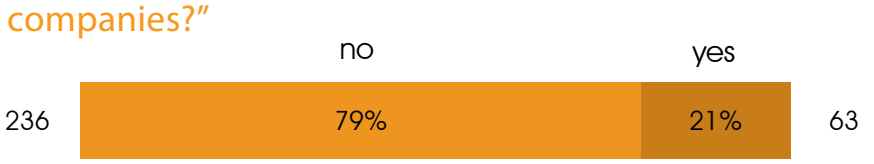
Almost 66% of the data privacy officers questioned argue in favor of a form of power to direct for the data privacy officer. The greater part of the data privacy officers regard the existing data privacy laws as neither understandable (80.7%) nor practical (72.5%).

2. "Changes are needed in the areas of:"



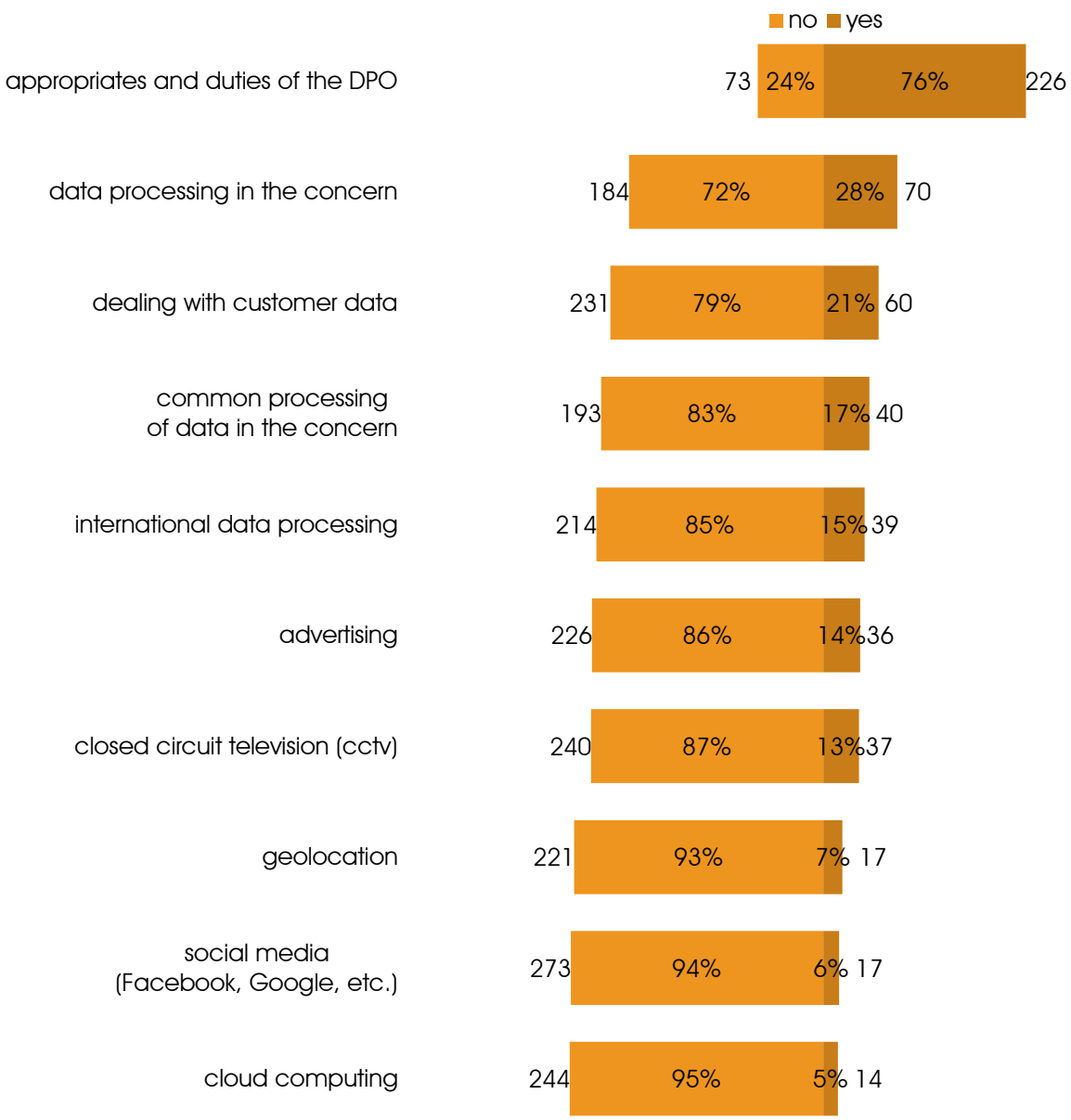
A large majority of the data privacy officers would like changes to the law in the areas of private internet and e-mail use at work (72.1%) and in employee data protection (70.2%). The data privacy officers also see the need for action on the regulations on data protection and advertising (64.5%). The general opinion with regard to the issue of video surveillance remains undecided. 46.7% spoke in favor of amendments to the legal situation and the exact same number spoke against them. A slight majority of 55.8% also wanted changes in the area of contract data processing.

3. "In your view, are the legislators orientated towards the real problems for data protection in companies?"



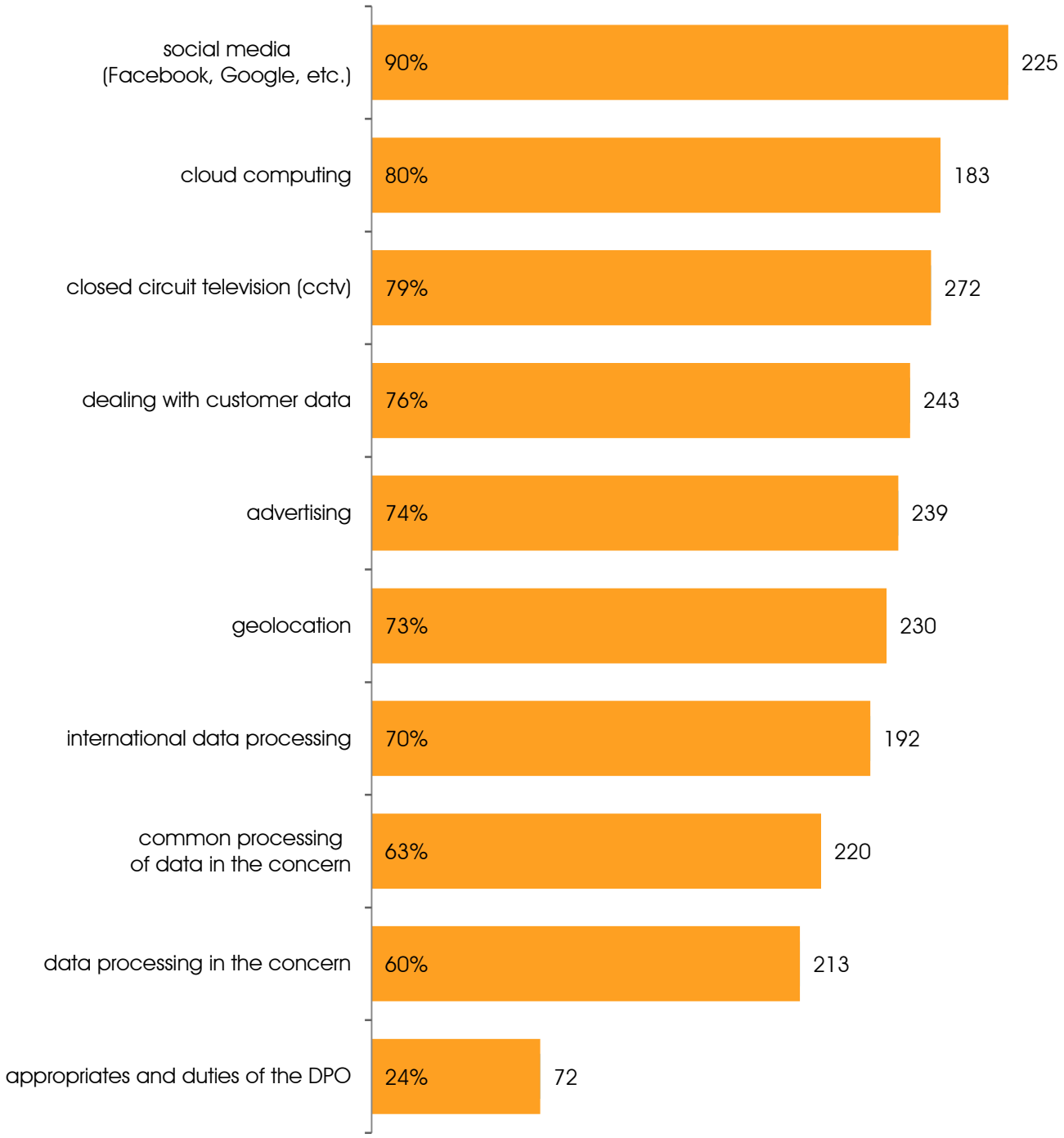
A full 21% of the data privacy officers questioned consider the legislators' orientation as focused on on data protection problems in companies; 79% deny this.

4. "In your view do the existing laws cover the following areas in a practical way?"



The data privacy officers questioned are mostly satisfied with the legal regulations concerning the rights and obligations of the data privacy officer. However, on all other areas of regulation raised, their view was negative.
"no opinion" has not been considered in the analysis. This is why there can be differences in the summation.

Top of the negative ranking are the topics of social media and cloud computing, and also video surveillance. Only the rights and duties of the data privacy officer seem here to be sufficiently legally clarified.



The opinion profile of the data privacy officers reflects the public discussion very clearly: the new challenges to data protection law as a result of international networking represent a significant task for the legislature. Traditional data protection law seems not to provide convincing answers for international communication. When it comes to so-called social networking offerings, not only does the relationship of informational self-determination and commercial utilization of private communication come up against technical limits, but the national regulations also come against the limits of internationally performed services. Even where the (im)permissibility of data processing actions outside Europe and by states with comparable levels of data protection is clearly set out in the law, the business models of cloud computing are economically viable or social media becomes attractive to such an extent that data protection regulations seem to be urgently needed. The new possibilities for networking and thus for the blending of data throw up a variety of problems - whether it be in video surveillance, in the handling of customer data, in international data processing particularly by corporations, or in the new geolocation possibilities for devices and thus also for people. Under the decision of the Federal Constitutional Court in the so-called census verdict (Volkszählungsurteil), the legislator is obliged to weigh up the conflicting interests and to resolve the conflict in accordance with data privacy laws.

5. "In which areas do you further see a need for the legislator to catch up?"

The participants had the opportunity to formulate additional topics in a free text field. In a total of 54 suggestions the participants argued for a fundamental simplification of the law and the application of the law for improved consideration of business concerns, particularly for the situation in corporations and the internationalization of the world of work and for better coherence of the data protection regulations in the different special laws. Particularly for the appointment, initial and advanced training and the equipping of in-company data privacy officers, more concretization is expected.

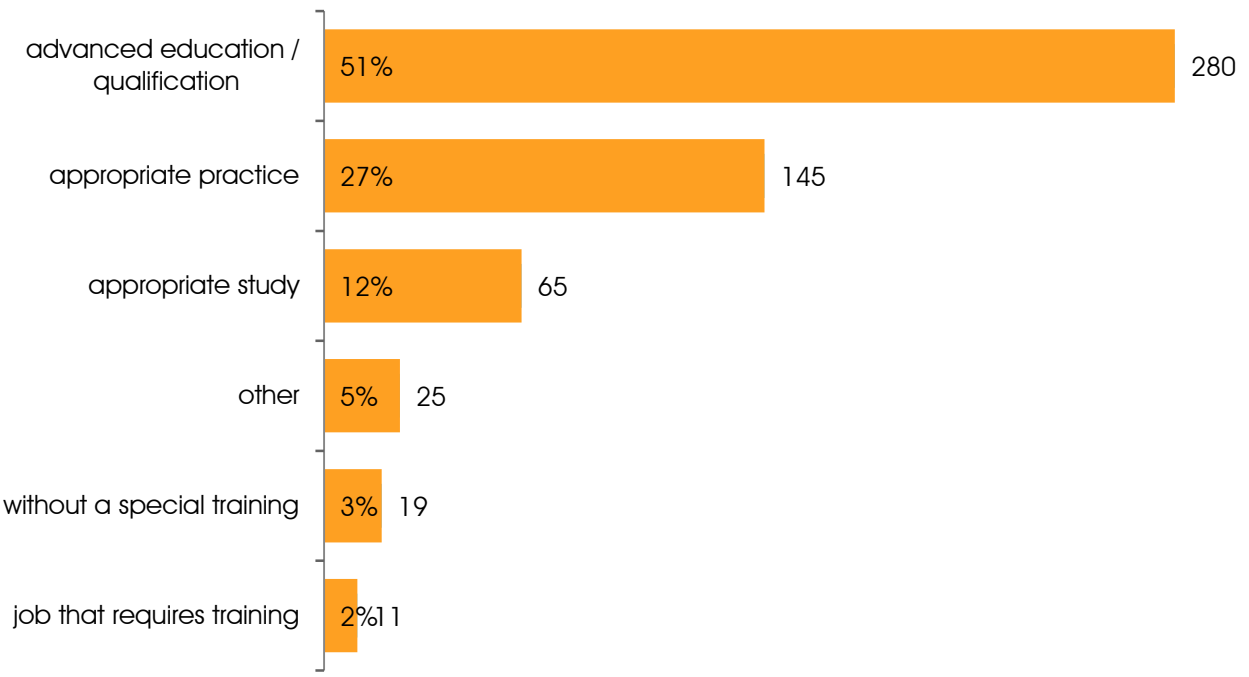
Legislative responses to the technical requirements created by social media, mobile end devices, cloud computing, web analysis and biometric data are particularly sought, and 11 respondents demand a regulation on employee data privacy.

4.9 Training of the data privacy officer

1. "Do you consider a legally prescribed training for data privacy officers to be useful?"

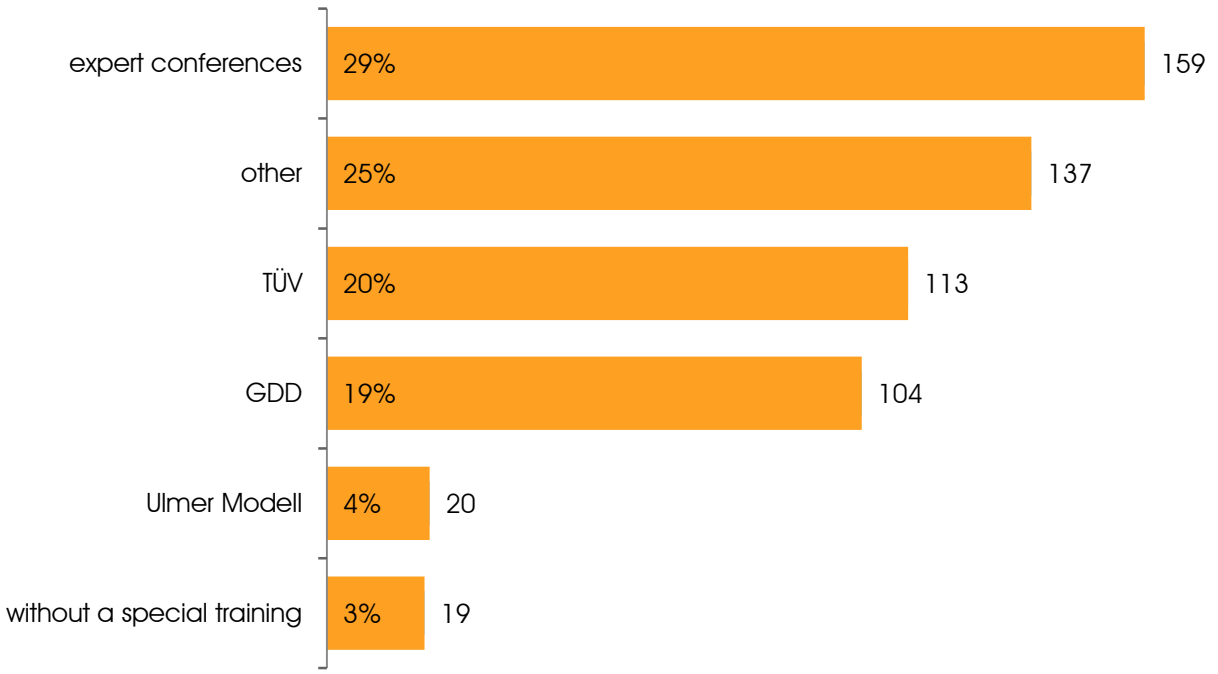
The BDSG sets personal and material requirements for the appointment of a data privacy officer that have been concretized by a resolution of the supreme regulatory body. To date there exists no vocational training or professional qualification with a legal basis. This lack is an issue of complaint not only for trainers and the professional association; 64% of respondents to the survey also argue for legally regulated training.

