Making data protection practicable and legally certain

Chamber of Commerce and Industry Survey on the GDPR

#GemeinsamWirtschaftStärken

DIHK Deutsche Industrie- und Handelskammer

IHK Deutsche Industrie- und Handelskammern

Table of contents

Imprint

Contact at the DIHK:

Kei-Lin Ting-Winarto
ting-winarto.kei-lin@dihk.de
+49 30 20308- 2717

Publisher and copyright

© German Chamber of Commerce and Industry
Postal address: 11052 Berlin | Street address: Breite Straße 29 | Berlin-Mitte
Phone +49 30 20308-0 | Fax + 49 30 20308-1000

DIHK Brussels
Representation of the German Chamber of Commerce and Industry at the European Union
19 A-D, Avenue des Arts | B-1000 Bruxelles
Phone : +32 2 286-1611 | Fax +32 2 286-1605

@ *info@dihk.de*
www.dihk.de

Graphics:
Sven Ehling, DIHK

Picture credits:
© Getty Images / Traitov

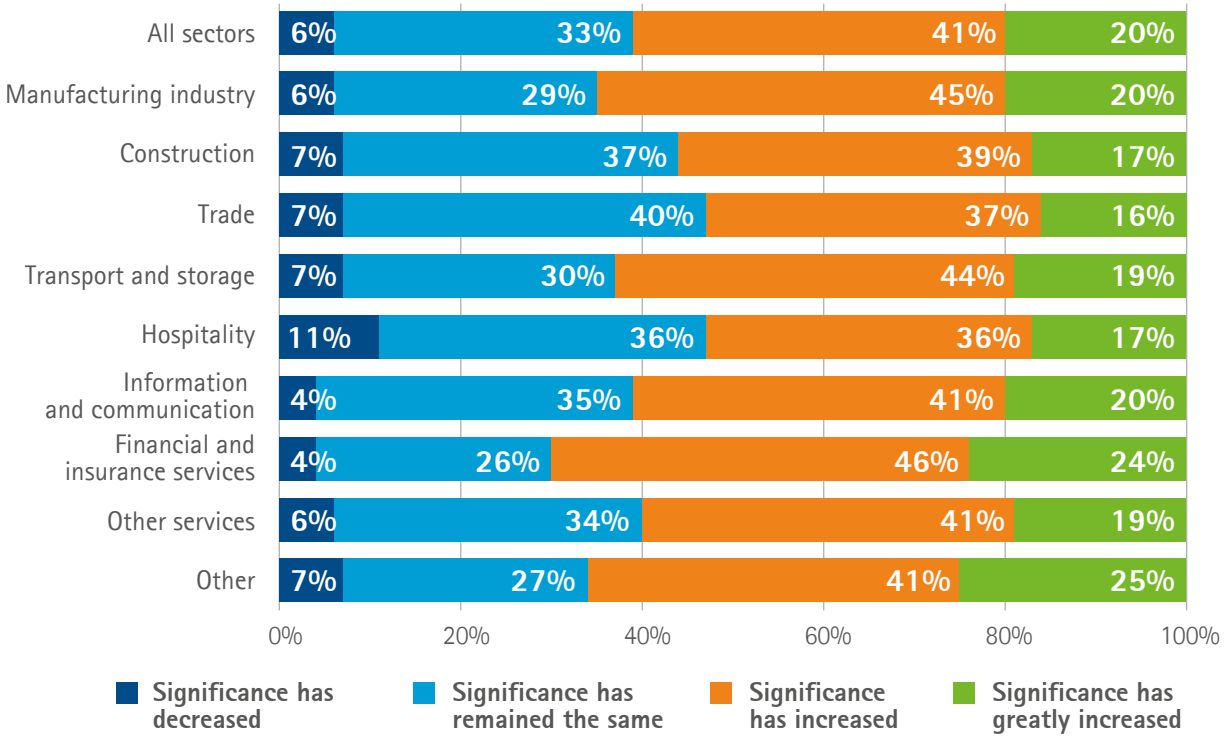
Situation as of:
January 2024

Evaluation of the GDPR

The General Data Protection Regulation (GDPR) provides in its Article 97 that by 25 May 2020 and every four years thereafter, the Commission must submit a report on the evaluation and review of the regulation. With support from the Chambers of Commerce and Industry (IHKs), the German Chamber of Commerce and Industry (DIHK) has used the occasion of the GDPR evaluation planned for the second quarter of 2024 to conduct a broad survey of companies of all sizes in all sectors. More than 4,900 companies took part in this survey. The findings are taken up in the positions framed in this paper, as drawn up regularly by the DIHK in safeguarding the overall interest of the business sector (section 1, section 10a of the Act on the Provisional Settlement of the Legislation Governing the Chambers of Commerce and Industry, IHK Act (Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern, IHKG).

