Ten Years of GDPR

An Interim Assessment of Data Protection in Companies

bitkom

Ten Years of GDPR

An Interim Assessment of Data Protection in Companies

Bitkom Dataverse

This and other Bitkom studies are available in our data portal.

To Bitkom Dataverse

To the study reports

DOI (German version)
10.64022/2026-DSGVO

Executive Summary

On 25 May 2026, the General Data Protection Regulation (GDPR) marks its tenth anniversary. Since its entry into force in 2016, Bitkom has been monitoring data protection in Germany through regular surveys of companies — from the preparation phase before the GDPR became applicable (2016-2018) to current challenges related to digitalisation, international data transfers and artificial intelligence. This year's findings provide a ten-year perspective on key developments from a business perspective. The results show that data protection has long since become part of companies' day-to-day operations. At the same time, the effort required for compliance, as well as legal uncertainty, remain high for many companies. This report analyses developments in individual areas between 2016 and 2025 and presents an interim assessment of the GDPR. It is based on representative surveys conducted by Bitkom Research using computer-assisted telephone interviews (CATI). The surveys covered companies from all sectors in Germany with 20 or more employees.

Key findings:

- **Data protection has become embedded in companies — but implementation is still incomplete**
  In 2024, 71 percent of companies reported that they had fully or largely implemented the GDPR — the highest figure in the time series. At the same time, 28 percent stated that the requirements had only been partially implemented or had not yet been implemented at all. The implementation of the GDPR therefore remains an ongoing task for many companies, even years after it became applicable.

- **Data protection is associated with an increasing workload for companies**
  In 2025, 97 percent of companies rated the effort required for data protection compliance as high — 44 percent as very high and 53 percent as fairly high. In addition, 84 percent stated that their data protection workload had increased since the introduction of the GDPR. There is therefore little indication that greater experience and routine have reduced the compliance burden.

- **Many companies believe that the GDPR adds complexity to business processes**
  In 2025, 81 percent of companies stated that the GDPR makes their business processes more complex. In 2016, this figure stood at just 25 percent. The perception that the GDPR creates additional complexity has therefore become significantly more widespread over time.

- **Legal uncertainty remains one of the greatest challenges**
  In 2025, 82 percent of companies cited uncertainty regarding the precise data protection requirements as a challenge. At the same time, 86 percent stated that GDPR implementation is never truly complete because companies must continuously adapt to technological and legal developments. Data protection is therefore widely perceived as a particularly demanding and ongoing compliance task.

- **Data protection is increasingly perceived as an obstacle to innovation**
  This particularly affects data-driven initiatives. By 2025, 59 percent of companies reported that the creation of data pools had failed due to data protection requirements or had not even been attempted. The figures are similarly high for data analytics tools, AI applications and the digitalisation of business processes. Data protection requirements are therefore perceived as a particular obstacle where innovation depends on the use of large datasets.
- **There is growing tension between data protection and AI**
  By 2025, 59 percent of companies viewed European data protection rules as an advantage for AI development in Germany and Europe by international comparison. At the same time, 69 percent stated that data protection makes it difficult to train AI models on sufficient data, while 63 percent believed that data protection encourages companies developing AI to relocate outside the EU. Data protection is therefore seen as a potential mark of quality, but in the practical development of AI it is often perceived as a competitive disadvantage.
- **International data transfers remain indispensable — but politically unresolved**
  The United States remains the most important third country for transfers of personal data outside the EU. By 2025, 61 percent of companies reported transferring personal data there.
- At the same time, 71 percent of companies called for sustainable political solutions for international data transfers. This demonstrates that global data flows are an economic reality, while their legal certainty remains a key challenge.
- **From the business community's perspective, reform of the GDPR is necessary**
  By 2025, 72 percent of companies agreed with the statement: «We are going overboard with data protection in Germany." This criticism is directed not at data protection as a fundamental right, but at an implementation framework that many companies perceive as overly complex, legally uncertain and excessively burdensome. Reform should therefore provide greater legal certainty, a more risk-based approach and better conditions for data-driven innovation.