2. "How did you gain your qualification as a data privacy officer?"



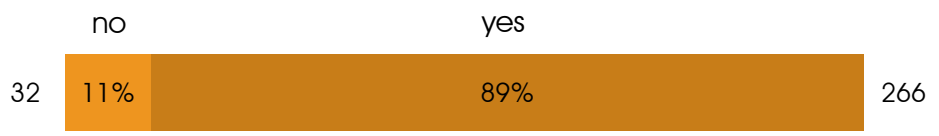
The professional qualification required for working as a data privacy officer can be obtained, for example, through a study of engineering or law at degree level. These disciplines, however, provide only a basic competence, which must be complemented by suitable advanced training. The market for such training includes various modular options spread over several weeks and also intensive courses lasting between one and five days. 51.4% of the participating data privacy officers stated that they gained their qualifications through continuing professional development measures; 26.6% rely on the experience they have gained in the course of their work and 11.9% rely on prior knowledge obtained from a course of study. These results demonstrate that the required qualifications are generally gained through advanced training and experience gained on the job.

3. "Which of the advanced training options have you used in addition?"



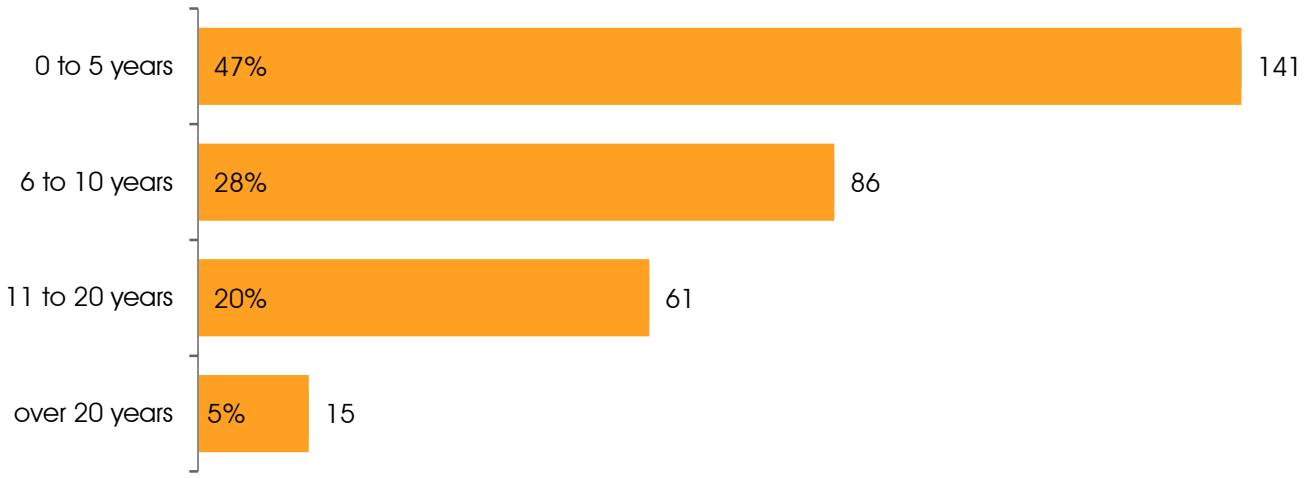
In the survey the most important providers of qualified advanced training were questioned. The Ulm Model and the German Association for Data Protection and Data Security (GDD) both offer modular courses spread over several weeks, while the TÜV and other providers generally offer only courses of a few days. Various expert congresses have also established themselves in the area of data protection as providers of specialist advanced training. Among a selection of continuing professional development options, specialist conventions were most frequently selected as a possibility for further training (28.8% of responses). The offerings of TÜV (20.4%) and GDD (18.8%) received almost equal preference. 33 survey respondents stated that they had participated in training events by both TÜV and GDD. 20 respondents were trained on the basis of the Ulm Model. Only 19 respondents said that they had not made use of any continuing professional development options. Of these, ten have been in

4. "Are you a lateral entrant into data protection?"



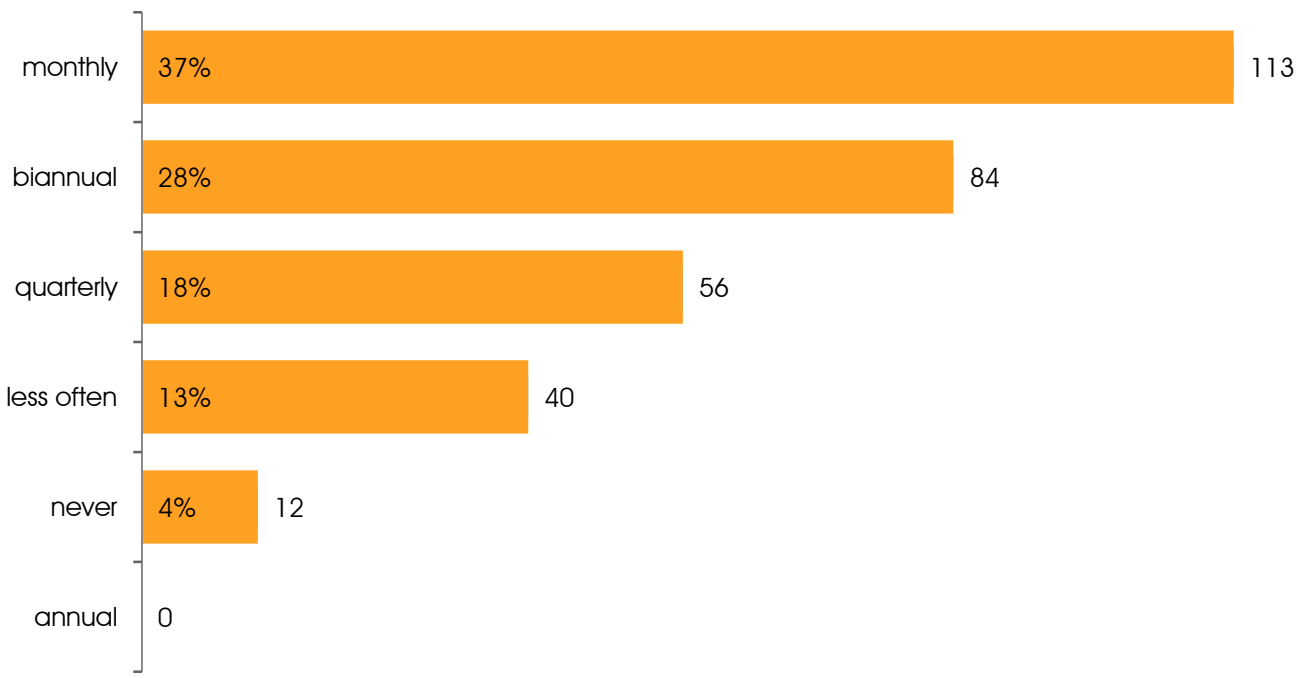
Unsurprisingly, 89% of the data privacy officers questioned stated that they had come to their work from another background.

5. "For how long have you worked in data protection in general?"



In Germany there has been an obligation, punishable with a fine if neglected, to appoint a data privacy officer since 1 July 1977. The data privacy officers questioned stated that on average they had worked in data protection for 7.7 years. 15 respondents to the survey have worked in the field of data protection for over 20 years, 61 between 10 and 20 years and 86 between six and ten years. 47% of respondents have worked in data protection for less than five years. The total amount of experience of all participants is thus 2335 years.

6. "How often on average do you attend advanced training events?"

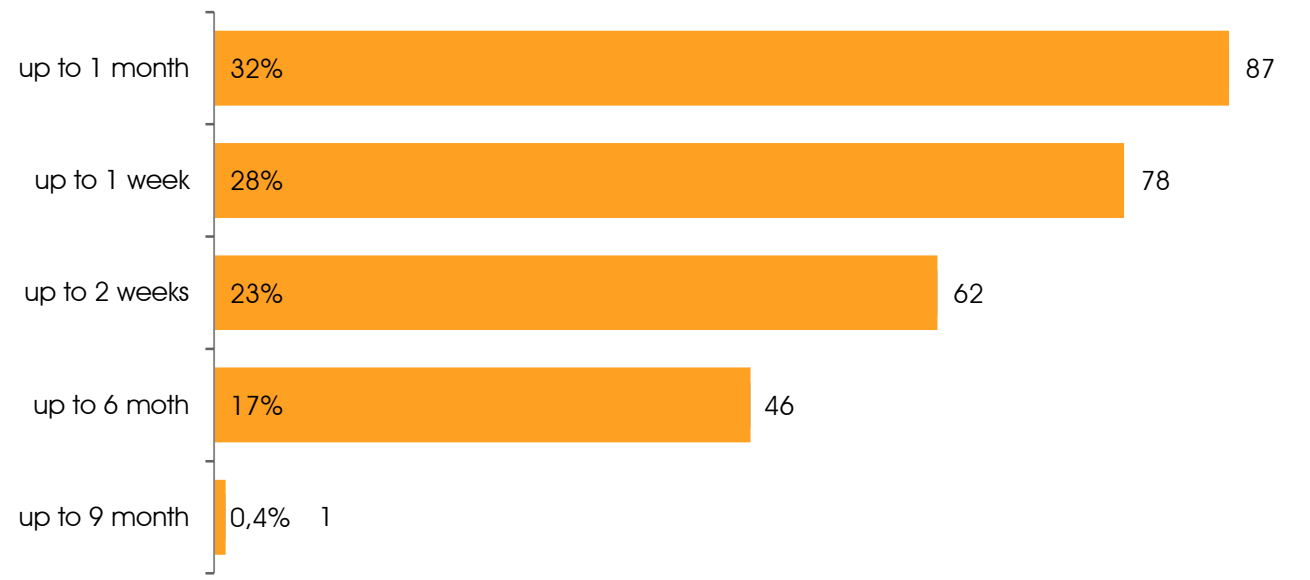


A particular challenge for the work of a data privacy officer arises not from the complexity of the tasks in the company but rather from continual changes in the legal framework and from technical developments. Regular training is therefore of particular importance. 37% of the data privacy officers questioned stated that they attend monthly training events; 28% do so twice per year and 18% quarterly. Overall, 83% of participants undertake training at least once per year and 13% less than once per year. Only 4% answered "never".

7. "What is your preferred mode of taking ongoing training?"

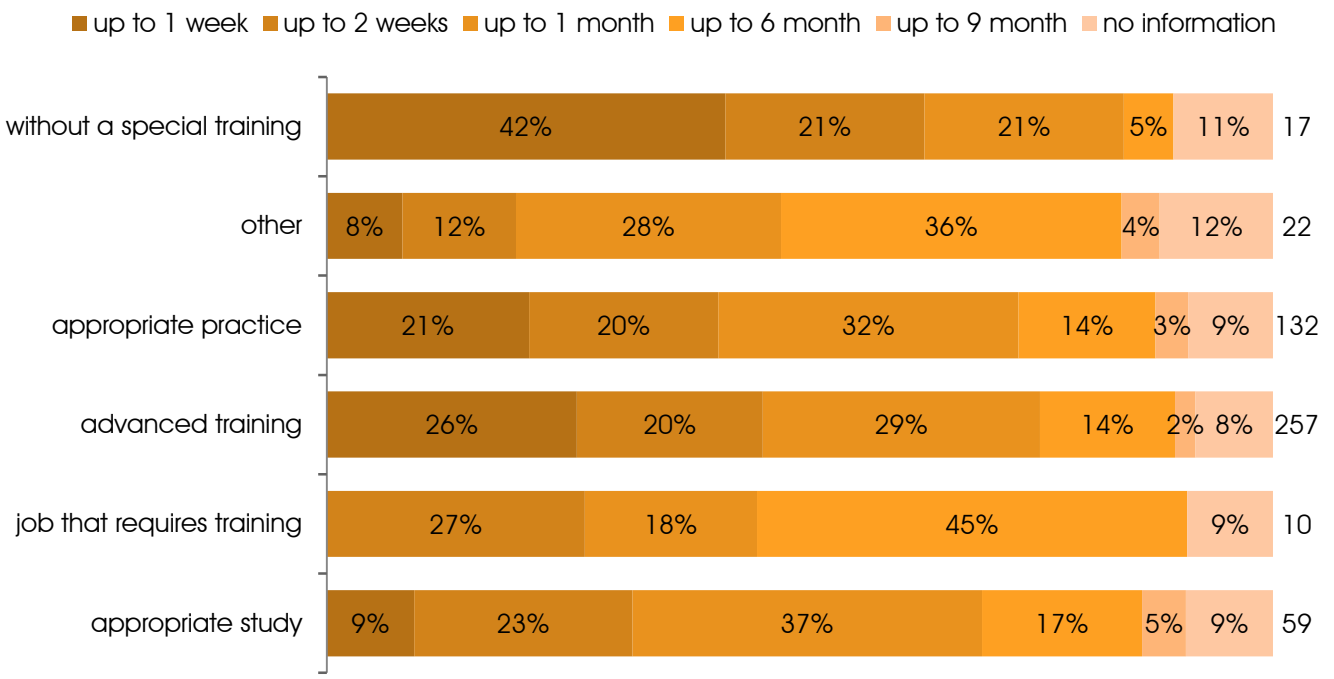
Answers to a question about preferences in respect of training formats is surely largely influenced by personal experience, but it also reflects the specific needs of the participants. The data privacy officers showed a strong preference for training in the form of external events. 83.1% of the respondents stated that they preferred to participate in external training events. Self-study is preferred by 11% of participants, while online training has become the preference of only 6% thus far. This result is unsurprising in the light of the specific need for advanced training. Data protection practitioners rely on highly specialized training options that as a rule are not available either in online training or in in-company training activities. Self study also has only a limited suitability for imparting highly up-to-date knowledge and competences.

8. "How many days have you invested in data protection training so far?"



