Data Protection in the German Economy

Bitkom Study Report

bitkom

Data Protection in the German Economy

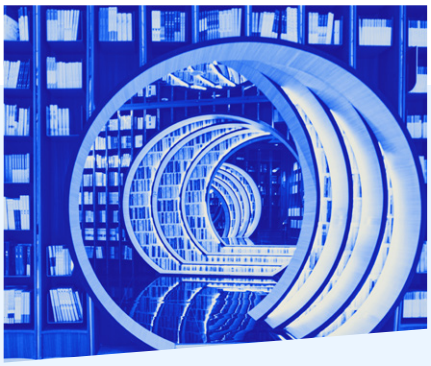
Bitkom Study Report

Bitkom Dataverse

All Bitkom studies are available in our data portal.

Bitkom Dataverse

Study Reports



DOI (German version)
10.64022/2026-datenschutz

Executive Summary

Eight years after the General Data Protection Regulation (GDPR) came into force, data protection is once again the focus of economic and digital policy debate. Companies generally support the objectives of data protection, but find its implementation in everyday life costly and complex. Advancing digitalisation, growing data volumes, international value chains and the increasing use of artificial intelligence raise the question of how workable data protection is in its current form and to what extent the existing legal framework should be further developed. How much effort is required to implement the data protection requirements? What are the biggest practical challenges? And what specific reforms do companies see as necessary in terms of regulation, supervision and policy?

The study is based on a representative computer-assisted telephone survey (CATI) of 603 companies in Germany with at least 20 employees across all sectors. The survey was conducted between calendar weeks 30 and 35 of 2025. Respondents included managing directors, board members and those responsible for IT, legal affairs, compliance and data protection officers.

Key Findings:

- **Data Protection Entails High and Increasing Effort for Companies**
  97 percent of companies state that the effort required for data protection is either very high (44 percent) or rather high (53 percent). For 69 percent, this effort has increased over the past year.
- **Documentation Obligations Are the Biggest Burden**
  73 percent of companies identify documentation requirements relating to processing activities as the primary driver of compliance costs.
- **Data Protection Remains an Ongoing Challenge**
  86 percent of companies report that implementing data protection requirements is never fully completed. 82 percent perceive legal uncertainty regarding the precise requirements of the GDPR.
- **The Vast Majority of Companies See a Need for Reform of the GDPR**
  81 percent of companies say that the GDPR makes their business processes more complex. 71 percent believe that the GDPR should be eased.
- **International Data Transfers Are Essential for Companies**
  A majority of companies transfer personal data to countries outside the EU. The main reasons are the use of cloud services (96 percent) and communication and video conferencing systems (90 percent).
- **Clear Expectations of Policymakers and Public Authorities**
  85 percent call for clearer data protection requirements and less bureaucracy. 79 percent advocate reform of the GDPR, 69 percent call for better alignment with other regulations, and 62 percent seek greater support from data protection authorities.

Content

Figures

1 Data Protection in Everyday Business Life

1 Data Protection in Everyday Business Life

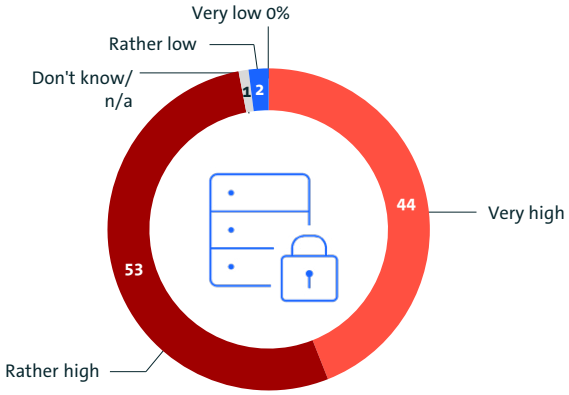
1.1 Effort Required for Data Protection

The vast majority of companies consider data protection costs to be high: 97 percent of companies rate them as 'very high' (44 percent) or 'rather high' (53 percent) overall. One percent rate the costs as 'rather low,' and not a single company rates them as 'very low.'

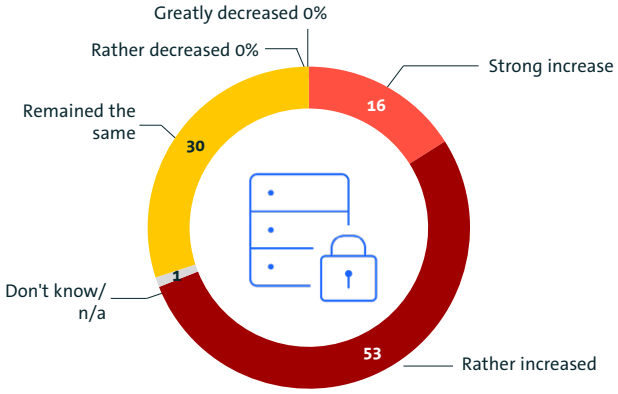
Compared to the previous year, the effort has increased for 69 percent of companies, with 16 percent reporting a significant increase and 53 percent reporting a slight increase.

30 percent report that the effort has remained the same, and no company reported a decrease in effort.

What is the general effort for data protection in your company?



How has the effort changed in the past year?



in percent

Base: All companies (n=603) | Source: Bitkom Research 2025

Figure 1: Effort Required for Data Protection in Companies and Changes in That Effort

> Data protection involves considerable effort: for companies, implementing data protection requirements is an ongoing issue that affects their day-to-day business and is becoming increasingly important, as a look at previous years shows.

1.2 Challenges in Implementing Data Protection Requirements

What are the biggest challenges in implementing data protection regulations such as the GDPR in your company?

Base: All companies (n=603) | Multiple answers possible | Source: Bitkom Research 2025

Figure 2: Greatest Challenges in Implementing Data Protection Requirements in Companies

A Permanent Work in Progress? The Challenges Companies Face in Data Protection

For companies, data protection remains an ongoing task: for 86 percent, implementation of data protection requirements is never fully completed. At the same time, uncertainty remains high: 82 percent report a lack of clarity regarding the precise requirements of the GDPR, and 80 percent must repeatedly undergo new assessments when rolling out new tools. 69 percent consider the overall requirements to be excessive.

Structural challenges further compound the situation. 54 percent state that data protection rules are interpreted inconsistently across the EU, and the same share report insufficient guidance from supervisory authorities. 53 percent encounter conflicting legal requirements, while 40 percent observe inconsistent interpretation within Germany.