Overall, the findings of the study show that the GDPR has firmly embedded data protection within the German economy. However, it has not resulted in less effort, greater clarity or simpler processes. Companies accept data protection as an important framework for trust in the digital economy, but they are calling for a more practical and risk-based application. Ten years after its entry into force, the GDPR has reached a new stage of development. It must ensure effective protection of fundamental rights while also enabling innovation, AI development and international competitiveness.

Key Milestones

From the Data Protection Directive to the GDPR

1995

European Data Protection Directive

With Directive 95/46/EC, the EU establishes, for the first time, a common framework for the protection of personal data and the free movement of data within the internal market. It forms the foundation of European data protection law prior to the GDPR.

2012

Proposal for Data Protection Reform

The European Commission presents the draft General Data Protection Regulation (GDPR). The aim is to create a harmonised legal framework that applies directly to an increasingly digital and data-driven economy.

2016

Adoption of the GDPR

The European Parliament and the Council of the European Union adopt the GDPR. It is published in the Official Journal of the European Union on 4 May 2016 and enters into force on 24 May 2016. Companies are given a two-year transition period before the Regulation becomes applicable.

25 May 2018

The GDPR becomes applicable

The GDPR becomes directly applicable in all EU Member States. Companies are required to comprehensively review and adapt their data protection processes, documentation, legal bases, data subjects' rights, processor relationships, and governance structures.

2019/2020

Consent and cookies come into focus

In its Planet49 judgment, the Court of Justice of the European Union (CJEU) clarifies the requirements for valid cookie consent. In Germany, the TTDSG — now the TDDDG — establishes an independent legal framework for the protection of privacy in telecommunications and digital services.

2020

Schrems II and international data transfers

In its Schrems II judgment, the CJEU invalidates the EU–US Privacy Shield. Companies are required to reassess international data transfers, particularly those involving US service providers, and to examine additional safeguards.

2021

New Standard Contractual Clauses

The European Commission publishes modernised Standard Contractual Clauses (SCCs) for transfers to third countries. Following Schrems II, they become the primary instrument for many international data transfers.

2023

EU-US Data Privacy Framework

The EU establishes a new legal basis for transfers of personal data to the United States. At the same time, generative AI and new digital legislation increasingly shape the data protection debate.

since 2024

Data protection in the context of new digital regulation

With the Digital Services Act (DSA) and the AI Act, data protection is increasingly becoming part of a broader European digital regulatory framework. For companies, the focus is shifting from pure GDPR compliance towards integrated data, platform and AI governance.

Inhalt

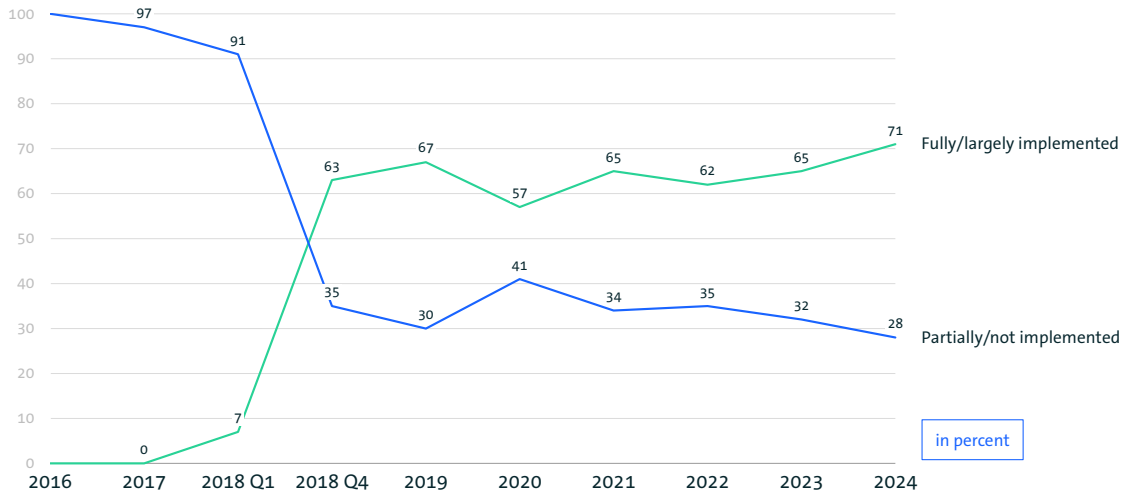
Figures

1 Implementation & Burden

1 Implementation & Burden

1.1 How far has the GDPR been implemented in companies?

How advanced is your company's GDPR implementation?