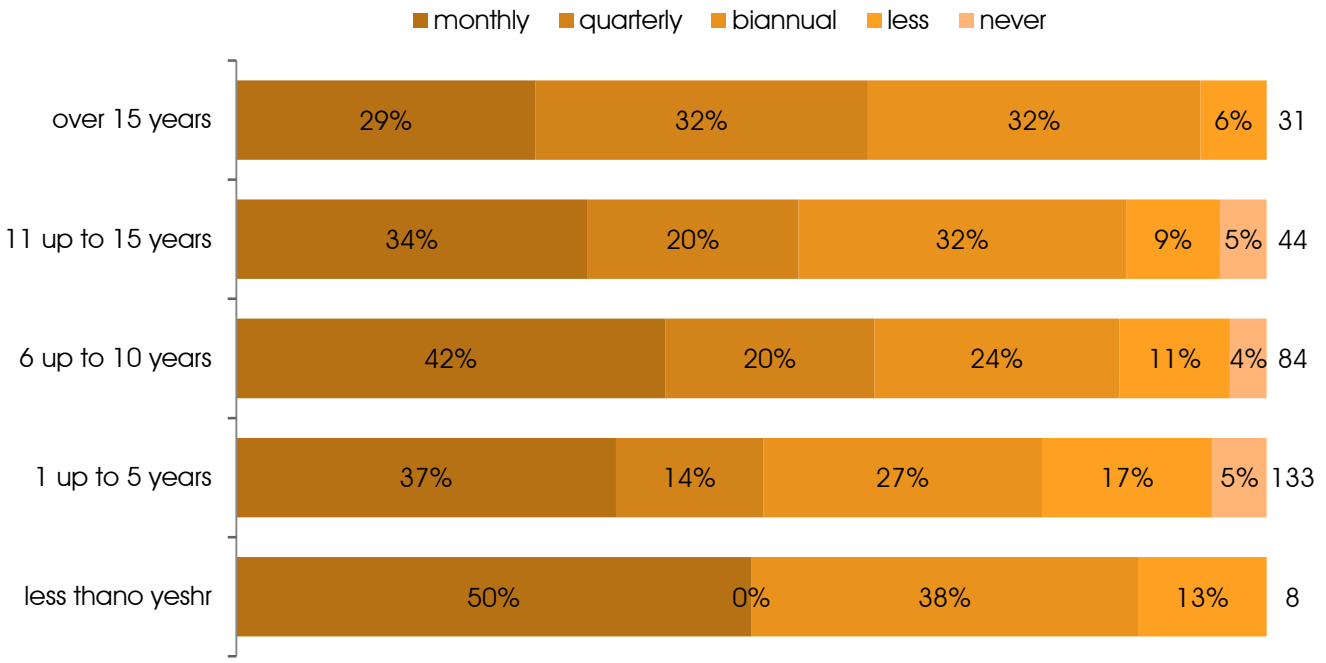
On average the data privacy officers questioned stated that they had invested 22 days in their own training in data protection.

"Does the type of initial training you had have an influence on the amount of time you have subsequently spent in advanced training?"



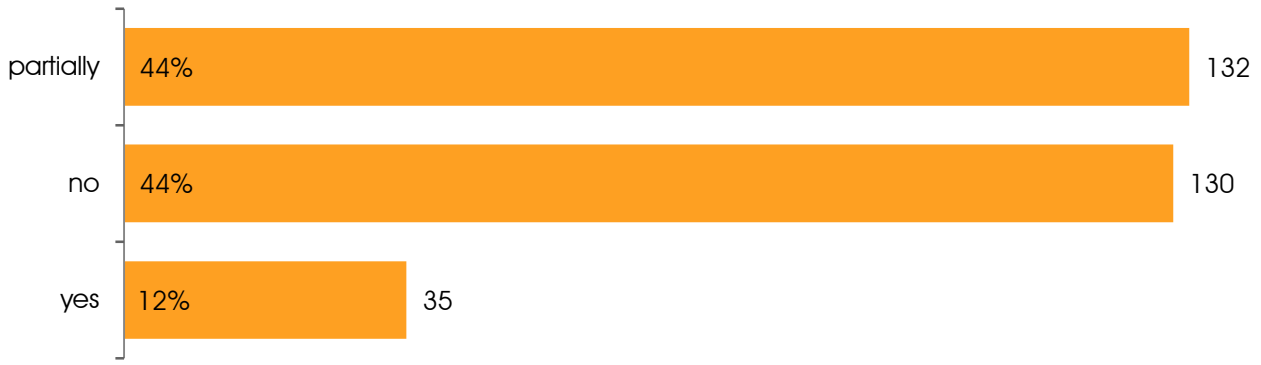
On closer examination it can be seen that less qualified data privacy officers tend to undertake less advanced training while highly qualified officers undertake training significantly more often, including within their work.

"Does the length of your appointment as a data privacy officer have an influence on the amount of time you have subsequently spent in advanced training?"



In the first year of appointment the proportion of monthly training among the data privacy officers questioned is highest. Overall, however, the the need in the first five years is not yet covered. Here, 13% and 17% of the respondents, respectively, state that they have undertaken no advanced training. This proportion falls as professional experience increases. As the length of professional experience increases, the time spent on personal training decreases, though only slightly. Even among data privacy officers with more than 15 years of on-the-job experience, 29% undertake monthly advanced training, 32% do so at least quarterly and as many again do so half-yearly. These figures underline the high importance of advanced training for data privacy officers.

9. "Do these trainings include a final exam?"

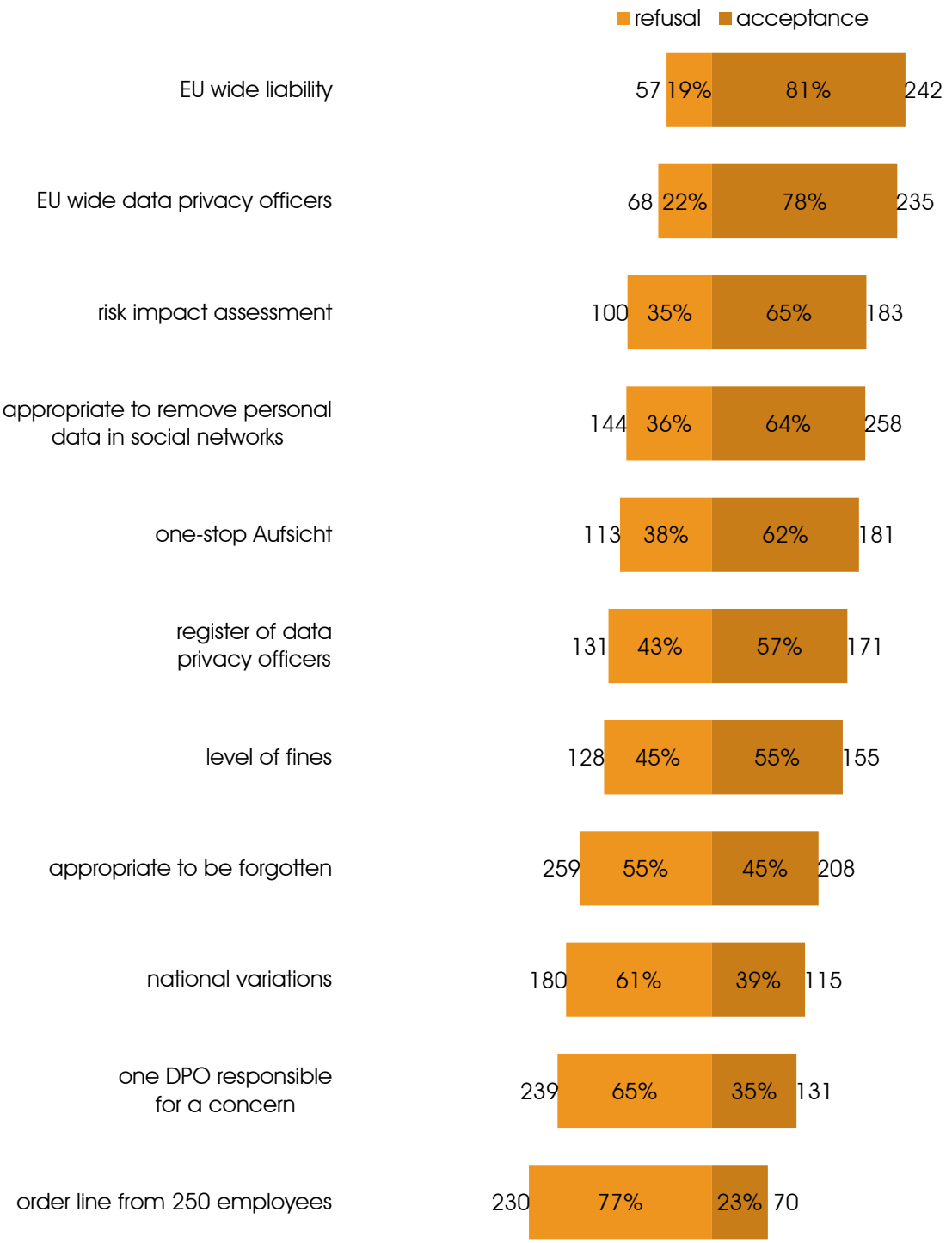


Of the training events used by the data privacy officers, 56% also include a final examination on at least some of the training outcome.

4.10 The new EU data protection regulation

On 25 January 2012 the EU Commission published its proposals for a new legal framework for data protection, including an EU general data protection regulation to regulate matters such as company data protection uniformly throughout Europe. The Data Protection Practice 2012 survey serves as a compilation of the first reactions from practitioners to this.

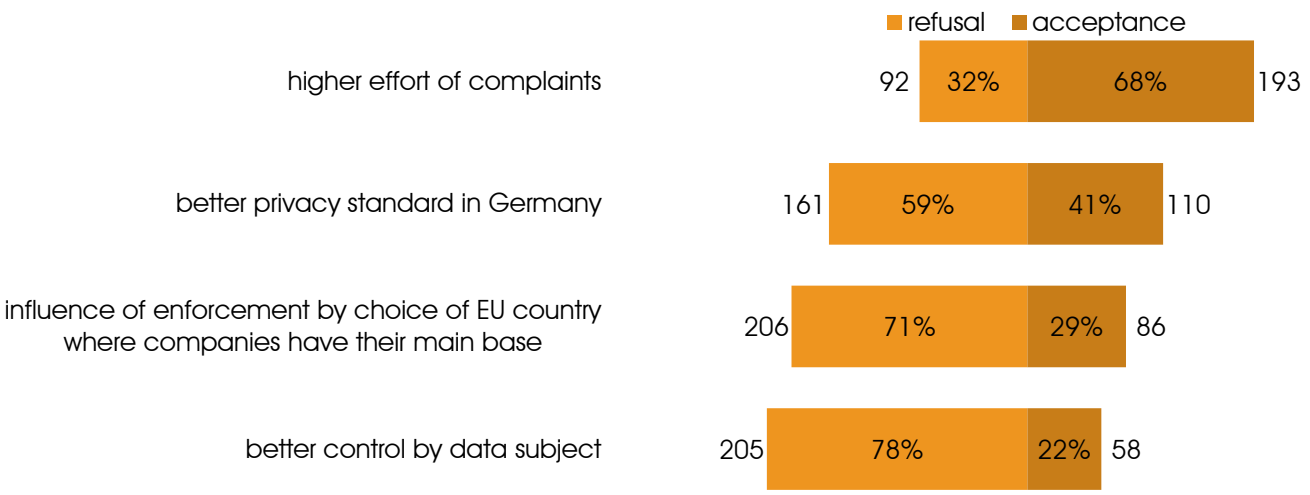
In summary, the appraisal of the proposals by German data privacy officers of selected points appears as follows:



The practitioners regard the EU Commission's intention to unify data privacy law throughout the EU by means of a regulation as predominantly positive (see 4.10.3). The elaboration of the function of an in-company data privacy officer (see 4.10.10), the proposed maximum level of fines (see 4.10.7) and the proposed lead regulatory body (a "one-stop authority", see 4.10.19) generally receive the agreement of the practitioners. Even the proposed registration of all data privacy officers with the regulatory authorities gains a slight majority in agreement.

The response is different if there is a possibility of national deviations: a majority of the practitioners opposed such an escape clause (see 4.10.4). The proposed number of 250 employees per company as the threshold at which the obligation to appoint a data privacy officer begins was also regarded with criticism by the practitioners (see 4.10.14). The Commission's proposal to introduce a corporate privilege, such that a corporation need only appoint one data privacy officer for the whole group, was also generally met with incomprehension (see 4.10.15).

As for the material data protection regulations, the practitioners were generally divided – while there was a majority of agreement for the objective of the regulation, there is often a lack of certainty as to how it can be implemented. The right to remove personal data in social networks is regarded by 69% as positive (see 4.10.8); the risk impact assessment obligation likewise by 65% (see 4.10.16), and the onward notification of the erasure request to all data recipients (the "erasure chain", see 4.10.9) is regarded by 56% as mainly positive.



A majority of practitioners regard the achievement by the Commission of the most important goals with pessimism; they expect neither better control possibilities for data subjects over their personal data (see 4.10.6) nor overall a better level of data protection in Germany (see 4.10.5). On the other hand, a majority believe that higher expenses will be incurred in the event of complaints (4.10.20). The effect of the new regulations on data protection supervision, much feared in discussions, on the choice of country of domicile for large companies is in fact feared by only 30% of the practitioners. 70% consider such an influence to be "unlikely" or "fairly unlikely" (see 4.10.21).

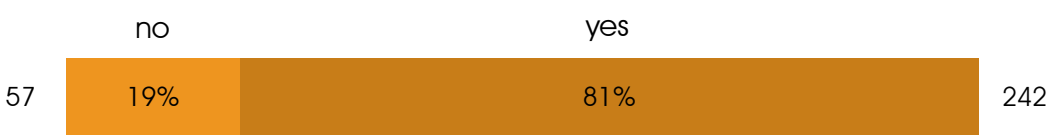
1. "Have you read the EU data privacy regulation?"

At the time of the survey, February to April 2012, 46% of respondents had already read the drafts published on 25 January 2012. The date of publication of the Commission's proposals had been announced long in advance, although rumors had been spread in December that resistance from the Commission meant that the date could not be held. The announcement of the proposals at the World Economic Summit by the vice president of the Commission, Viviane Reding, added greatly to public awareness and particularly to professional interest in them. However, there were at first serious reservations on the part of data privacy professionals, since the direct legal effect of a European regulation - i.e. its effectiveness even without a national implementation law - was in many respects new and surprising for them. Many recognized its direct relevance to their practical work only later. It is therefore not surprising that only 46% of the data privacy officers questioned had already set aside time to study the proposals.

2. "Have you informed yourself about the regulation from the media?"

70.5% of respondents had already informed themselves about the draft regulation through the media.

3. "Is an EU-wide unification of data protection the right way forward?"

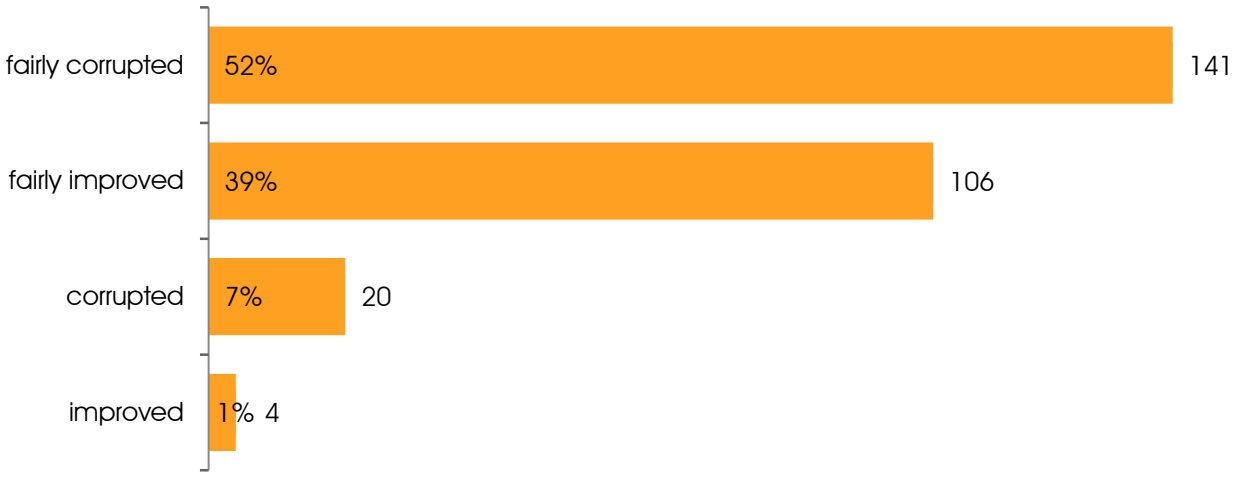


81% of all data privacy officers questioned consider that an EU-wide unification of data protection is generally the right way forward.