Companies also face internal constraints. 50 percent cite the time required for necessary IT and system adjustments as a hurdle, and 46 percent point to the effort involved in making complex requirements understandable for employees. Other obstacles include a shortage of qualified professionals (38 percent), limited financial resources (31 percent), and insufficient involvement of data protection officers (25 percent). 12 percent report a lack of internal support for data protection.

> 82 percent of companies are uncertain about how the GDPR should be interpreted in practice.

1.3 Areas with the Greatest Data Protection Requirements

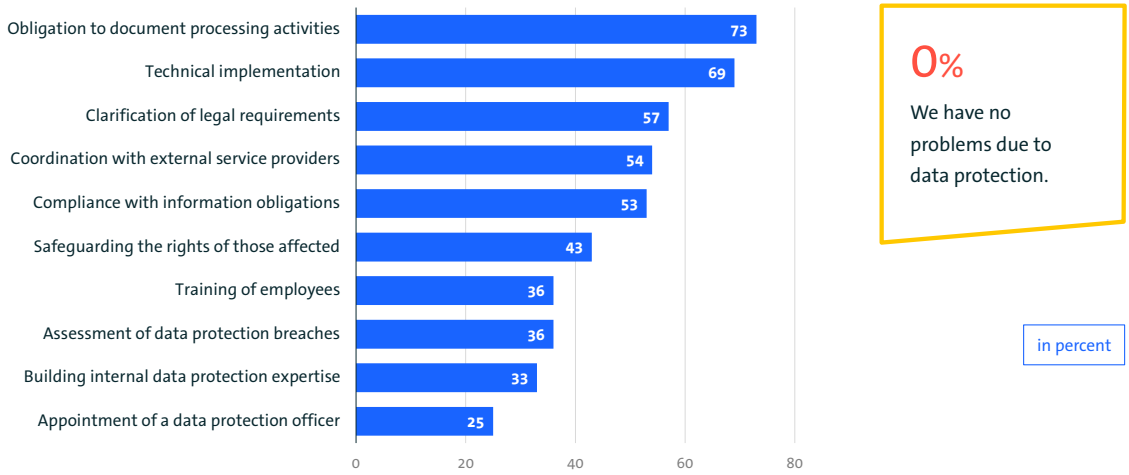
The greatest expense in implementing data protection arises in companies due to the documentation requirements for processing activities: 73 percent of companies cite this area as the biggest expense factor.

Other key cost drivers are the technical implementation of data protection measures (69 percent), clarification of legal requirements (57 percent), coordination with external service providers (54 percent) and compliance with information obligations (53 percent).

In addition, 43 percent cite ensuring the rights of data subjects as costly. Thirty-six percent report high costs for training employees and assessing data protection violations.

Not a single company states that it has no problems due to data protection.

What causes your company the most effort in implementing data protection?



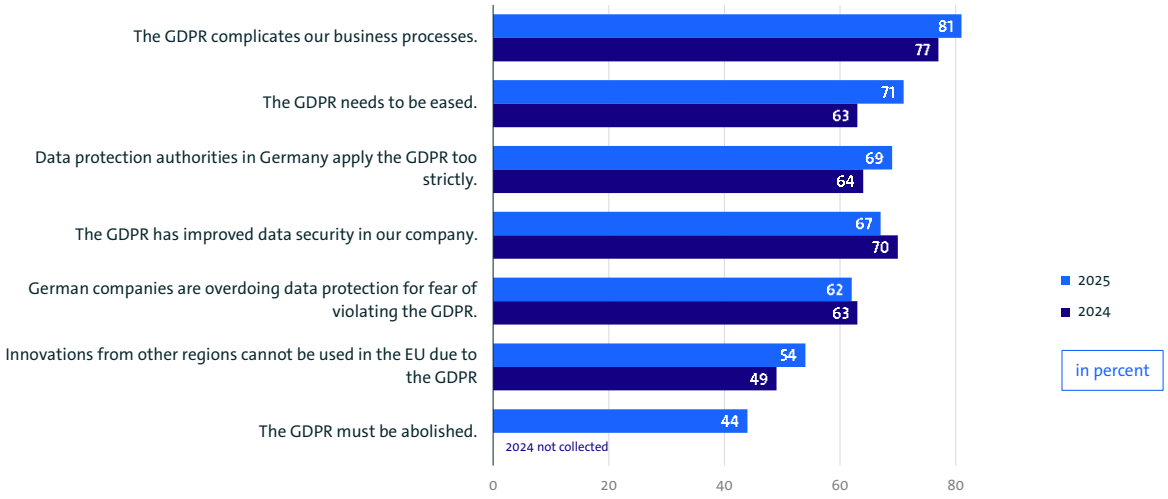
Base: All companies (n=603) | Multiple answers possible | Source: Bitkom Research 2025

Figure 3: Areas Involving the Greatest Effort in Implementing Data Protection

> Documentation causes the most work: for companies, it is the largest single expense in implementing data protection requirements.

1.4 Companies' Attitudes Towards the GDPR

Which of the following statements do you think apply to the GDPR?



Base: All companies (n=603) | Percentages for "Strongly Agree" and "Tend to Apply" | Source: Bitkom Research 2025

Figure 4: Statements on the General Data Protection Regulation (GDPR)

Eight years after the General Data Protection Regulation came into force, the picture is mixed:

Although many companies (67 percent) recognise that the GDPR has contributed to improved data security, at the same time 81 percent of the companies surveyed state that the GDPR makes their business processes more complicated.