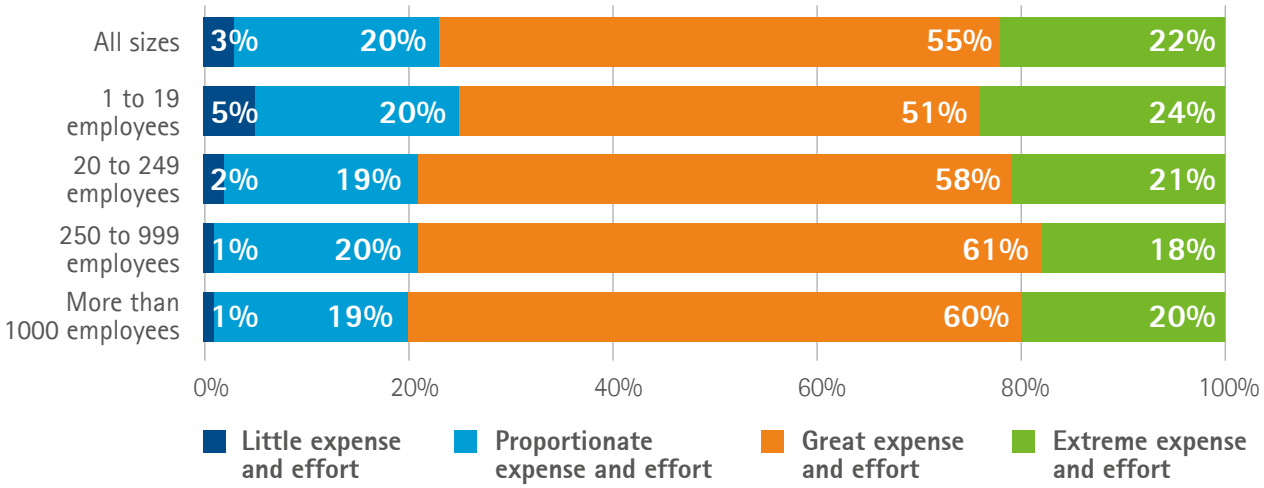
The entry into force of the GDPR provided an occasion for companies to review, optimise and professionalise their own processes and structures. For a majority of companies across all sectors (61 percent), the subject of data protection has gained significance in the last three years.

How has the significance of the subject of data protection changed for your company in the last three years, for example, due to the threat of cyber crime?



By means of the GDPR, the EU is endeavouring to be a trailblazer and even a global model for modern data protection legislation and a correspondingly high level of data protection. Many companies come up against their limits when implementing the ambitious policy specifications, however. Nearly four out of five companies (77 percent) stated that implementing the GDPR requires great or extreme expense and effort. In developing data protection legislation within Europe and at international level, it is essential to consider not only ideals, but also the practicability and viability of data protection provisions.

How do companies judge the expense and effort involved in implementing the GDPR?



Key findings

- **Bureaucracy:** Even six years after the GDPR entered into force, its implementation involves "great to extreme" expense and effort for more than three quarters of companies – across all company sizes. The GDPR remains a key driver of red tape. A risk-based approach, guided by company size and the type of data processing, could bring relief.

- **Legal uncertainty:** A majority of companies with experience of the GDPR in other EU Member States experience the data protection authorities there as less strict then the German authorities. Approximately half of companies report of diverging views of legal supervisory bodies, even within Germany itself. On the positive side, more than half of companies regard contacts with the authorities as satisfactory when they are based on companies' own initiative.

- **Liability risk:** The great majority of companies see unclarities and risks regarding possible legal consequences of infringements of the GDPR (69 percent). Damages in particular still remain unclarified. Class actions under the new Consumer Rights Enforcement Act (Verbraucherrechtedurchsetzungsgesetz, VDuG) increase the risk still further.

- **International exchange:** Globally networked economic relations are of fundamental significance for companies in Germany and Europe. To maintain them, international data transfer is essential. The overwhelming majority of companies that see data protection challenges in international data transfer cannot themselves independently judge the level of data protection in third countries, however (88 percent). Since there are often no adequacy decisions by the European Commission on the level of protection or these are not permanent, as in the case of the USA, there are liability risks at the expense of the companies.

- **Data economy and data protection:** The majority of companies that criticise legal unclarities (59 percent) also identified considerable unclarities between new data economy provisions (such as the Data Act) and the GDPR. For Europe to play a leading role in the future-oriented issues of AI and data economy, legal certainty is needed here.