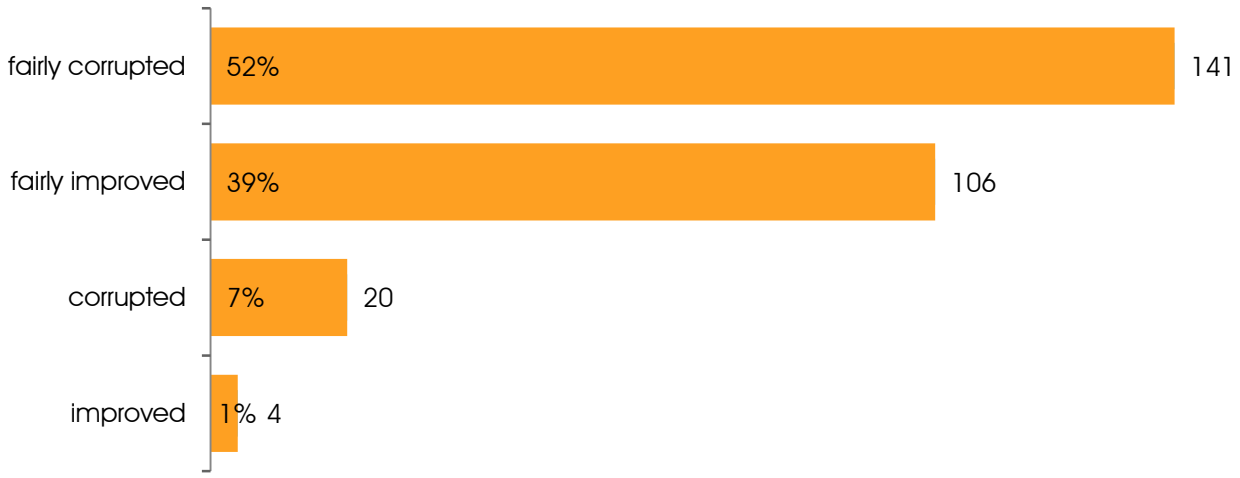
4. "Should member states have the right to deviate from the level of data protection set out in the regulation?"

Even when a significant majority argue against deviations at the national level, still 39% of the data privacy officers still want the possibility for member states to be able to deviate from the level of data protection proposed in the regulation.

5. "Will the EU data privacy regulation result in the level of data protection in Germany being improved or worsened?"



40.6% of the data privacy officers questioned expect an improvement in the level of data protection in Germany, while 59.4% of those questioned anticipate a worsening. Among those who have already read the regulation this value improves by only one percentage point, as the following chart shows:



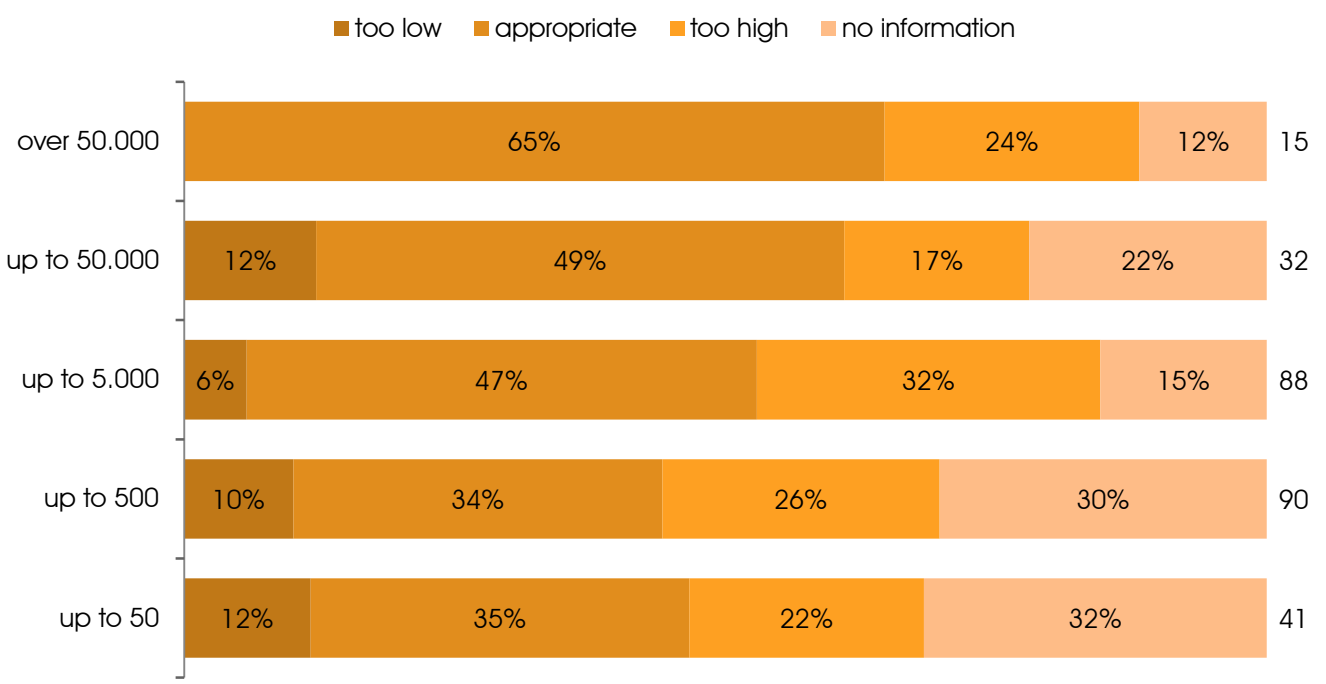
6. "In your view, does the EU data protection regulation restore control over personal data to the data subject?"

As understood in German data protection, the right to informational self-determination has the objective of allowing the data subject control over his or her data. The Commission is also committed to this objective in its implementation of article 8 of the Charter of Fundamental Rights, article 16 of the Treaty on the Functioning of the European Union and in article 8 of the European Convention on Human Rights. The data privacy practitioners nevertheless are mostly in doubt as to the possibility of implementing this proposed objective. 78% 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.

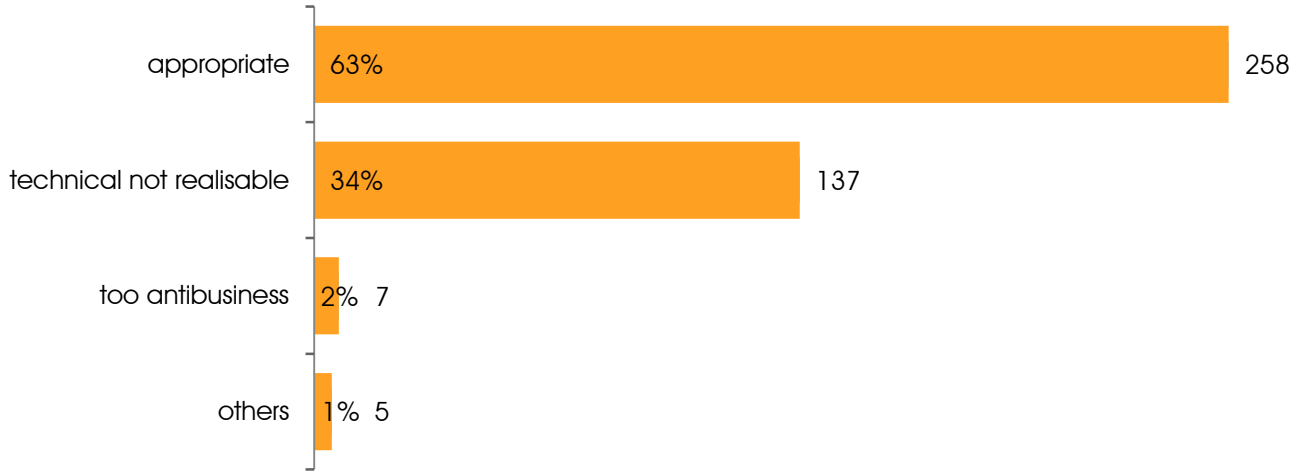
7. "What is your view of the amount of the fines of up to €2 million or 2% of turnover?"

The data privacy officers regard this proposed framework of fine levels as relatively balanced. Almost 55% of respondents consider fines of up to €2 million or 2% of turnover as "exactly right", 11.6% as "too low" and 33.8% as "too high".

Views of the data privacy officers by company size:

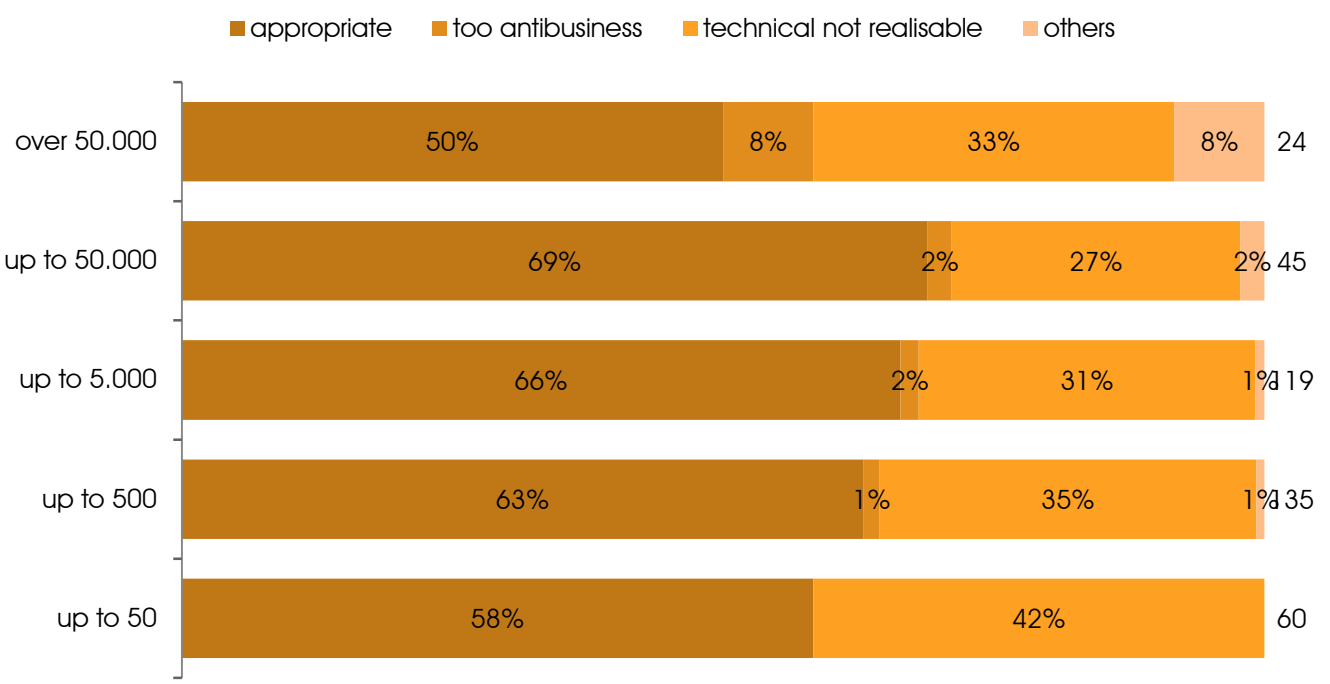


8. "How do you view the right to remove personal data in social networks?"

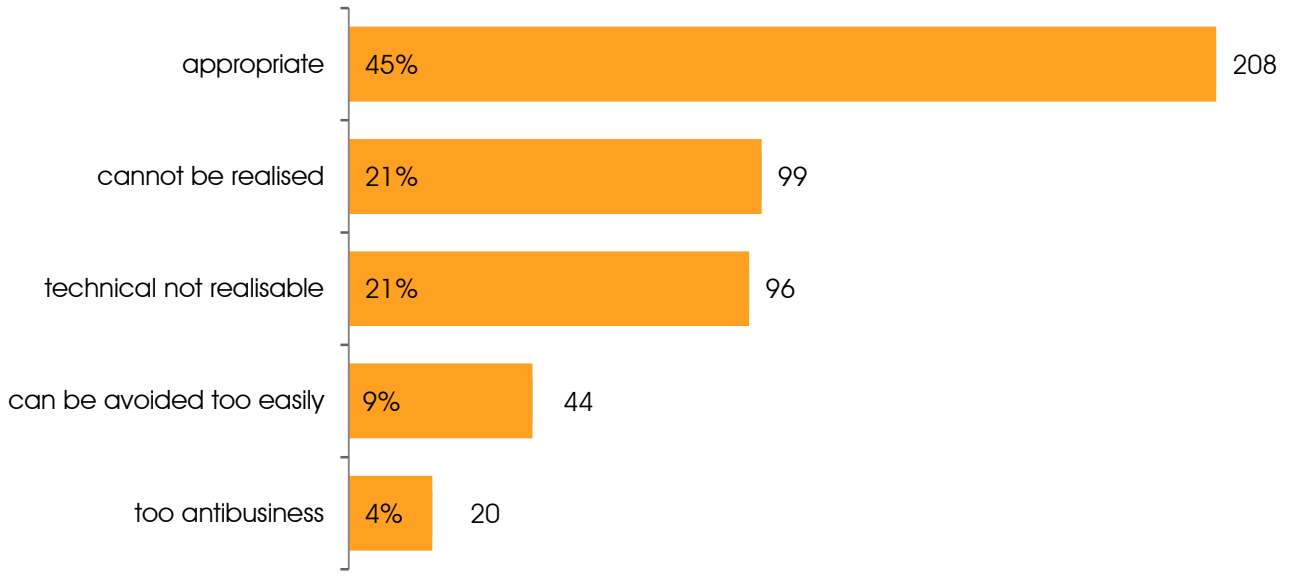


The right to remove personal data in social networks is considered correct by 69% of respondents, though 36.9% see it as not technically realizable. The figures exceed 100% because it was possible to give multiple answers to this question. Still, 98, or 27.5% of respondents consider the introduction of such a right as both "correct" and "technically unrealizable". This shows a clear support of the intention but also doubts as to the technical feasibility of these proposals.

Opinions of data privacy officers by company size:

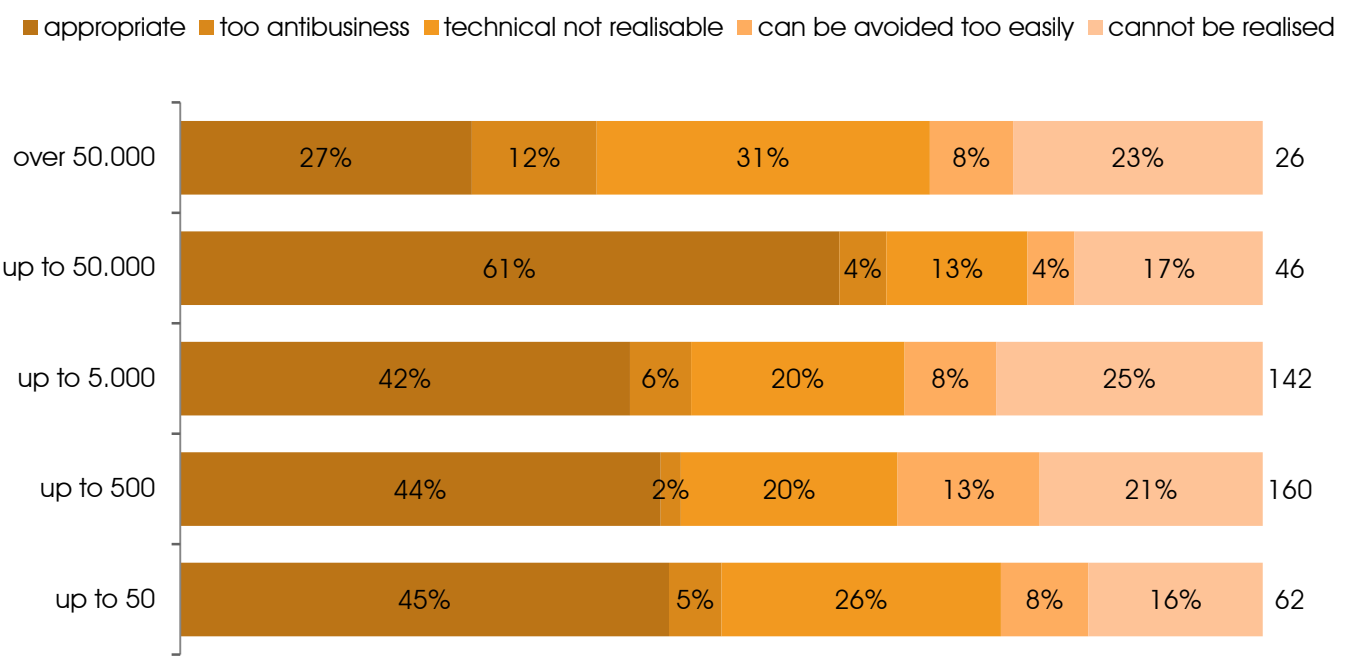


9. "What is your view of the fact that companies must take all reasonable measures to inform third parties who process this data of the user's intention to erase it?"