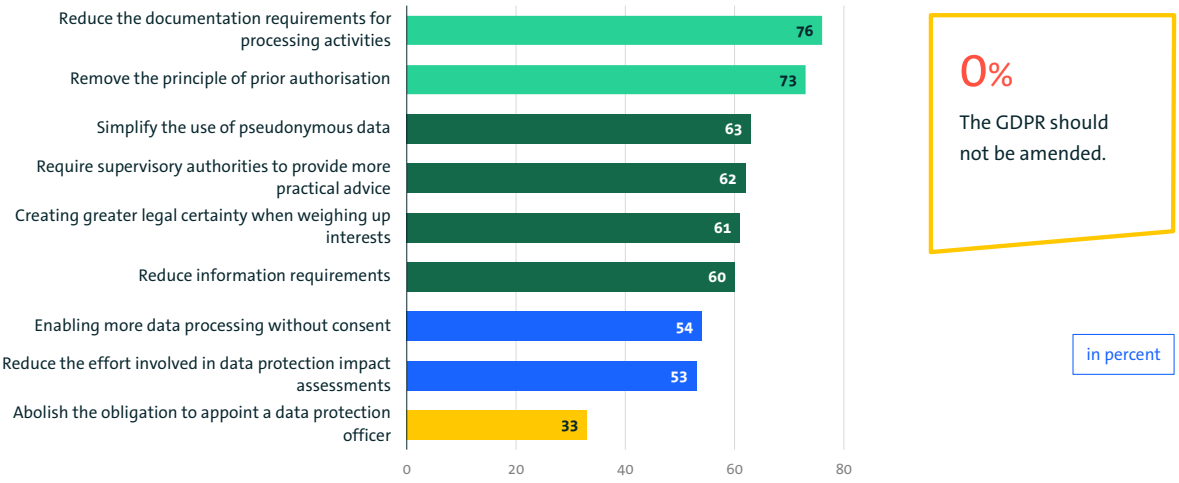
The General Data Protection Regulation is viewed critically by most companies: 81 percent of companies state that the GDPR complicates their business processes. 71 percent also believe that the GDPR should be relaxed, and 44 percent even agree that it should be abolished.

The application of the GDPR by supervisory authorities is also viewed critically: 69 percent of companies believe that data protection authorities in Germany apply the GDPR too strictly. In addition, 62 percent state that companies are acting overly cautiously for fear of data protection violations.

More than half of companies (54 percent) also believe that innovations from other regions cannot be used in the European Union because of the GDPR. At the same time, 67 percent agree with the statement that the GDPR has improved data security in companies.

1.5 Specific Reform Needs Regarding the GDPR

If you think specifically of the GDPR, where should it be improved?



Base: All companies (n=603) | Multiple answers possible | Source: Bitkom Research 2025

Figure 5: Areas in Which Companies Consider Amendments to the GDPR Necessary

76 Percent of Companies Support Reducing Documentation Requirements and Regulatory Restrictions

Companies identify a need for adjustments to the General Data Protection Regulation (GDPR) in numerous areas. The most frequently cited measures are a reduction in documentation requirements for processing activities (76 percent) and the abolition of the principle of prohibition subject to authorisation (73 percent).

In addition, around six in ten companies advocate simplified use of pseudonymised data (63 percent), mandatory, more practice-oriented guidance from supervisory authorities (62 percent), greater legal certainty in the balancing of interests (61 percent), and a reduction in information obligations (60 percent).

Further proposals include expanding the scope for data processing without consent (54 percent) and reducing the review requirements for data protection impact assessments (53 percent). One third of companies (33 percent) support abolishing the obligation to appoint a data protection officer. Not a single company states that no amendments to the GDPR are needed.

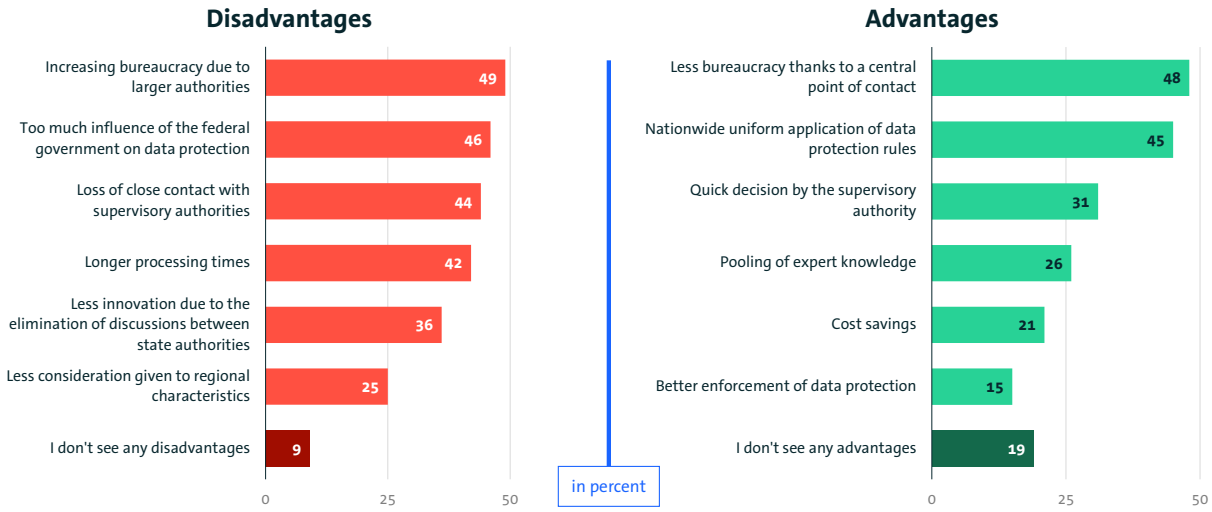
> "It is about making the GDPR workable in practice after seven years. Data protection must be clear and applicable", says Susanne Dehmel, Member of the Executive Board of Bitkom ↗ Bitkom press release

2 Data Protection Supervisory Authority

2 Data Protection Supervisory Authority

2.1 Centralisation of Data Protection Supervisory Authority

Where do you see disadvantages or advantages of centralising the data protection authority?



Base: All companies (n=603) | Multiple answers possible | Source: Bitkom Research 2025

Figure 6: Advantages and Disadvantages of Centralising Data Protection Supervisory Authority

What Speaks for and Against Centralised Data Protection?

The current debate extends beyond the GDPR to include a potential reform of Germany's data protection supervisory structure. When it comes to the proposal to centralise the data protection authority at federal level, the business community is divided.

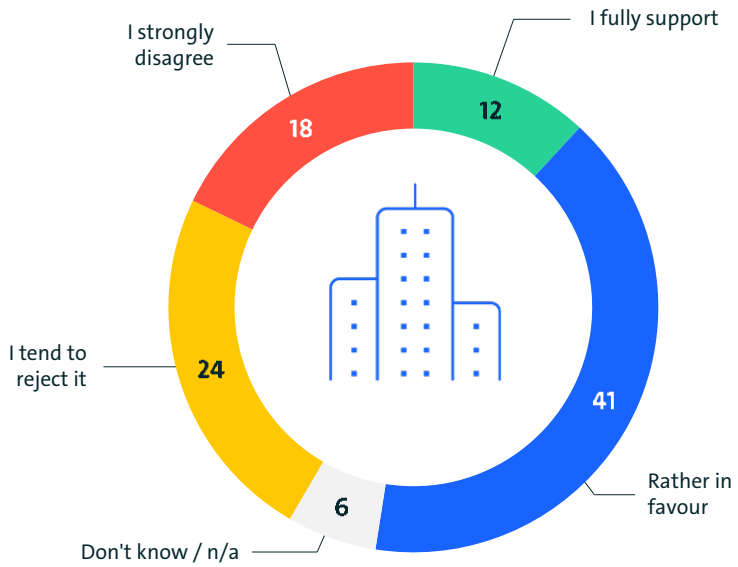
From the companies' perspective, the main arguments in favour of centralised supervision are a more consistent interpretation of data protection requirements and clearer responsibilities. 45 percent expect more uniform application of data protection rules across Germany, and 48 percent anticipate less bureaucracy through a single central point of contact.