Requirements

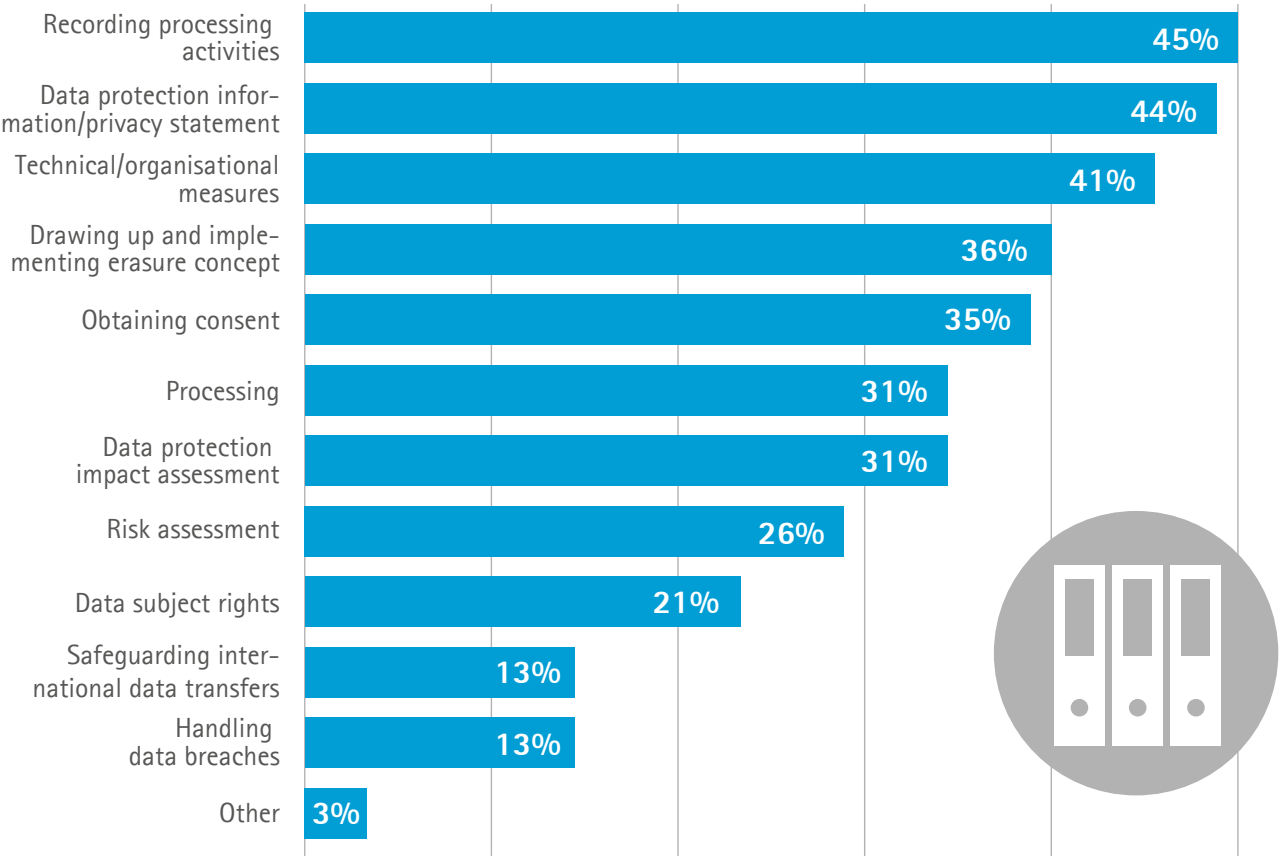
The following aspects should be taken into account by the European Commission in evaluating the GDPR – also in the context of the survey results:

Relieving the burden, particularly for SMEs

Relief is needed regarding documentation, information and burden of proof obligations. The risk-based approach should be given greater consideration here. Recital 13 of the GDPR, which recognises the special situation of small and medium-sized enterprises, has been of little practical relevance to date. Thus, consideration should now be given to this specific situation in the regulation itself.

Note:
The GDPR evaluation should be taken as an occasion to adapt provisions, and in particular to take greater account of companies' practical reality. Improvements should be made, providing clear relief or exceptions for SMEs, as already laid out in the GDPR. Implementation to date has shown that the high demands placed on companies cause great difficulty. Even nearly six years after the GDPR became applicable, 77 percent of companies state that implementing it involves great or extreme expense and effort. Nearly one in four companies with up to 19 employees (24 percent) referred to the expense and effort as extreme. The documentation, information and burden of proof obligations are proving to be too bureaucratic for many companies. In the case of processing involving small amounts of data or low to normal risk, the extensive documentation, information and burden of proof obligations are disproportionate and not commensurate with the risk.

Which obligations under the GDPR involve the greatest expense and effort for you? (up to four answers possible)



Companies expend the greatest expense and effort in recording their processing activities (45 percent), providing data protection information (44 percent) and taking technical and organisational measures (41 percent) that have to be updated on an ongoing basis. The risk-based approach should apply here and the special situation of SMEs should also be taken into account. The one-size-fits-all approach, to which the supervisory authorities adhere too closely, is not in line with corporate realities and also does not improve data protection. It is not proportionate for all obligations to apply, regardless of company size or business purpose.

Specific examples of relief in this context:

- Waiver of information obligation in the B2B sector
- No record of processing activity for normal-risk processing
- Introduction of a checklist laying down precisely in binding form when the obligation to record processing activity is waived for SMEs. The exception for SMEs provided for in Article 30 (5) of the GDPR is rarely applied in practice
- The provisions for data processing agreements should be adjusted according to the risk and be less bureaucratic.