Data transfers are an everyday occurrence in our networked society and they are the biggest problem for enforcing a demand for erasure. The proposed obligation to notify data recipients of an intention to erase ("erasure chain") is agreed to by 56% of the data privacy officers, but 45.9% of them doubt its enforceability (technically unrealizable, can be bypassed, or unenforceable, or combinations of these).

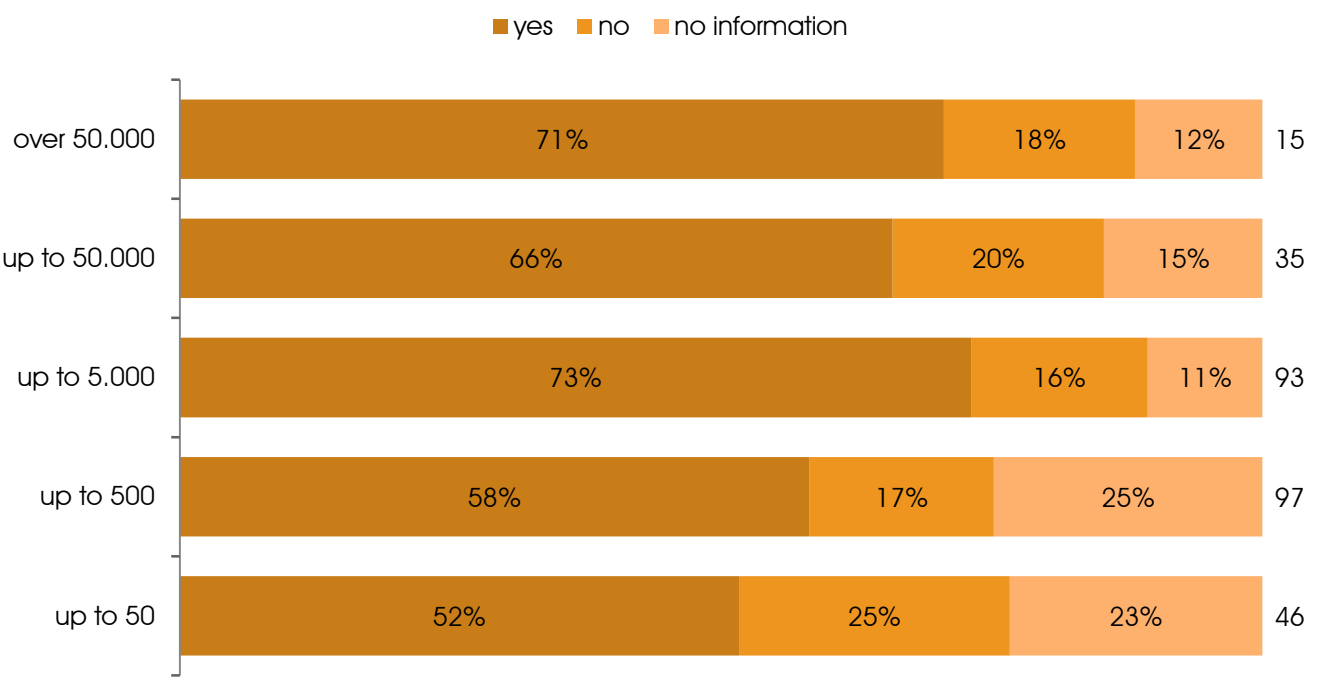
Opinions of data privacy officers by company size:



10. "Do you consider it right that the requirements of data privacy officers should be legally governed?"

77.6% of respondents consider a legal regulation of the requirements of data privacy officers to be correct.

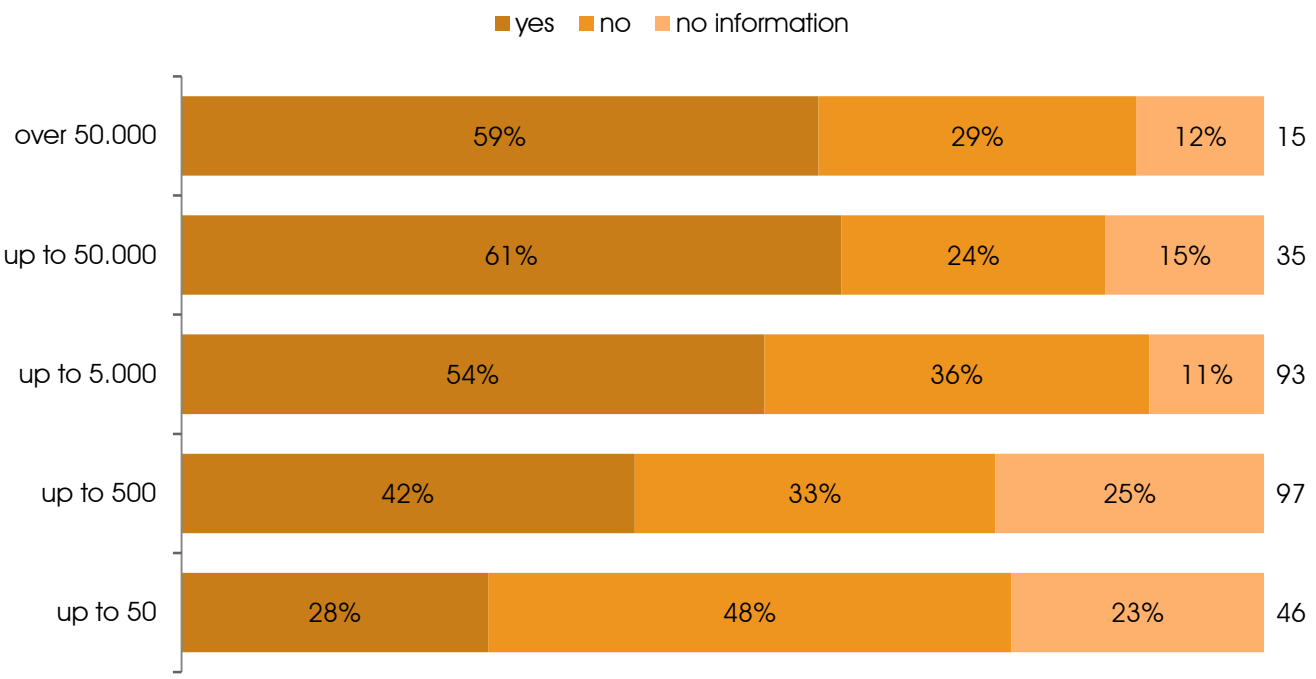
Opinions of data privacy officers by company size:



11. "Do you welcome registration by name of data privacy officers with the regulatory authority?"

The obligation to register the names of data privacy officers with the regulator authority is welcomed by an average of 56% of the survey participants. Agreement is lowest among data privacy officers from small companies with under 50 employees at 28%.

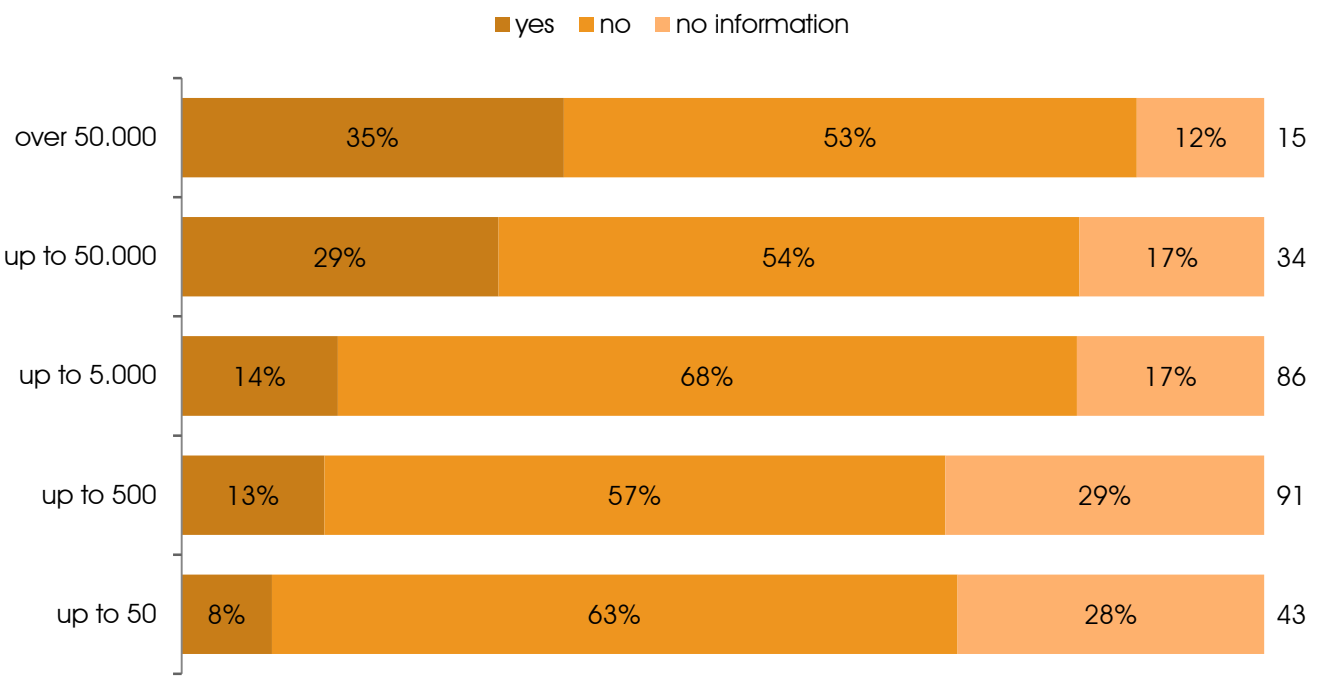
Opinions of data privacy officers by company size:



12. "Do you believe that the new EU data privacy regulation will make your work as a data privacy officer easier?"

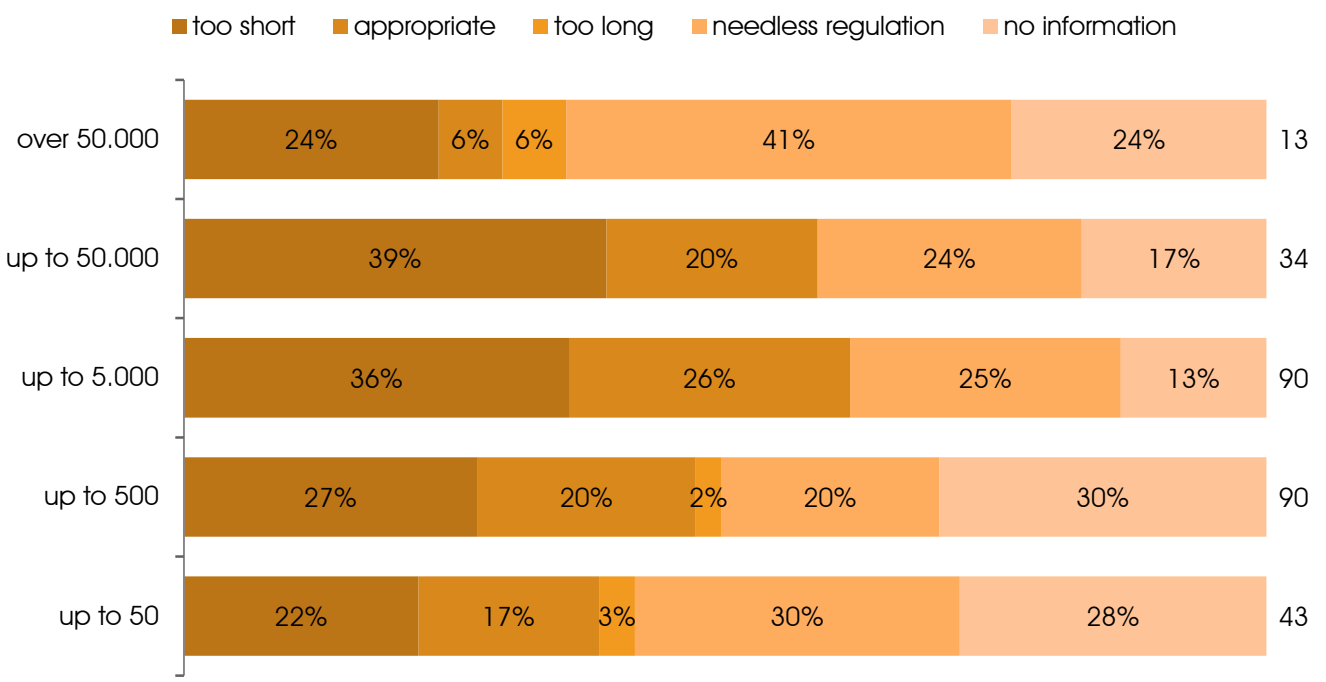
Only 20.3% of participating data privacy officers expect the new EU general data privacy regulation to make their job easier.

Opinions of data privacy officers by company size:



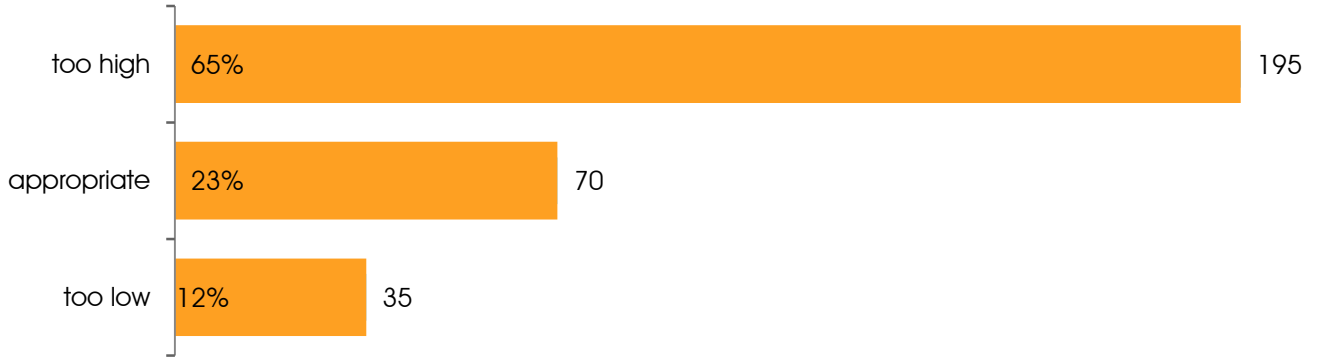
13. "What is your view of the obligation to register data privacy violations within 24 hours?"