In addition, 31 percent see advantages in faster supervisory decisions, and 26 percent in the pooling of expert knowledge.

On the other hand, concerns focus primarily on additional bureaucracy and greater distance from business practice. 49 percent fear increased bureaucracy as a result of a larger authority, and 44 percent see a loss of proximity and direct points of contact. 42 percent expect longer processing times, and 46 percent express concern about excessive federal influence over data protection.

Overall, however, a narrow majority of companies are in favour of centralising data protection supervision at federal level: 53 percent support the proposal, while 42 percent reject it:

How do you assess the proposal to centralise the data protection authority at the federal level?



in percent

Base: All companies (n=603) | Deviations of 100 percent are due to rounding | Source: Bitkom Research 2025

Figure 7: Assessment of the Proposal to Centralise the Data Protection Authority at Federal Level

> "The discussion about reforming data protection supervision in Germany is important. Given the multitude of challenges facing companies, we must make the best possible use of the authorities' resources and, in particular, ensure that good advice is provided and that interpretation and enforcement are consistent."
>
> Susanne Dehmel ↗Bitkom press release

3 Data Protection Violations

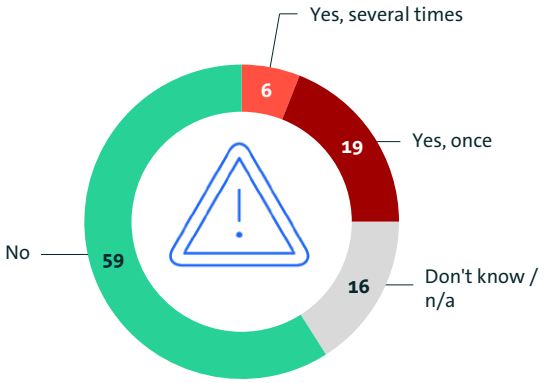
3 Data Protection Violations

3.1 Data Protection Violations in Companies

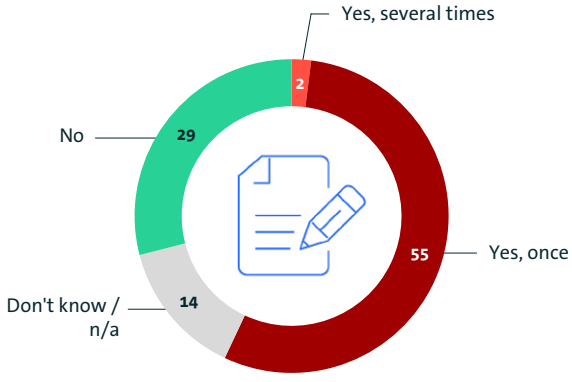
A quarter of companies report data protection breaches in the past twelve months. 19 percent of companies experienced one data protection breach, while a further 6 percent experienced multiple breaches. 59 percent state that they have not had any data protection breaches, while 16 percent are unable or unwilling to provide any information on this.

Of the companies that experienced data protection breaches, 57 percent reported them to the relevant supervisory authority. 29 percent did not report them, and 14 percent stated that they were unable or unwilling to provide any information on this matter.

Have there been any data protection violations in your company in the past twelve months?



Were there any data protection violations that you reported to the supervisory authority?



in percent

Base (left): All companies (n=603) | Base (right): Companies with data protection violations (n=153) | Source: Bitkom Research 2025

Figure 8: Occurrence and Reporting of Data Protection Violations in the Past Twelve Months

Data protection violations occur regularly within companies: one quarter report having experienced such breaches in the past twelve months. A large proportion of the affected companies notified the competent supervisory authorities; at the same time, for a relevant share it remains unclear whether and to what extent notifications were made.

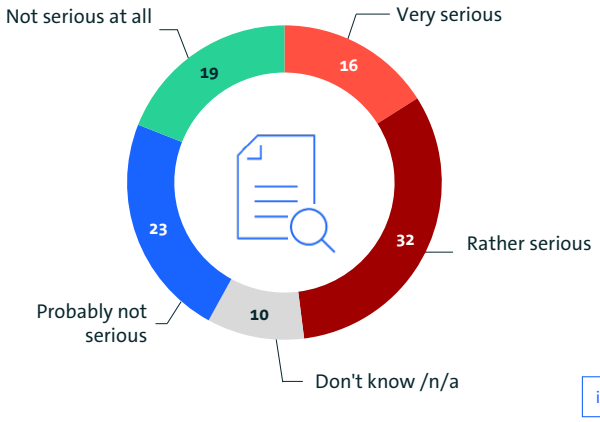
3.2 Consequences of Data Protection Violations

Data protection violations have tangible consequences for many companies: around one in two companies that have experienced a data protection breach rate the impact as very severe (16 percent) or rather severe (32 percent). 23 percent assess the consequences as rather not severe, and 19 percent as not severe at all. 10 percent of companies are unable or unwilling to provide an assessment.

When asked about the specific consequences of the most significant data protection breach in the past twelve months, the findings primarily point to a high organisational burden: 93 percent of affected companies cite this as a consequence. Fines follow at a considerable distance, reported by 51 percent. 18 percent state that they lost customers as a result of a data protection violation. 7 percent each report claims for damages and reputational harm.

Only 5 percent of companies state that a data protection violation had no consequences for them.

How serious were the consequences of the data breach for your company?



When you think about the biggest breach, what were the consequences of this data breach?