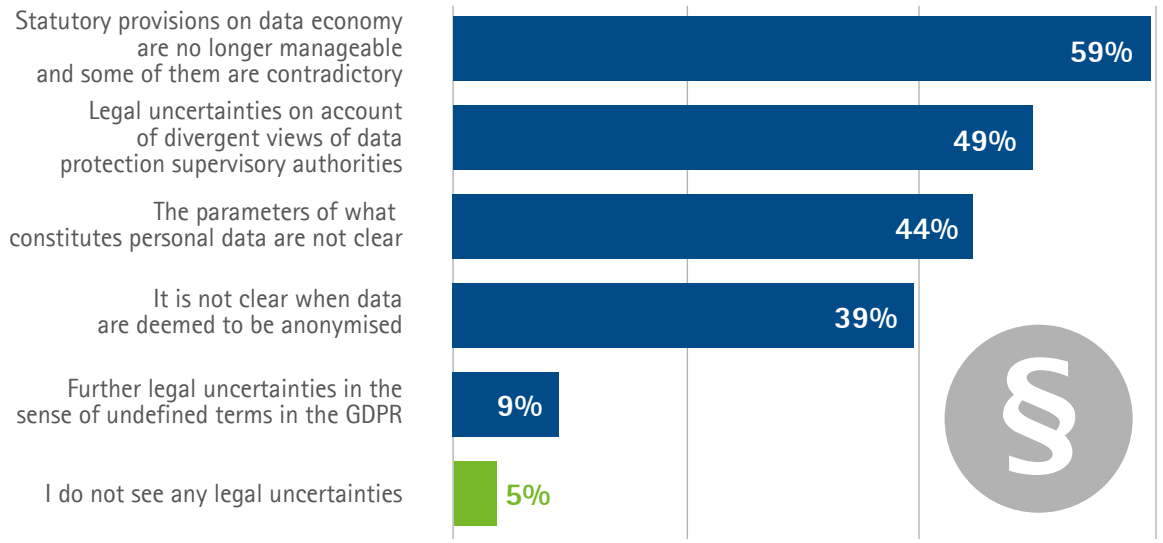
Achieving greater legal certainty

Legal certainty and clarity must be achieved directly within the GDPR itself and should not be left to lengthy and protracted official or court proceedings. Furthermore, faster and more reliable adequacy decisions for international data transfers are needed. In the absence of an adequacy decision, standardised information on the level of data protection in third countries is needed, to be provided by the European Commission/the supervisory authorities.

Note:
In practice, the many undefined legal terms deliberately introduced by the EU as a compromise lead to great uncertainty among companies. Only 5 percent of companies stated that they see no legal uncertainties in the GDPR[1] . Legal uncertainties exist in particular on account of divergent views of data protection supervisory authorities (49 percent). Another frequently-cited impediment is that the parameters of what constitutes personal data are not clear (44 percent). At the same time, it is unclear for many companies when data are deemed to be anonymised (39 percent). These legal uncertainties slow down companies in pursing new business models and innovations.

[1] 17 percent of the companies taking part in the survey were unable to answer the question "Where do you see legal uncertainties in the GDPR?" They were not included in the evaluation.

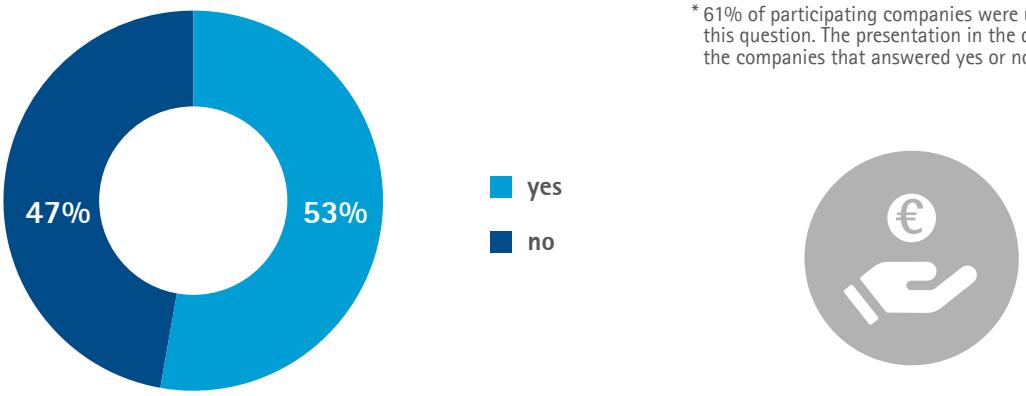
Where do you see legal uncertainties in the GDPR? (multiple answers possible)*



*17% of participating companies were unable to answer this question. They are not included in the presentation in the diagram.

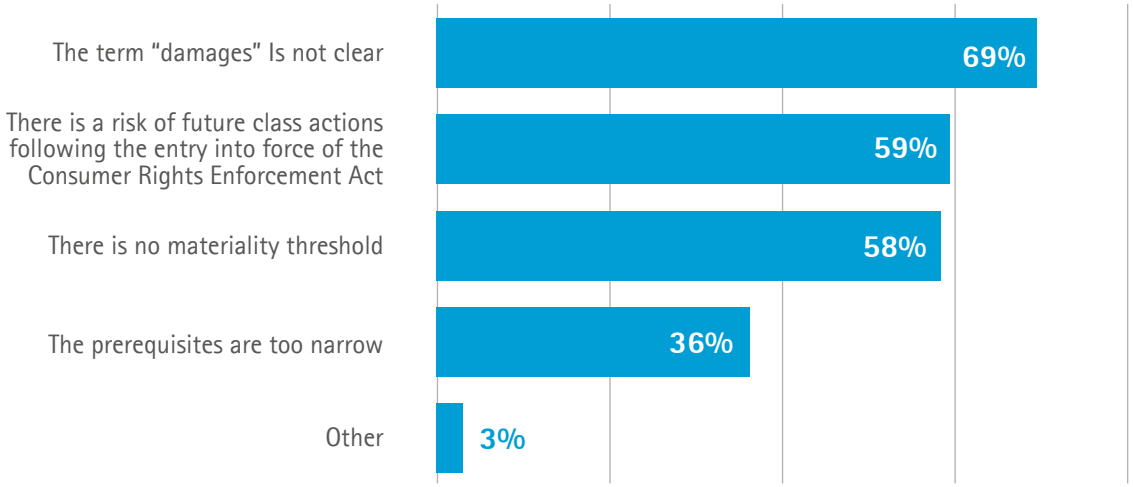
There are also great uncertainties in connection with the law of damages. Despite the case-law of the Court of Justice of the European Union, which has meanwhile clarified some questions, it remains unclear in practice under what conditions and to what extent damages can be claimed in case of infringements of the GDPR. This leads to incalculable risks that place a burden on and impede business.