Opinions of data privacy officers by company size:



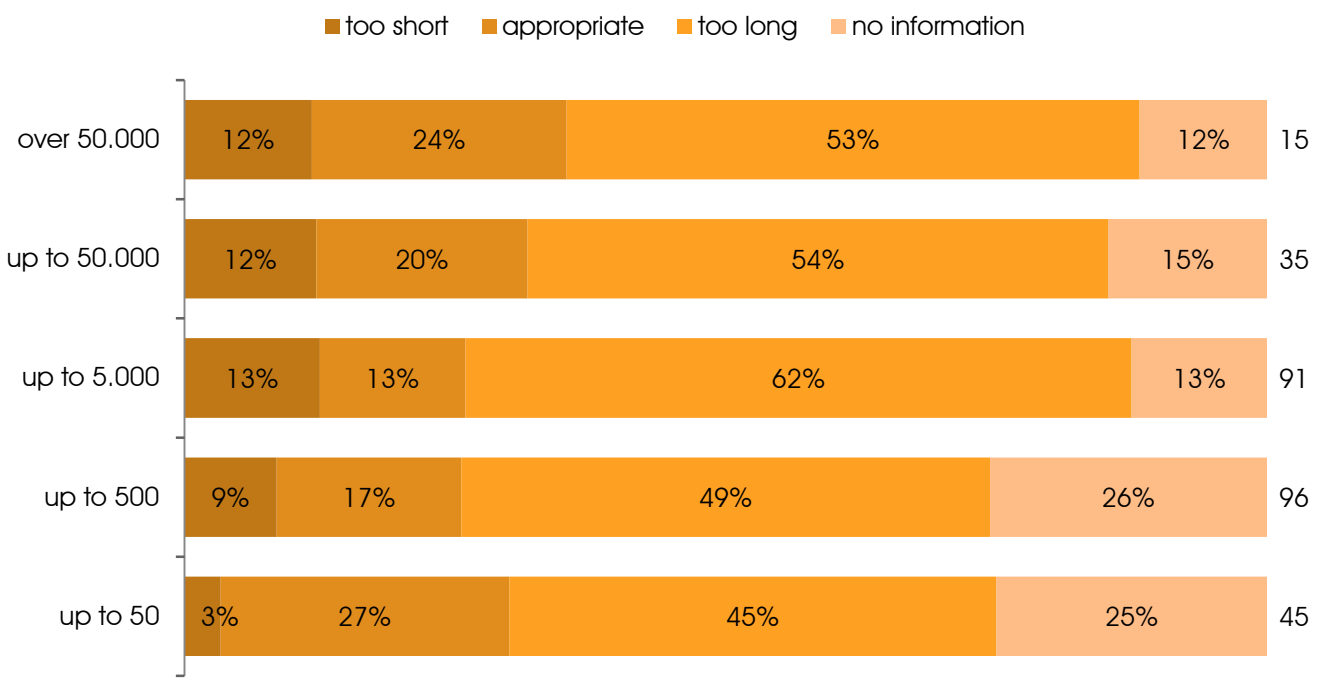
The proposed 24-hour period for registering data privacy violations is considered by 38.4% of the questioned data privacy officers to be too short, 26.4% to be appropriate and by 33% as superfluous. Six data privacy officers nevertheless consider this period to be too long.

14. "What is your view of the proposed threshold for appointing a data privacy officer as a company size of over 250 employees?"



65% of the data privacy officers questioned consider the selected threshold for appointment of a data privacy officer in companies of over 250 employees as too high, 23.2% as appropriate and 11.6% as still too low.

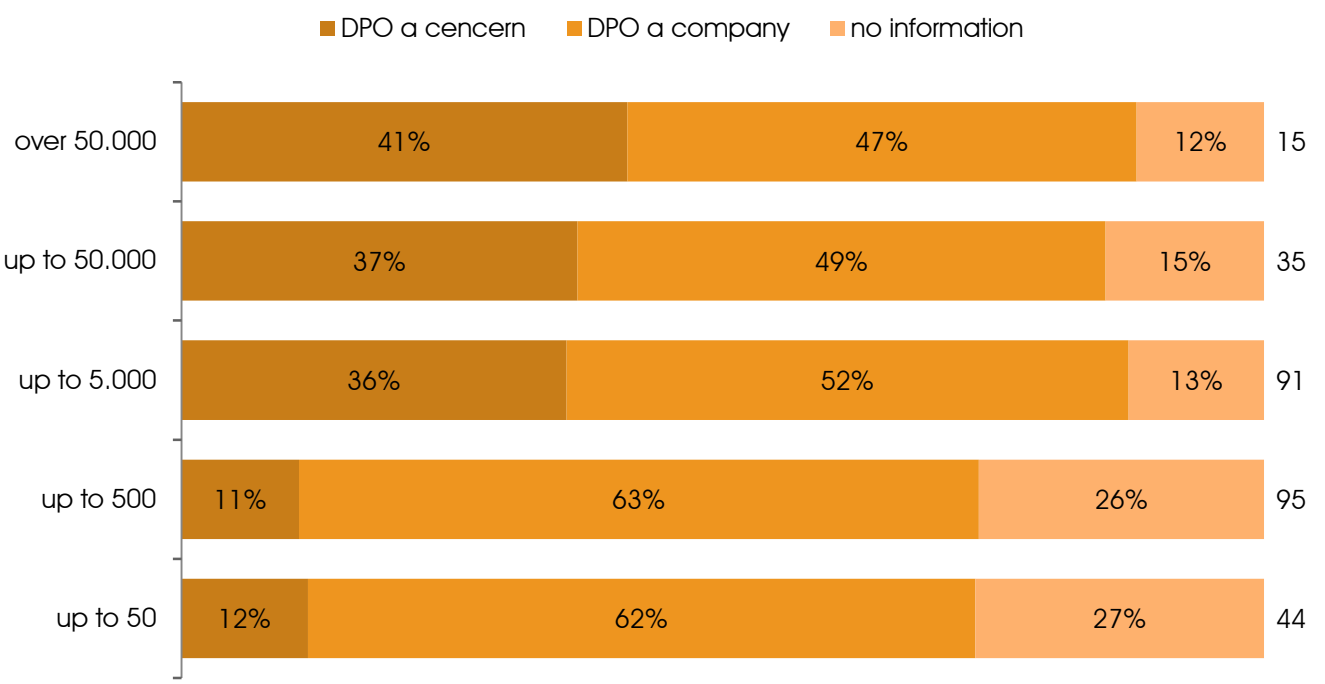
Opinions of data privacy officers by company size:



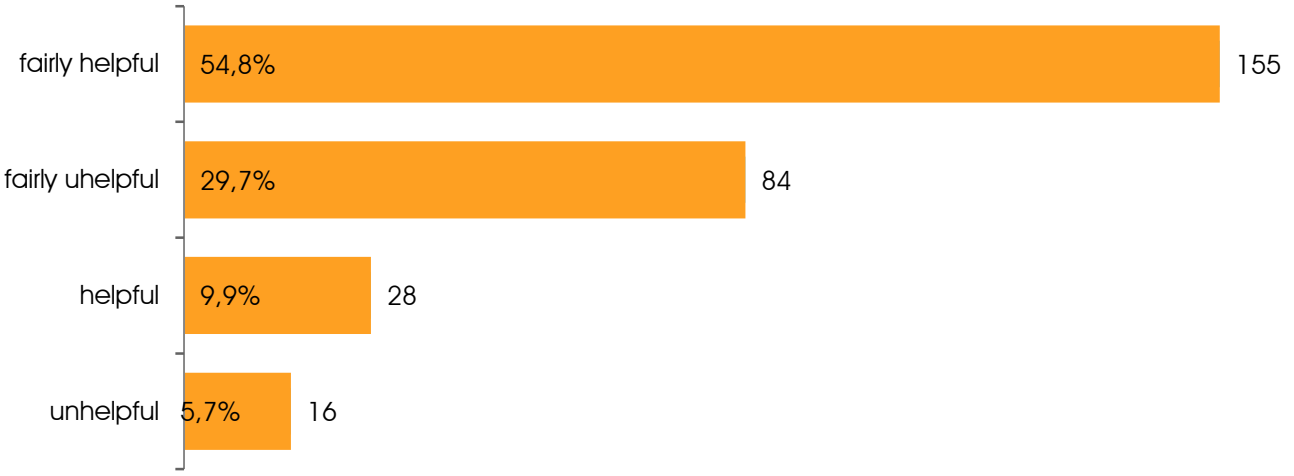
15. "Is one data privacy officer enough in a corporation, or should each member company also have its own officer?"

29.5% of participants in the survey consider that one data privacy officer per corporation is sufficient; the substantial majority, however, see it differently. The data privacy officers of large companies consistently see it more positively. On average 30% of data privacy officers in companies with over 500 to over 50,000 employees prefer a single data privacy officer per corporation.

Opinions of data privacy officers by company size:

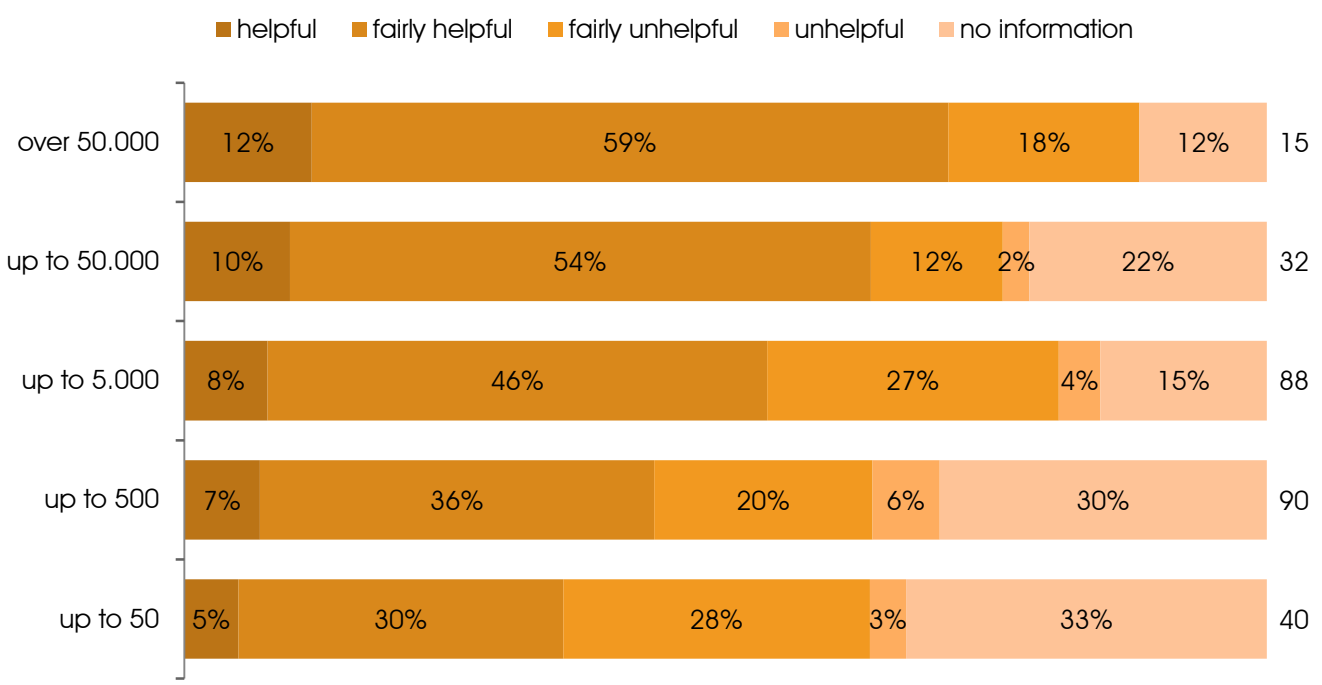


16. "What is your view of the risk impact assessment that is expected to be mandatory in future?"

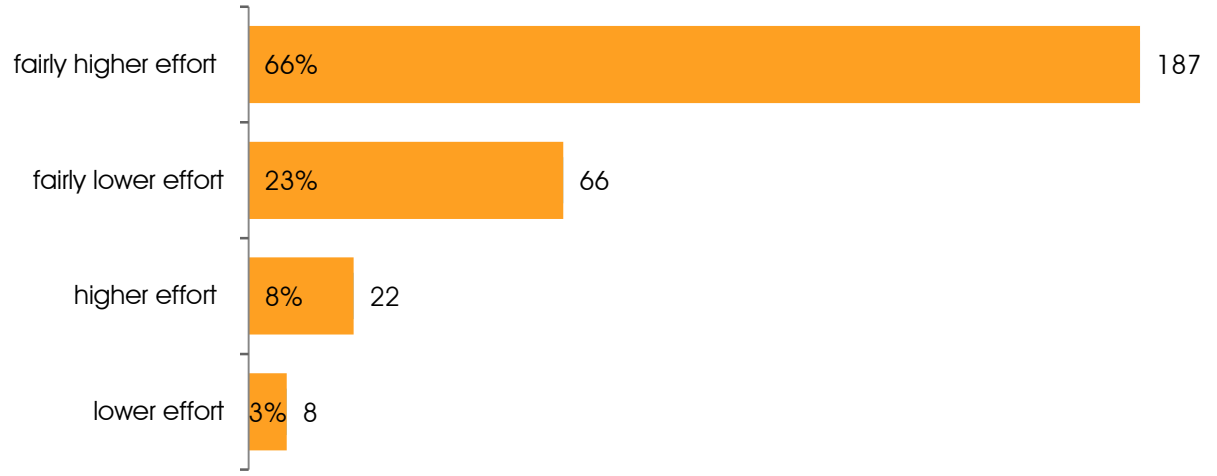


Article 33 of the Commission's draft obliges the controller and the party contracted by the controller for processing, before any processing commences that may, on account of their nature, scope or purposes, may present specific risks to the rights and freedoms of data subjects, to carry out a data protection impact assessment. In German data protection law a risk assessment is already known as a prior check (Vorabkontrolle), although the content of this may not be exactly the same. 64.7% of the data privacy officers questioned consider the proposed risk impact assessment to be "helpful" or "fairly helpful".

Opinions of data privacy officers by company size:

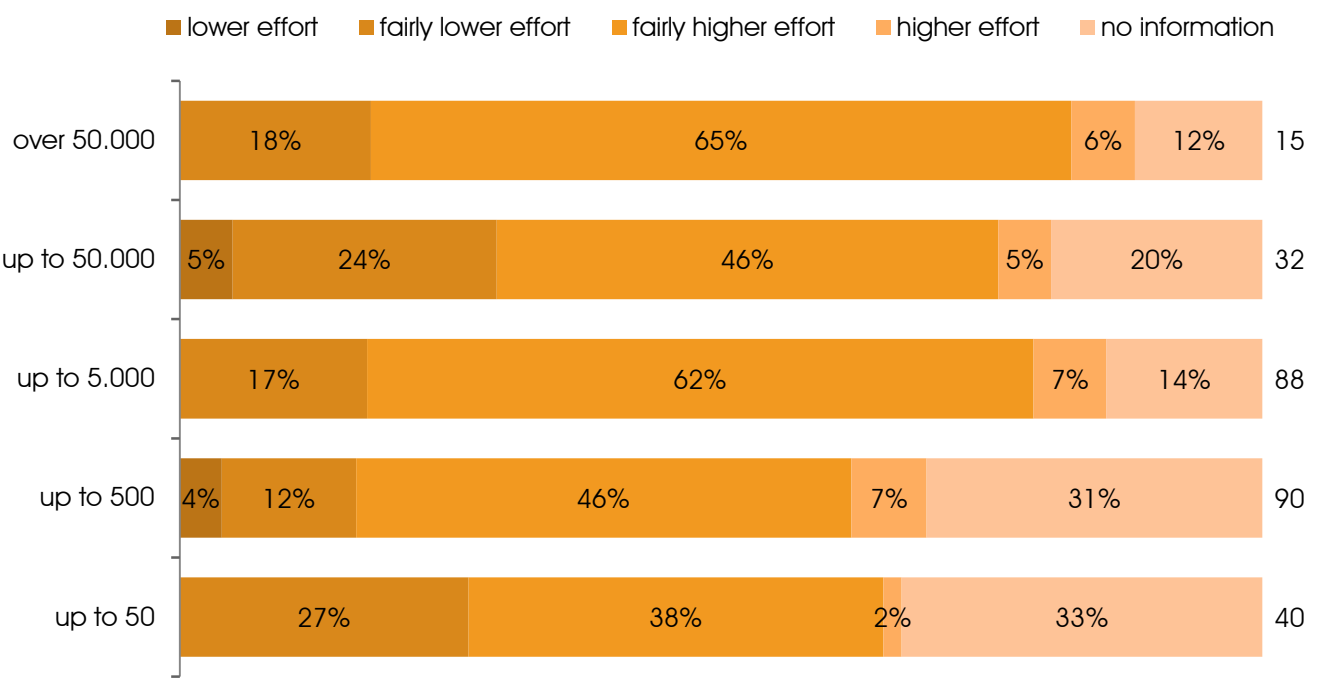


17. "In your view will the risk impact assessment mean additional expenditure for the company?"