Base: Companies with data protection violations (n=153) | right: multiple answers possible | Source: Bitkom Research 2025

Figure 9: Severity and Consequences of Data Protection Violations from the Perspective of Affected Companies

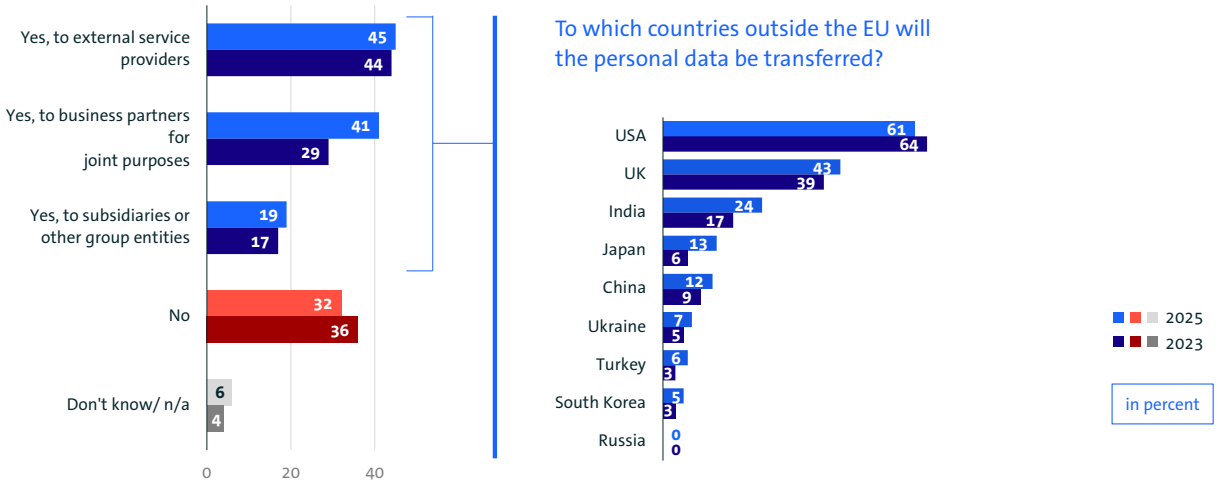
Data protection violations entail significant consequences for many companies: in addition to organisational burdens (93 percent), affected companies also report financial impacts (51 percent) and reputational consequences (7 percent).

4 International Data Transfers

4 International Data Transfers

4.1 Transfer of Personal Data Outside the EU

Does your company transfer personal data outside the EU?



Base (left): All companies (n=603) | Base (right): Companies transferring personal data outside the EU (n=376) | Multiple answers possible | Source: Bitkom Research 2025

Figure 10: Scope and Destination Regions of International Transfers of Personal Data

International Data Transfers Are Widespread

The majority of companies in Germany transfer personal data to countries outside the EU. In doing so, data are primarily transferred to external service providers (45 percent) and to business partners for joint purposes (41 percent). 19 percent of companies transfer personal data to subsidiaries or other entities within their corporate group.

Personal data are most frequently transferred to the United States (61 percent), followed by the United Kingdom (43 percent) and India (24 percent).

For many companies, international data transfers are closely linked to core digital applications and globally organised business processes. Accordingly, there is a strong need for clear and reliable framework conditions for cross-border data processing.

"International data transfers are indispensable for a global economy. At the same time, the often unclear legal framework creates uncertainty for many companies."

Susanne Dehmel, Member of the Executive Board of Bitkom

4.2 Reasons for International Data Transfers

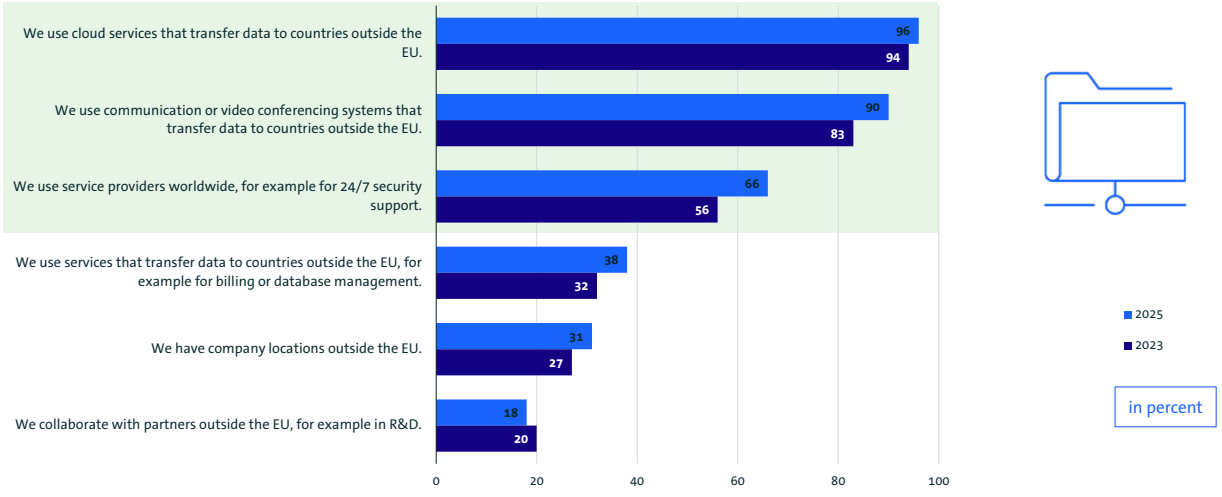
Companies engage in international data transfers for a variety of reasons. The most frequently cited is the use of cloud services that transfer data to countries outside the EU (96 percent). The use of communication or video conferencing systems involving data processing outside the EU is also widespread (90 percent).

In addition, 66 percent of companies rely on global service providers, for example to ensure around-the-clock IT or security support.

Other reasons include services for billing or database management (38 percent), company locations outside the EU (31 percent), and cooperation with partners outside the EU, for example in research and development (18 percent).

> Cloud services and communication solutions are the most frequently cited reasons for international data transfers.

Why does your company transfer personal data to non-EU countries?



Base: Companies that transfer personal data outside the EU (n=376) | Multiple answers possible | Source: Bitkom Research 2025

Figure 11: Reasons for Transferring Personal Data to Countries Outside the EU

> From a business perspective, international data transfers are therefore not a voluntary additional option, but are often a prerequisite for the use of centralised digital applications and services.