In your view, are there any problems with damages under Article 82 of the GDPR (for example in connection with warning letters, data leaks etc.)? *



* 61% of participating companies were unable to answer this question. The presentation in the diagram includes the companies that answered yes or no.

What problems relating to damages under Article 82 of the GDPR do you see? (multiple answers possible)



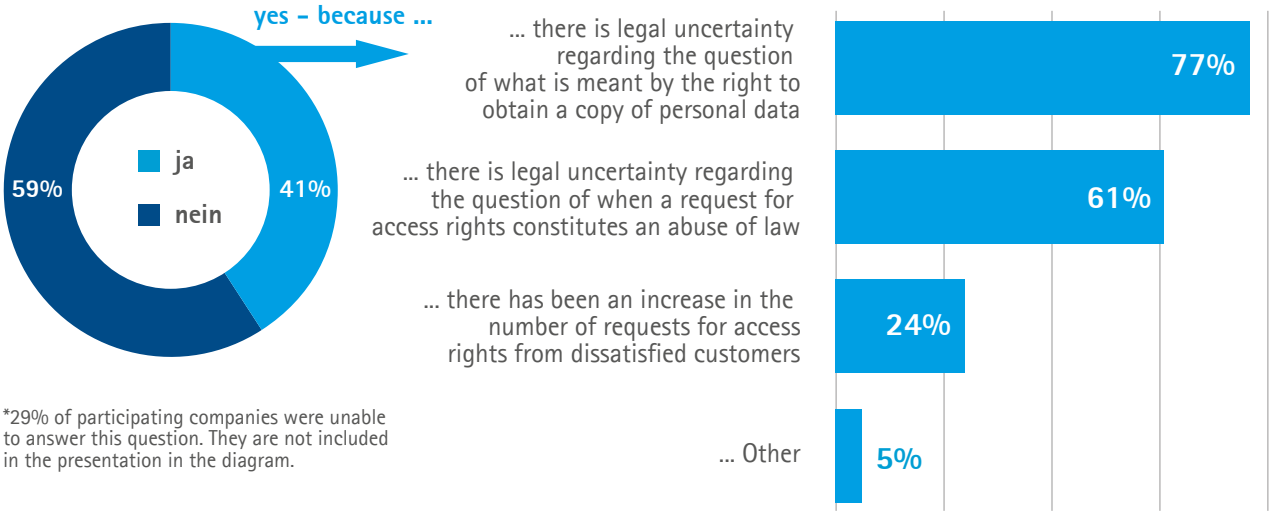
More than half of companies (53 percent) stated that in their view, there are problems relating to damages under Article 82 of the GDPR[2] . Of these, 69 percent of companies stated that the term "damages" is not clearly defined. Due to the ongoing legal uncertainty, there is the risk of a situation where strategic innovation potential is being impeded, particularly in connection with class actions. 59 percent of companies that see problems with damages see a risk of future class actions following entry into force of the Consumer Rights Enforcement Act. In this connection, it should therefore be clearly specified

[2] 61 percent of the participating companies were unable to answer this question. They were not taken into account in the evaluation.

under what – only strict - conditions leave may be granted to bring a class action. In the view of the broad business sector, the significance of data protection law on its own cannot in itself justify such leave to bring class action.

The lack of a materiality threshold for damages is also seen as a problem by many companies (58 percent).

Do you have difficulty in responding to requests for access rights under Article 15? (Under Article 15 of the GDPR, data subjects have the right to obtain information on which of their personal data is being processed in your company). (multiple answers possible)*



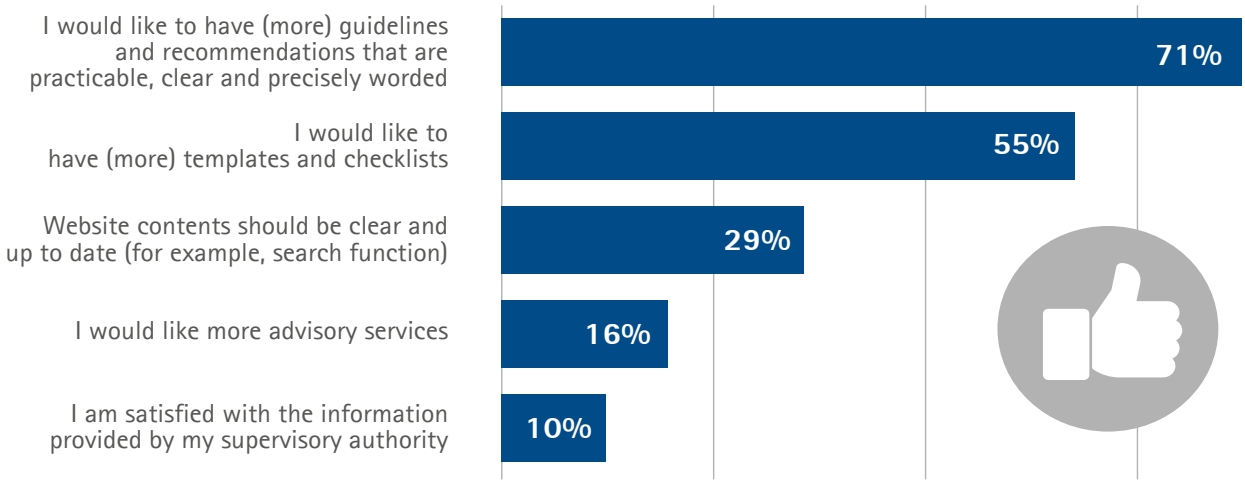
*29% of participating companies were unable to answer this question. They are not included in the presentation in the diagram.