Despite the work involved with the impact assessment, 26.4% of the data privacy officers questioned consider the extra expenditure by the company to be "low" or "fairly low"; 73.6% consider it "high" or "fairly high".

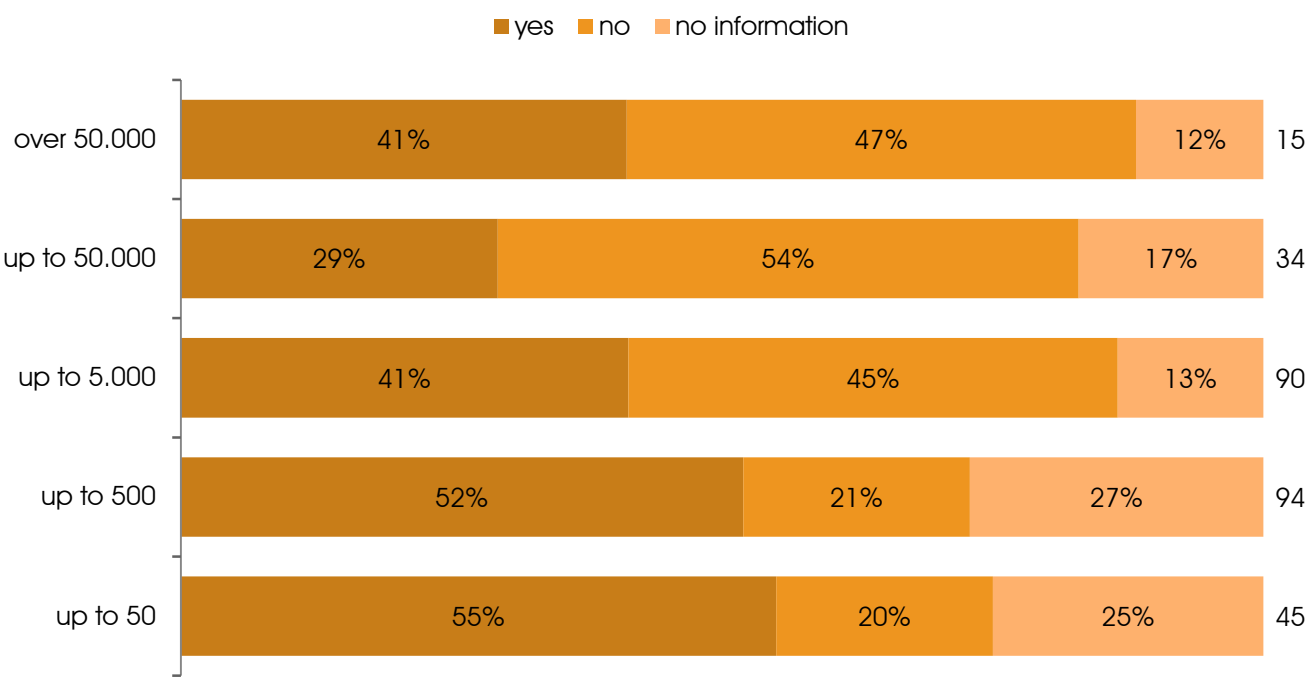
Opinions of data privacy officers by company size:



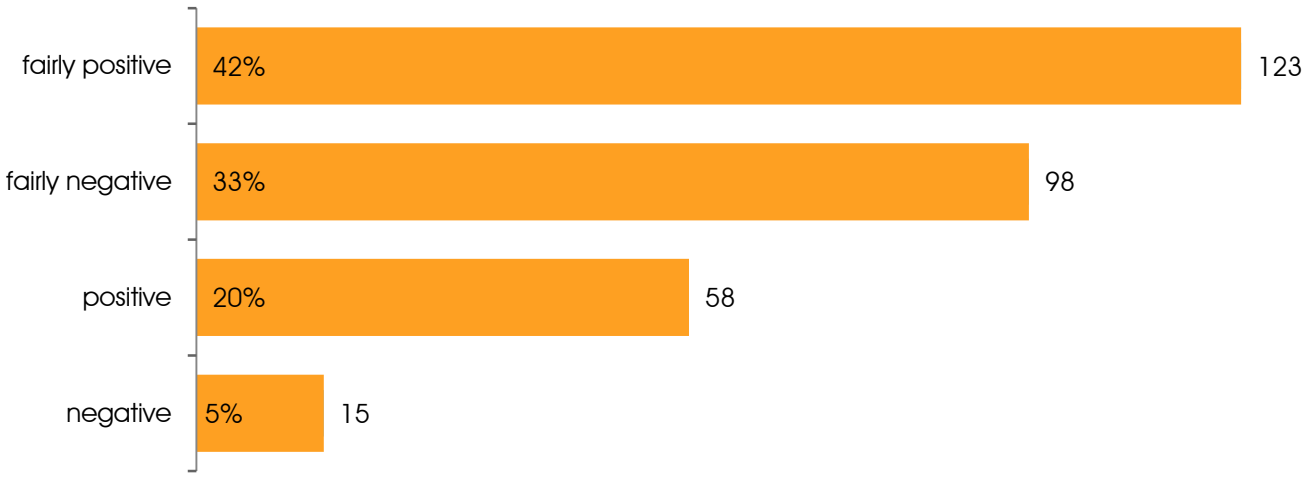
18. "Is there already something like a risk assessment in your company?"

41.6% of the data privacy officers questioned have previous experience with risk impact assessments.

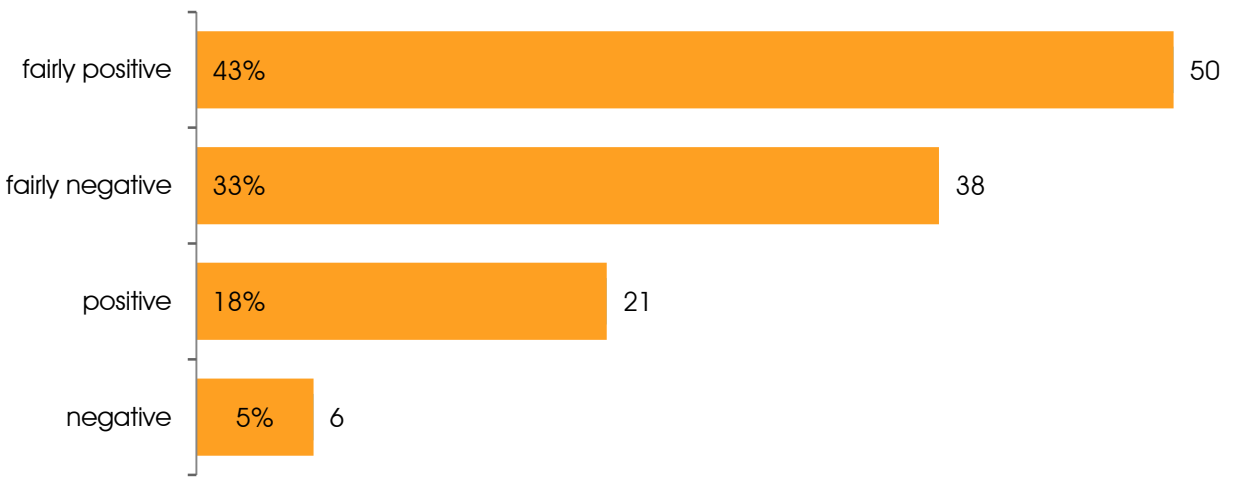
Response of data privacy officers by company size:



19. "Under the draft EU data protection regulation, there should in future be only one competent regulatory authority in European corporations. How do you see this?"

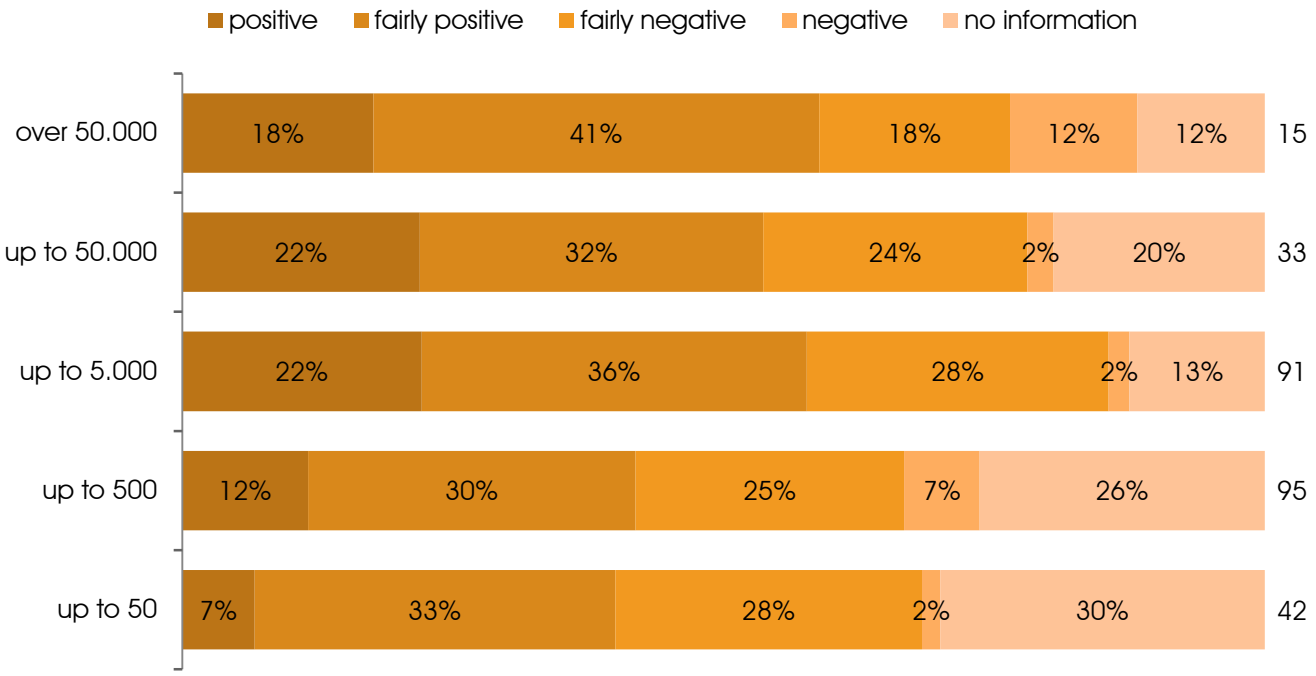


Opinions excluding those of corporate data privacy officers:

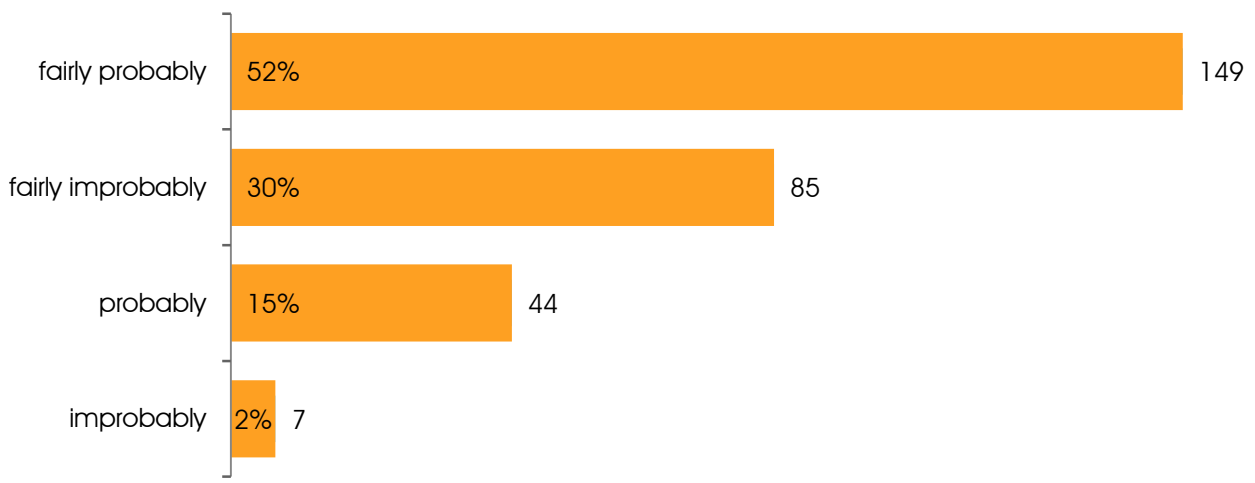


The proposed introduction of only one competent regulatory authority for companies operating throughout Europe (a "one-stop authority") is considered by 61.8% of respondents as "positive" or "fairly positive". There is no significant difference in the appraisal by the corporate data privacy officers within the respondents.

Opinions of data privacy officers by company size:

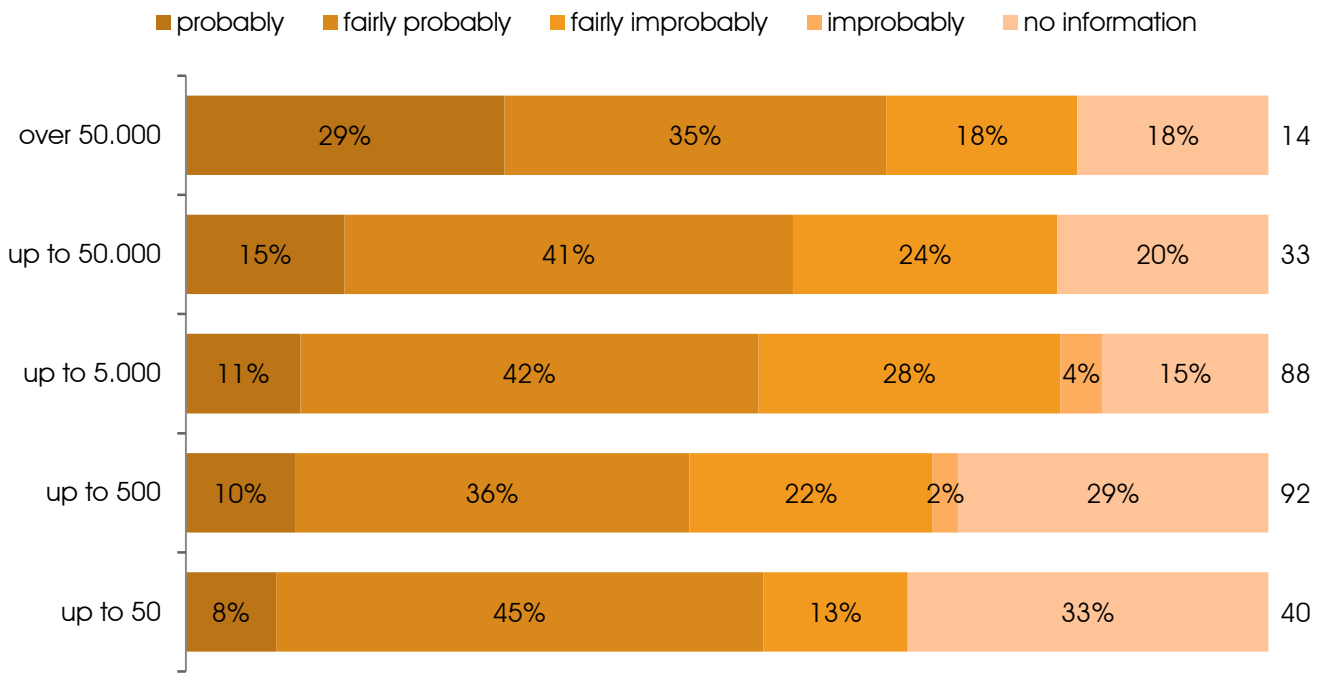


20. "How probable do you consider it to be that under these regulations a higher level of work in the processing of data subject requests will fall onto subsidiaries in other member states?"