4.3 Consequences of Refraining from International Data Transfers

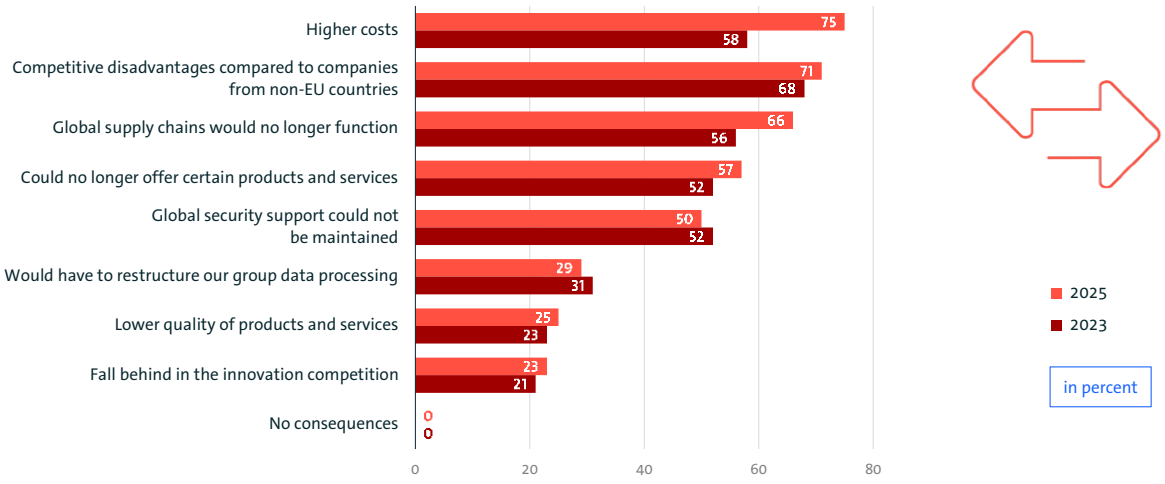
From the companies' point of view, refraining from processing personal data outside the EU would have far-reaching consequences: most frequently, companies expect higher costs (75 percent) and competitive disadvantages compared to companies from non-EU countries (68 percent). 66 percent assume that global supply chains would no longer function in this case.

In addition, 57 percent of companies state that they would no longer be able to offer certain products or services. Around half (50 percent) see global security support as being at risk. 31 percent would have to restructure their corporate data processing.

Further consequences would include poorer quality products and services (25 percent) and a decline in innovation competitiveness (23 percent).

No company states that abandoning international data transfers would have no consequences.

What would be the consequences if you had to refrain from processing personal data outside the EU?



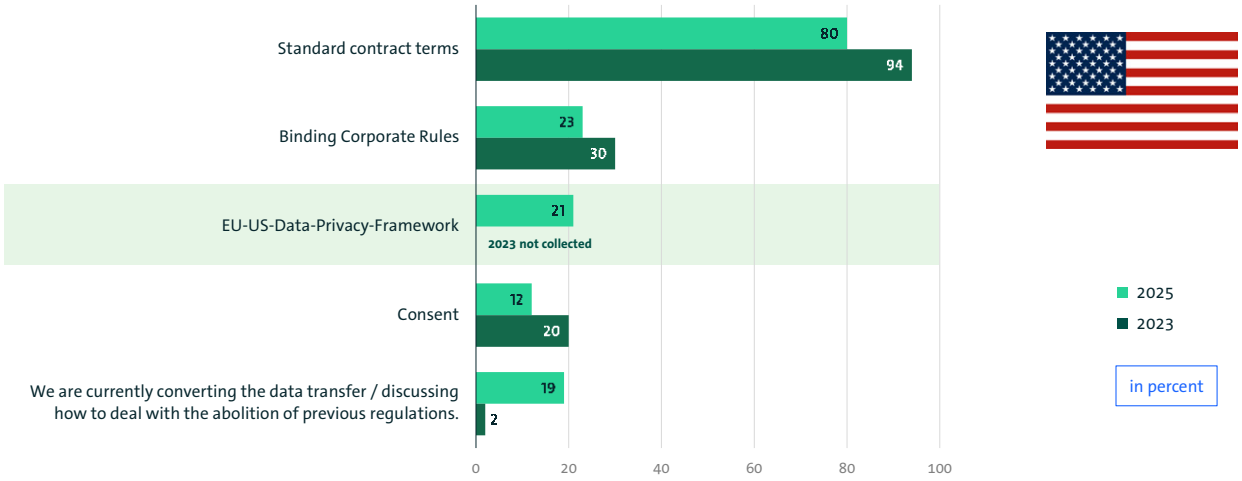
Base: Companies that transfer personal data outside the EU (n=376) | Multiple answers possible | Source: Bitkom Research 2025

Figure 12: Expected Consequences of Refraining from the Processing of Personal Data Outside the EU

> Companies cannot dispense with international data transfers: from their perspective, any suspension would have tangible economic and organisational consequences, potentially leading to competitive disadvantages and restrictions on core business processes.

4.4 Legal Bases for Transfers of Personal Data to the United States

What is your company's current legal basis for transferring personal information to the U.S.?



Base: Companies that transfer personal data to the USA(n=229) | Multiple answers possible | Source: Bitkom Research 2025

Figure 13: Legal Bases for Personal Data Transfers to the United States

One Fifth Relies on the EU–US Data Privacy Framework

Companies that transfer personal data to the United States predominantly rely on standard contractual clauses. 80 percent of companies cite these as the legal basis. Standard contractual clauses thus remain by far the most important basis for data transfers to the United States.

In addition, 23 percent of companies use binding corporate rules. One-fifth of companies (21 percent) state that they use the EU-US Data Privacy Framework as the legal basis for data transfers to the US. 12 percent base data transfers on the consent of the data subjects.

In addition, 19 percent of companies state that they are currently still working on converting their data transfers or discussing how to deal with the discontinuation of previous regulations.