Moreover, many companies have difficulty in answering questions on access rights. 45 percent of companies stating that they had difficulty in responding to requests for access rights criticised the fact that it was not clear what had to be provided in the case of a "right to request a copy of the data"[3] . Thus, the question arose, for example, as to whether data have to be provided which the person requesting the information already has. The person is already aware of this information and it contradicts the intent and purpose of access rights to be required to hand out this information again as a copy.

There is also great legal uncertainty concerning the question of when a data subject's request for access rights is deemed to be an abuse of law (61 percent).

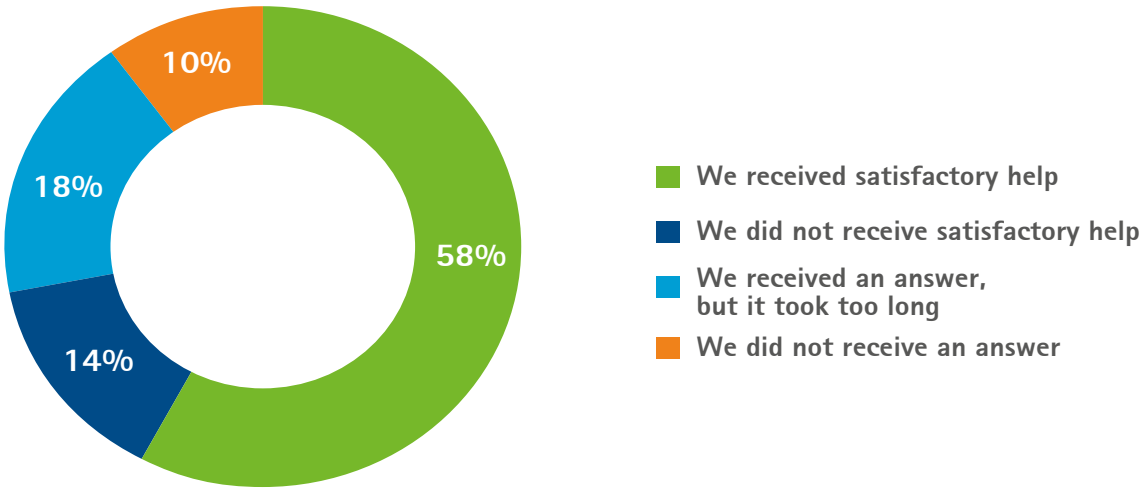
[3] 29% of the participating companies were unable to answer this question. They were not included in the evaluation.

In what ways should the data protection authority improve?



To counter legal uncertainty, textual clarification is needed in the GDPR itself, or at least in its recitals. This would take a necessary step towards the urgently required standardisation. Templates and checklists as well as guidelines and recommendations that are practical and provide for entrepreneurial room for manoeuvre can then reduce remaining legal uncertainties. Also the majority of companies would like to have guidelines and recommendations that are practical and clearly and precisely worded (71 percent) as well as templates and checklists (55 percent). The requirement that supervisory authorities word their statements vis-à-vis other supervisory authorities succinctly, clearly and precisely so that they are easily comprehensible should also apply here[4].

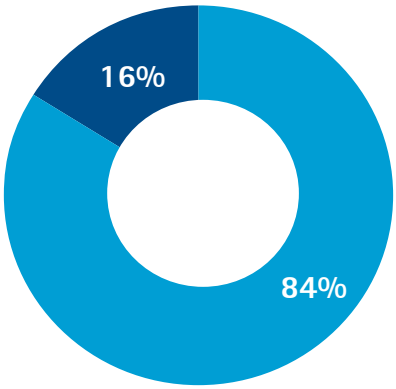
If you had contact with your data protection supervisory authority on your own initiative, how satisfied were you with that contact?



Overall, the majority of companies that had contact with their supervisory authority on their own initiative were satisfied (58 percent); conversely, that also means that 42 percent were not satisfied.

[4] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679.

Do you see challenges relating to data protection law in the international transfer of data to third countries?*

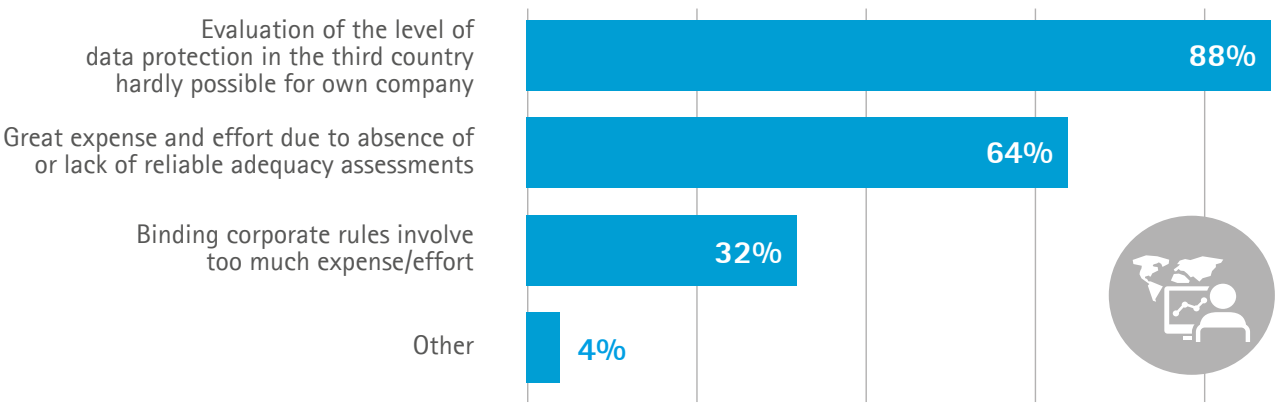


*45% of participating companies were unable to answer this question. The presentation in the diagram includes the companies that answered yes or no