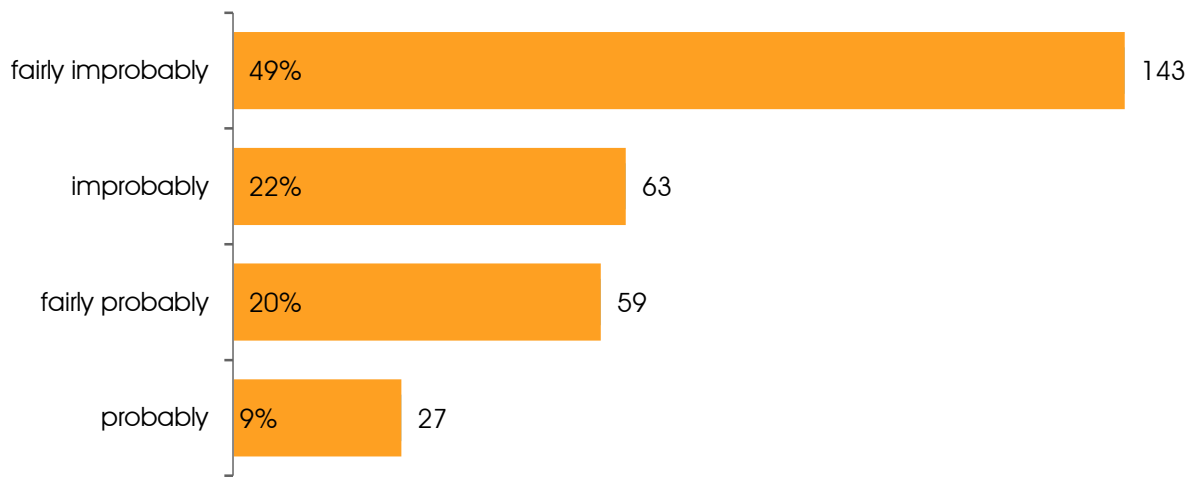


69.4% of the data privacy officers questioned expect a higher level of work to be demanded of data privacy officers in the event of complaints.

Opinions of data privacy officers by company size:

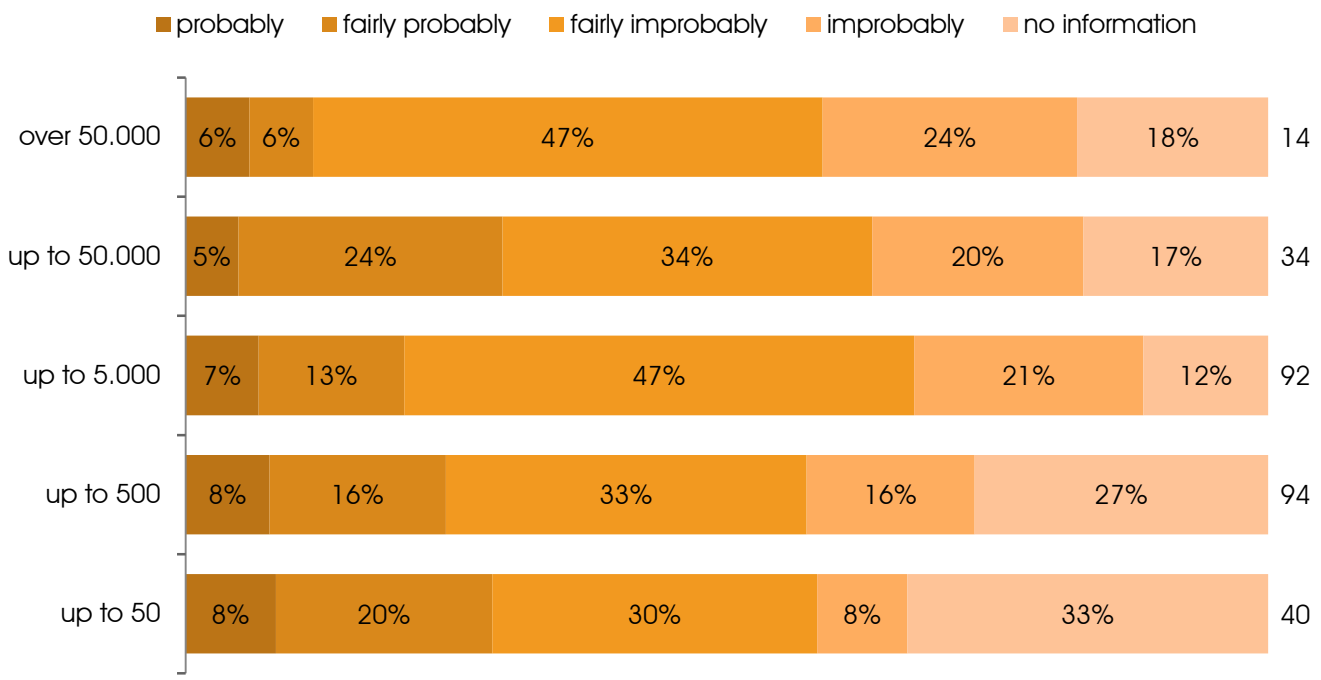


21. "How probable do you think it is that these regulations will influence the choice of headquarters for companies?"



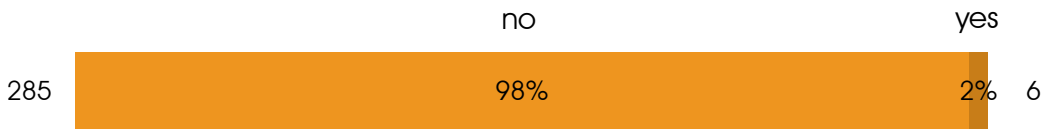
The fear that the competent data protection regulatory authority could have an influence through its activities on a company's choice of head office location within Europe, resulting in a "race to the bottom", was shared by 33% of the data privacy officers questioned. A clear majority of 77% of the data privacy officers however regard this fear as "fairly improbable" or "probably not".

Opinions of data privacy officers by company size:



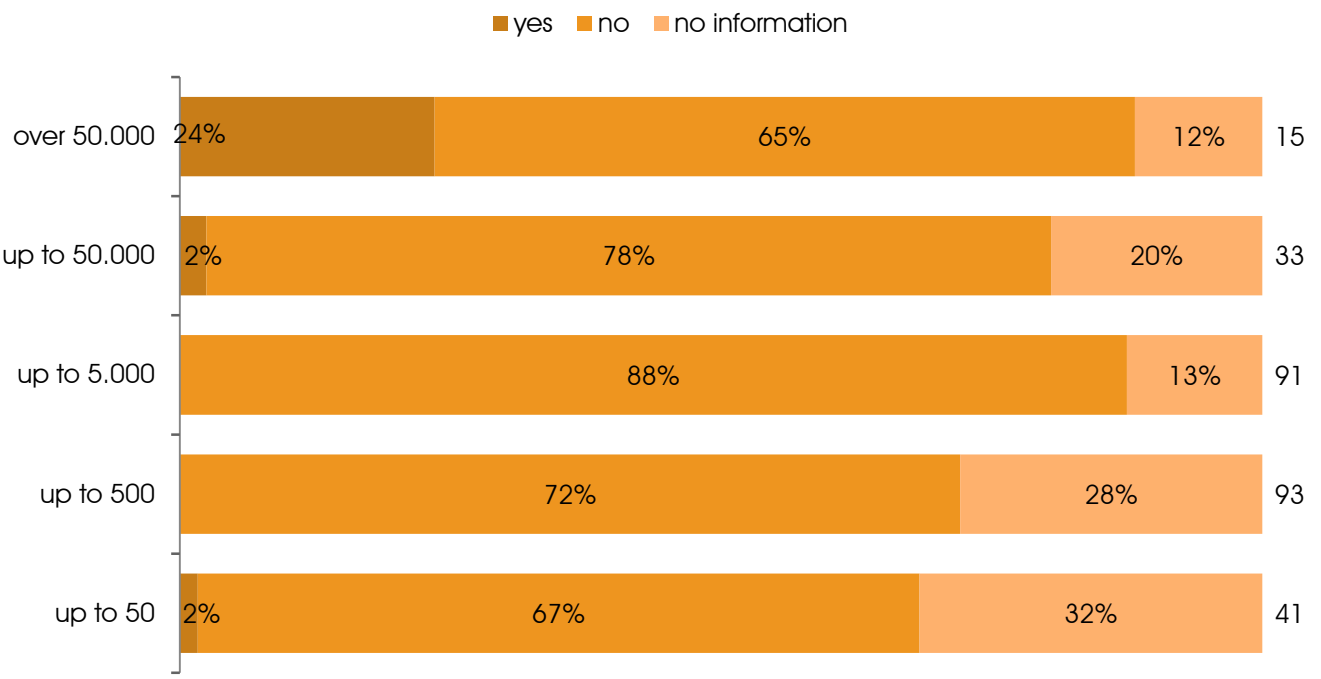
The high proportion of undecided respondents from companies with under 500 employees demonstrates that it is mainly data privacy officers from large companies that have engaged with this question. In their basic statement, however, the practitioners are unanimous: they do not fear that supervisory practice will influence a company's choice of domicile. The statement is particularly clear among data privacy officers in companies with over 50,000 employees: here only 12% of participants consider such an influence to be "fairly probable" or "probable".

22. "Does your company already have binding corporate rules authorized by the regulatory authority?"

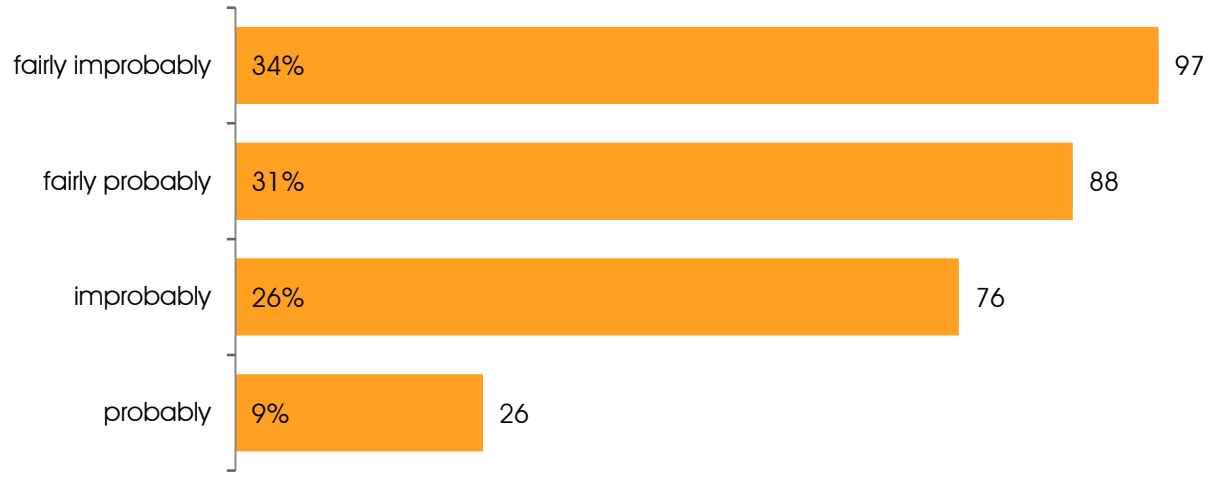


Under section 4c para 2 BDSG the competent regulatory authority can authorize individual cross-border data transfer processes outside Europe and secure third countries if the company has enacted generally binding regulations for protection of the data. So far 2% of the data privacy officers questioned have experience of this procedure. According to European Commission statistics, in Germany only the binding corporate rules of a corporation have been definitively approved.

Opinions of data privacy officers by company size:

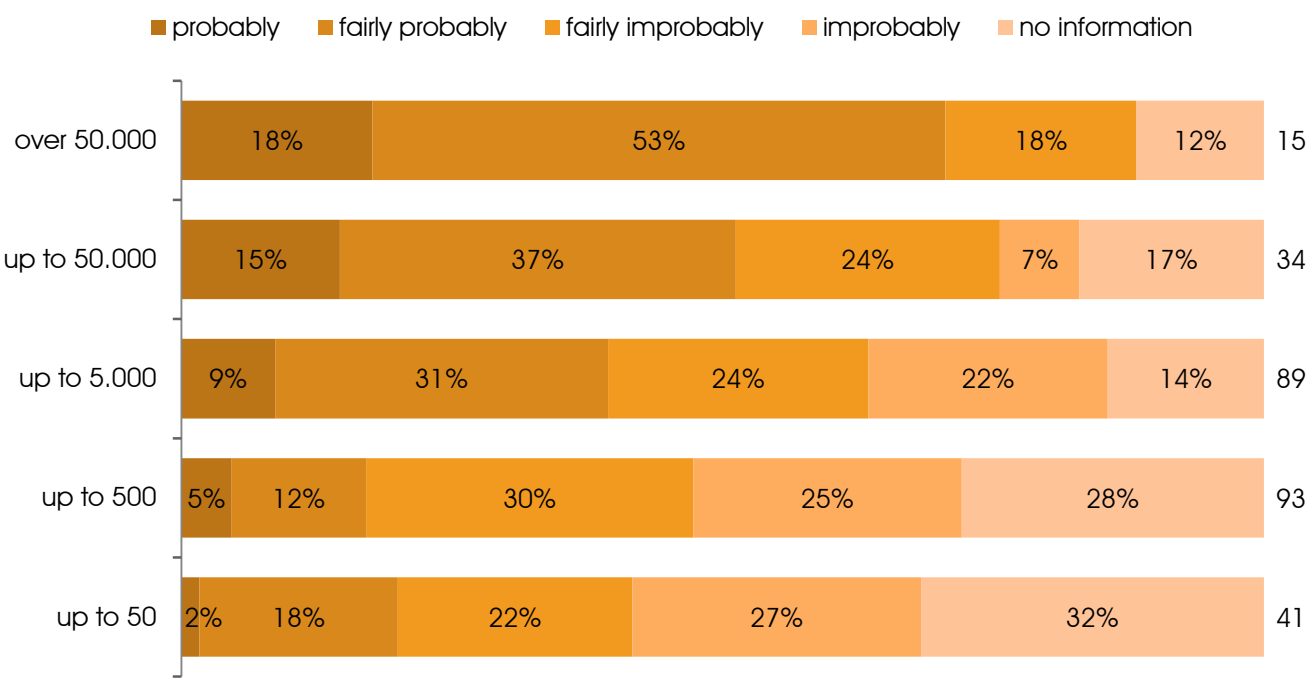


23. "How probable do you think it is that your company will make use of binding corporate rules (BCR) in future?"

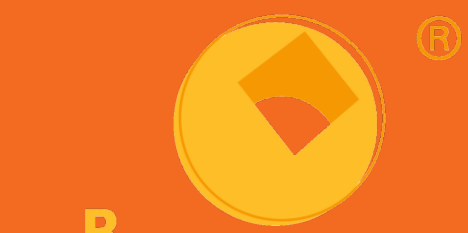


39.7% of participating data privacy officers consider it probable or fairly probable that their company will make use in future of the possibility of binding corporate rules (BCR). This interest is particularly strong among large companies with over 5000 employees.

Opinions of data privacy officers by company size:



Article 43 of the draft general data protection regulation makes data transfers on the basis of binding internal corporate rules permissible if a regulatory authority has authorized binding internal corporate rules in accordance with the consistency mechanism described in article 58. Despite the immense expenditure required for such a procedure, the practitioners of the large companies in particular consider it probable that their company will make use of this regulation in future.
For practitioners in small and medium-sized companies, this appears predominantly unlikely.



2B Advice®

THE PRIVACY BENCHMARK

Berlin | Bonn | Brezno | Munich | New York

2B Advice GmbH

Wilhelmstraße 40-42 | 53111 Bonn

Fon_+49 228 926165-100

Fax_+49 228 926165-109

www.2b-advice.com