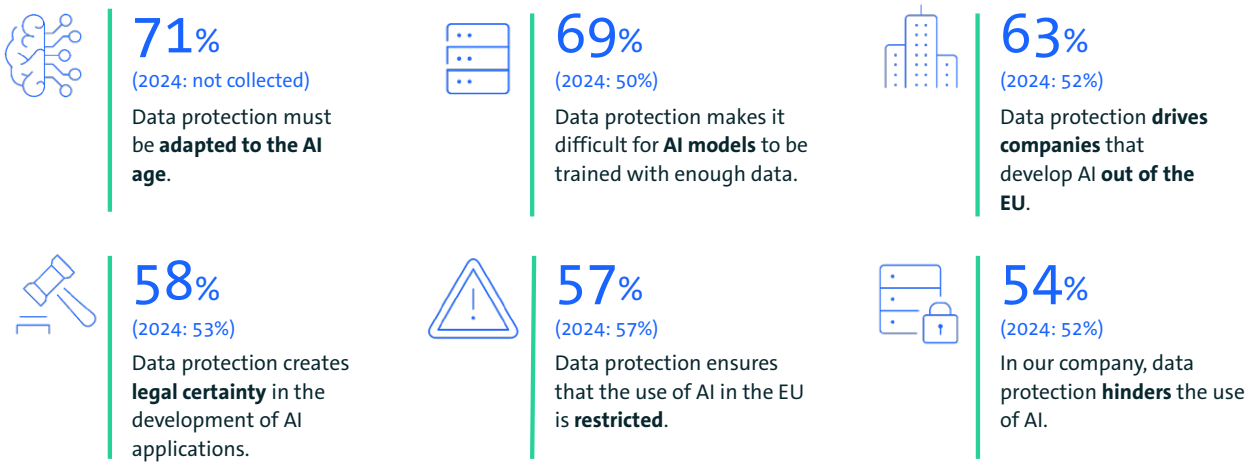
> Standard contractual clauses remain the central basis for data transfers to the United States. In addition, the EU-US Data Privacy Framework is becoming increasingly important for some companies.

5 Artificial Intelligence and Data Protection

5 Artificial Intelligence and Data Protection

5.1 Data Protection as a Factor in the Development & Deployment of AI

Which of the following statements apply to your company or in your opinion?



Base: All companies (n=603) | Percentages for "Strongly Agree" and "Tend to Apply" | Source: Bitkom Research 2025

Figure 14: Companies' Assessment of the Impact of Data Protection on the Development and Deployment of Artificial Intelligence

Data Protection Slows Down Artificial Intelligence

With regard to artificial intelligence, companies predominantly take a critical view of data protection. 71 percent believe that data protection rules need to be adapted to the age of AI. 69 percent state that data protection regulations make it more difficult to train AI models with sufficient data — a significant increase compared with the previous year (2024: 50 percent). 63 percent see a risk that companies developing AI will relocate outside the EU due to data protection requirements.

At the same time, 57 percent report that data protection restricts the use of AI within the EU, and 54 percent say it hampers the deployment of AI in their own company.

However, 58 percent also agree that data protection provides legal certainty for the development of AI applications.

> "Artificial intelligence is the key technology of the future, and AI needs data. Data protection regulations should also be reviewed with a view to Germany's position in the future world of AI."
>
> Susanne Dehmel ↗Bitkom press release

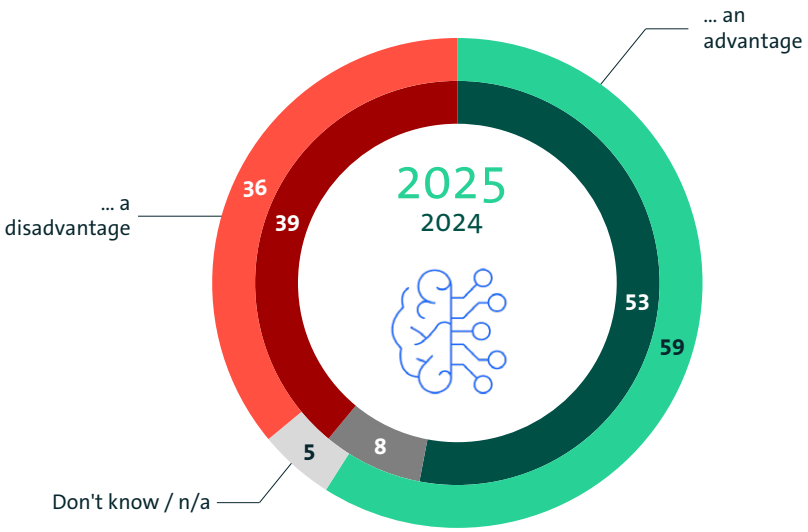
5.2 AI: European Data Protection in International Comparison

Despite the considerable effort involved, many companies view European data protection as a competitive advantage for the development of artificial intelligence in an international comparison.

At the same time, companies are increasingly exploring how AI itself can be used to support data protection. Almost half are considering such applications: in 2024, 5 percent were already using AI-based solutions for data protection purposes, 24 percent were planning their deployment, and a further 19 percent were discussing their use (see Bitkom Data Protection Study 2024).

Applications include chatbots for responding to data protection queries, systems for detecting data protection violations, and tools for the automated anonymisation or pseudonymisation of data.

For the development of AI in Germany and Europe, European data protection in international comparison is...



in percent

Base: All companies (n=603) | Source: Bitkom Research 2025

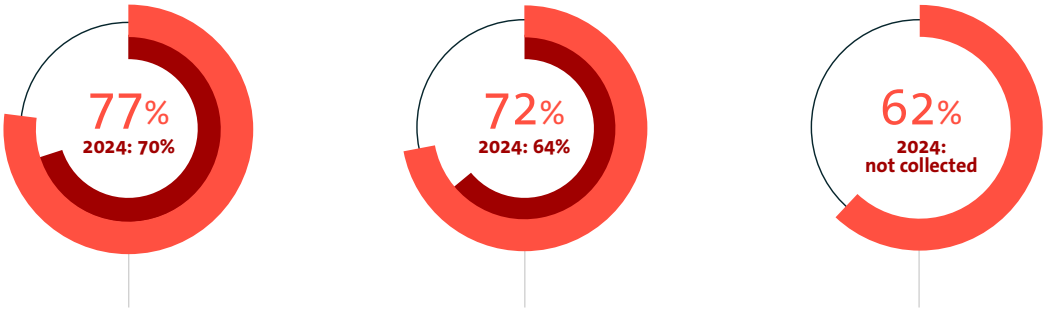
Figure 15: Companies' Assessment of the Impact of European Data Protection on AI Development in International Comparison

6 Data Protection Policy

6 Data Protection Policy

6.1 Data Protection Policy – Statements

To what extent do you think the following statements are true?



Base: All companies (n=603) | Percentages for "Strongly Agree" and "Tend to Apply" | Source: Bitkom Research 2025

Figure 16: Companies' Assessment of the Impact of Data Protection Policy on Digitalisation and Practical Implementation

Three quarters consider German data protection to be excessive

The results show that companies take a highly critical view of current data protection policy:

77 percent believe that data protection is hindering digitalisation in Germany. 72 percent think that data protection in Germany is excessive. In addition, 62 percent consider existing data protection regulations to be virtually impossible to implement, especially for smaller companies.