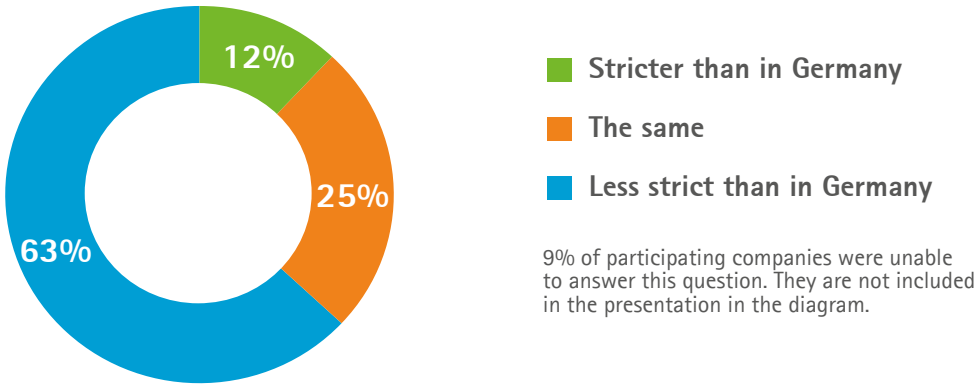
Companies continue to face a great challenge with regard to international data transfer. Globally networked business relations are of fundamental importance for people and companies in Germany and Europe. Due to global data flows, data protection rules can no longer be decided by nation states on their own; rather, transnational provisions are needed. The GDPR can only be one building block on the way to international provisions. Until there are binding international agreements, the EU must act faster than in the past, where there have been years of uncertainty, using the instrument of the adequacy decision. Moreover, decisions must be permanent and more reliable. A large majority of companies that deal with data protection challenges in international data transfer (84 percent) see data protection law challenges[5] . Of these companies, 88 percent state that it is practically impossible for them to evaluate the data protection level in the third country themselves. Therefore, the European Commission and data protection authorities should provide standardised information in a timely manner on the level of data protection in specific third countries so that individual authorities and companies do not have to establish this themselves.

[5] 45 percent of participating companies were unable to answer this question. They were not included in the evaluation.

Companies that see data protection challenges in the international data transfer to third countries specified the following challenges (multiple answers possible)



Generally speaking, were the data protection provisions, and particularly their implementation and monitoring, stricter or less strict in other EU States than in Germany?



9% of participating companies were unable to answer this question. They are not included in the presentation in the diagram.

Need for more stringent harmonisation

The objective of harmonisation and approximation of laws that the GDPR aims to achieve must be pursued more stringently.

Note:
The EU-wide application the GDPR aims to achieve has not yet materialised. In practice, the possibility of opening clauses leads to legal fragmentation, which in turn leads to different market conditions for companies within the EU. In Germany, that is particularly evident in the provisions for appointing a company data protection officer and for employee data protection. This is because a company operating in Germany, for example when appointing a data protection officer, must fulfil the requirements of the Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG) as well as those of the GDPR.

Also, a company that operates EU-wide has to adapt to different, sometimes contradictory interpretations and jurisprudence in different Member States. This leads to increased expense and effort for companies. While templates, checklists, guidelines, standard instructions and practical and solution-oriented advice may help, coordination and a consistent stance on the part of supervisory authorities remain the priority. Only 7 percent of companies taking part in the survey had any experience of data protection legislation in other EU Member States. However, the survey showed that of the companies that had had such contact with other data protection authorities in EU Member States, a majority (63 percent) perceived them to be less strict, 25 percent perceived them to be equally strict and 12 percent perceived them to be stricter.

Aligning data protection with the data economy

Data economy legislation must be consistent and coherent with the GDPR.

Note:
With regard to the data economy, a reliable legal framework is required with clear, competitive, internationally-coordinated conditions within which data processing is possible while at the same time ensuring the protection of citizens' and companies' legitimate interests. In creating the legal framework conditions for the data economy, coherence and consistency with existing provisions, for example, the GDPR, are urgently required. The phrase "the GDPR remains unaffected" used in many new EU data regulations often leads to legal uncertainty. If data economy provisions are based on the GDPR, legal uncertainties in the GDPR must first be removed. Data protection rules should not be extended beyond measure, however, as this endangers competitiveness and risks an exodus abroad, where requirements may be better met. 59 percent of the companies that saw legal uncertainties in the GDPR no longer have an overview of the statutory provisions on the data economy, some of which contradict the GDPR. Ultimately, this leads to inhibiting digitalisation and innovation in Europe.

Methodology

The nationwide survey on the GDPR was conducted with support from the 79 Chambers of Commerce and Industry (IHKs) in Germany. Approximately 4,900 companies took part in the survey between 9 and 27 October 2023. The distribution of companies' answers by company size was as follows: 46 percent of companies had up to 19 employees, 36 percent had up to 249 employees, 10 percent had up to 999 employees, 8 percent had more than 1,000 employees.