Compared to the previous year, this criticism from companies has increased further in all areas ↗ Bitkom Dataverse.

The assessments of companies show the need for data protection that is effective and can be implemented in a practical manner. ↗Despite initial attempts to ease the burden at European level, structural problems remain, particularly due to legal uncertainty and complex requirements. Many companies therefore see an urgent need for clearer rules and less bureaucracy.

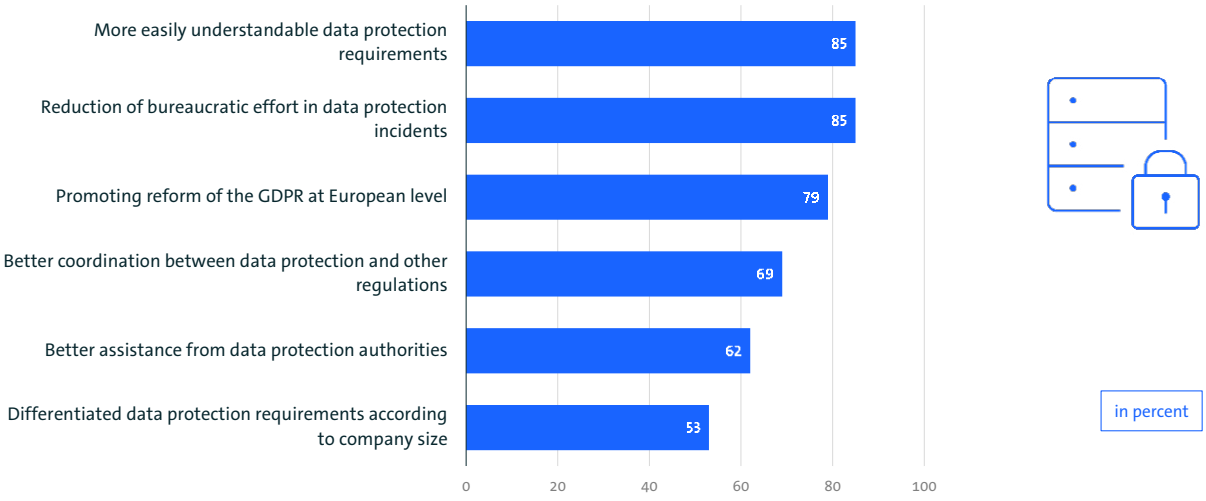
6.2 Expectations of Policymakers and Public Authorities

Companies articulate clear expectations of policymakers and public authorities regarding data protection. The two most important priorities are clearer data protection requirements and less bureaucracy: 85 percent advocate rules that are easier to understand, and an equal 85 percent call for a reduction in administrative burdens associated with data protection incidents.

79 percent urge policymakers to advance a reform of the General Data Protection Regulation (GDPR) at the European level.

In addition, 69 percent call for better alignment of data protection rules with other regulatory frameworks, and 62 percent seek greater guidance from data protection authorities. More than half of companies (53 percent) favour differentiated data protection requirements based on company size.

What measures do you expect from policymakers and public authorities in terms of data protection?



Base: All companies (n=603) | Multiple answers possible | Source: Bitkom Research 2025

Figure 17: Companies' Expectations for the Future Development of Data Protection

Clear Rules, Less Bureaucracy – What Companies Expect from Policymakers:

Companies expect policymakers and public authorities to deliver data protection rules that are clear, comprehensible and workable in practice. Their priorities are clearly formulated requirements, a tangible reduction in administrative burdens and a reform of the GDPR at European level that preserves effective data protection while making compliance significantly easier in day-to-day business operations.

7 Conclusion

The results of this survey show that data protection has become a key economic and location policy issue for companies: almost all companies (97 percent) report high or very high implementation costs, with 69 percent seeing a further increase in costs over the past year. For 86 percent, data protection is not a completed task, but an ongoing burden in everyday business life.

At the same time, criticism of the current data protection regulations is growing: 77 percent of companies believe that data protection is hindering digitalisation in Germany, while 72 percent consider it to be excessive. The assessment of the General Data Protection Regulation (GDPR) is correspondingly negative: 81 percent of the companies surveyed say that the GDPR complicates business processes, 71 percent are in favour of relaxing it, and 44 percent even consider it necessary to abolish the GDPR.

The pressure to act is particularly evident in the field of Artificial Intelligence: seven out of ten companies (71 percent) are calling for data protection to be adapted to the AI age. 69 percent see data protection as an obstacle to training AI models. At the same time, however, 58 percent of the companies surveyed recognise that data protection creates legal certainty for AI.

International data transfers also highlight the relevance of data protection policy to business locations: cloud services, communication solutions and global support are indispensable for the majority of companies. The elimination of such transfers would have serious economic consequences: 75 percent expect higher costs, and 71 percent expect competitive disadvantages.

The findings of this study highlight that data protection has become a key location factor for the German economy. Companies are not calling for a lowering of protection standards; rather, they seek clearer, more practicable and innovation-friendly framework conditions. Modern data protection must provide legal certainty, facilitate international data flows and actively enable technological developments such as artificial intelligence. An approach of this kind would not only safeguard the protection of personal data, but also strengthen Germany’s capacity for innovation and its overall competitiveness.

8 Methodology

On behalf of	Bitkom
Methodology	Computer Assisted Telephone Interview (CATI)
Statistical population	Companies in Germany with at least 20 employees
Target persons	Management, executive board, chief information officers or data protection officers, heads of legal departments, legal advisors or compliance officers
Nominal sample size	n=603
Period of interviewing	From week 30 to week 35 of 2025
Weighting	Representative weighting of the dataset based on the current Business Register of the Federal Statistical Office of Germany
Statistical fault tolerance	+/- 4 percent

Publisher
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Policy and Content Lead
Susanne Dehmel
Isabelle Stroot

Head of Research
Bettina Lange

Editor
Alissa Geffert

DOI (German version)
10.64022/2026-datenschutz

Data protection is an integral part of the digital economy – and at the same time a major challenge for companies. Eight years after the General Data Protection Regulation (GDPR) came into force, this study shows how companies in Germany experience data protection today. The results of a representative survey of 603 companies clearly show where the greatest burdens lie, how great the need for reform is estimated to be, and what expectations companies have of politics, supervision and regulation. At the same time, this study highlights the importance of international data transfers and the increasing conflict between data protection and the use of artificial intelligence.

DOI (german version)
10.64022/2026-datenschutz

bitkom