Survey

1. How do you judge the expense and effort involved in implementing the GDPR? (one answer)

- ☐ Little expense and effort
- ☐ Proportionate expense and effort
- ☐ Great expense and effort
- ☐ Extreme expense and effort

2. Which obligations under the GDPR involve the greatest expense and effort for you? (up to four answers possible, as well as "Other")

- ☐ Recording processing activities
- ☐ Data subject rights
- ☐ Data protection information/ privacy statement
- ☐ Risk assessment
- ☐ Handling data breaches
- ☐ Data protection impact assessment
- ☐ Processing
- ☐ Technical/organisational measures
- ☐ Safeguarding international data transfers
- ☐ Drawing up and implementing an erasure concept
- ☐ Obtaining consent
- ☐ Other (please specify): free text

3. What modifications would you like to see? (up to three answers possible; in addition "Other")

- ☐ No information obligations in the B2B sector
- ☐ No record of processing activities for normal-risk processing
- ☐ Introduction of a checklist with binding, precise specifications as to when a record of processing obligation is waived for SMEs

- ☐ No data leak notification to the data protection authority if the company itself is able to comprehensively clarify and resolve the incident
- ☐ Processing agreement should be adapted according to risk and be less bureaucratic
- ☐ Clear prerequisites as to when there is joint responsibility
- ☐ Other (free text)

4. Do you have difficulty in responding to requests for access rights under Article 15? (Under Article 15 of the GDPR, data subjects have the right to obtain information on which of their personal data is being processed in your company). (multiple answers possible)

- ☐ It is not possible to say
- ☐ No
- ☐ Yes – there is legal uncertainty regarding the question of what is meant by the right to obtain a copy of personal data
- ☐ Yes – there is legal uncertainty regarding the question of when a request for access rights constitutes an abuse of law
- ☐ Yes – because there has been an increase in the number of requests for access rights from dissatisfied customers
- ☐ Other (free text)

5. In your view, are there any problems with damages under Article 82 of the GDPR (for example, in connection with warning letters, data leaks, etc.)? (one answer possible)

- ☐ Yes
- ☐ No
- ☐ It is not possible to say

If yes, continue with question 5.1
If no, continue with question 6
If it is not possible to say, continue with question 6

5.1. What problems relating to damages under Article 82 of the GDPR do you see? (multiple answers possible)

- ☐ There is no materiality threshold
- ☐ The prerequisites are too narrow
- ☐ The term "damages" is not clear
- ☐ There is a risk of future class actions following the entry into force of the Consumer Rights Enforcement Act
- ☐ Other (free text)

6. Do you see challenges relating to data protection in the international transfer of data to third countries? (one answer possible)

☐ Yes

☐ No

☐ It is not possible to say

If yes, continue with question 6.1
If no, continue with question 7
If it is not possible to say, continue with question 7

6.1. What challenges do you see? (multiple answers possible)

☐ High level of expense and effort due to an absence of adequacy decisions or a lack of reliable adequacy decisions

☐ Binding corporate rules are too expensive/involve too much effort

☐ It is hardly possible for my own company to estimate the data protection level in a third country

☐ Other (free text)

7. Where do you see legal uncertainties in the GDPR (multiple answers possible)

☐ It is not possible to say

☐ I do not see any legal uncertainties

☐ The parameters of what constitutes personal data are not clear

☐ It is not clear when data are deemed to be anonymised

☐ Legal uncertainties on account of divergent views of data protection authorities

☐ Statutory provisions on the data economy are no longer manageable and some of them contradict the GDPR

☐ Other legal uncertainties in the sense of undefined terms in the GDPR (free text for examples)

8. Have you had contact with your data protection authority on your own initiative? (one answer)

☐ Yes

☐ No

If yes, continue with question 8.1
If no, continue with question 9

8.1. How satisfied were you with that contact? (one answer possible, as well as "Other")

☐ We received satisfactory help

☐ We did not receive satisfactory help

☐ We received an answer, but it took too long

☐ We did not receive an answer

☐ Other (free text)

9. In what ways should the data protection authority improve? (multiple answers possible)

☐ I am satisfied with the information my supervisory authority provides

☐ I would like to have (more) templates and checklists

☐ I would like to have (more) guidelines and recommendations that are practicable, clear and precisely worded

☐ Website contents should be clear and up to date (for example, search function)

☐ I would like more advisory services

☐ Other (free text)

10. Have you had any experience to date of data protection provisions, and in particular, their implementation and monitoring, in other EU Member States? (one answer)

☐ Yes

☐ No

If yes, continue with questions 10.1 and 10.2
If no, continue with question 11

10.1. In which EU Member State did you have this experience?

☐ In the following Member State: (free text)

10.2. Generally speaking, were the data protection provisions, and particularly their implementation and monitoring, stricter or less strict there than in Germany? (one answer possible)

☐ Stricter than in Germany

☐ The same

☐ Less strict that in Germany

☐ It is not possible to say

11. How has the significance of the subject of data protection changed for your company in the last three years, for example, due to the threat of cyber crime? (one answer)

☐ significance has decreased

☐ significance has remained the same

☐ significance has increased

☐ significance has greatly increased

Company information: How many employees does your company have?

- ☐ 1 to 19 employees
- ☐ 20 to 249 employees
- ☐ 250 to 999 employees
- ☐ more than 1000 employees

Which sector does your company belong to?

- ☐ Manufacturing industry
- ☐ Construction
- ☐ Trade
- ☐ Transport and storage
- ☐ Hospitality
- ☐ Information and communication
- ☐ Finance and insurance services
- ☐ Other services
- ☐ Other (free text)