Base: All surveyed companies with 20 or more employees | Totals may not equal 100 percent due to rounding | "Don't know/ no answer" not shown | Source: Bitkom Research

Figure 1: Implementation status of the GDPR

Data protection has become established — but implementation remains incomplete

The GDPR has become firmly embedded within companies. Before it became applicable in May 2018, full or substantial implementation was practically non-existent. In 2016 and 2017, the share stood at 0 percent, rising to just 7 percent in the first quarter of 2018. Once the GDPR became applicable, implementation accelerated significantly. By the fourth quarter of 2018, 63 percent of companies reported that they had fully or largely implemented the requirements. In 2019, this figure rose to 67 percent.

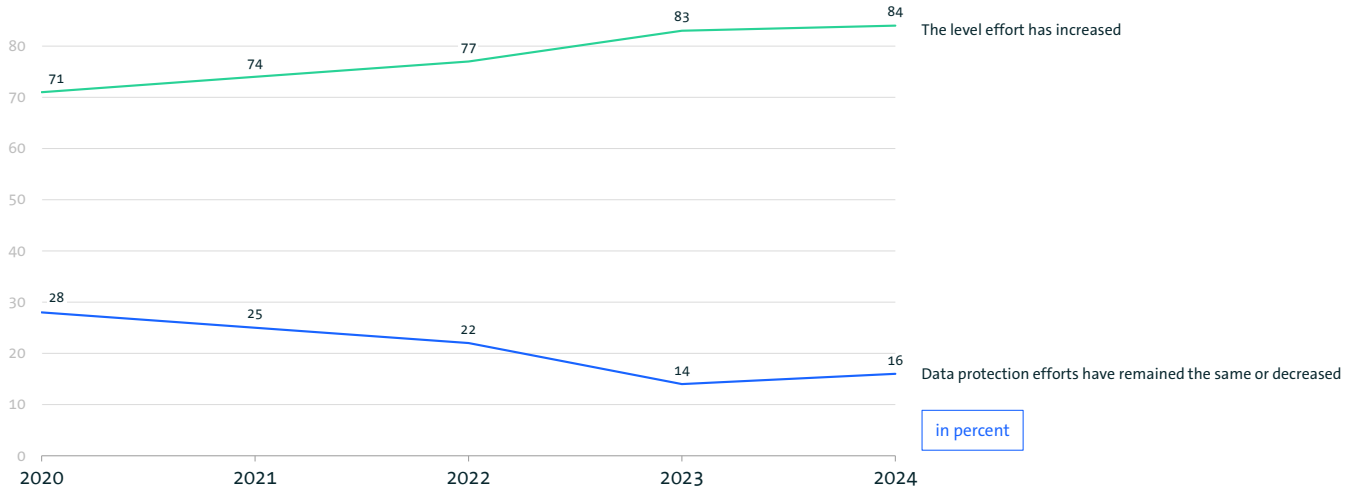
However, the decline to 57 percent in 2020 demonstrates that GDPR compliance is not a one-off implementation project. New legal requirements and continuing legal uncertainty — particularly regarding international data transfers following the Schrems II judgment — likely led many companies to reassess their level of implementation more critically. In its July 2020 ruling, the Court of Justice of the European Union (CJEU) invalidated the EU–US Privacy Shield. As a result, companies were required to carry out additional assessments and, where necessary, implement supplementary safeguards in connection with Standard Contractual Clauses (SCCs).

The developments in 2022 also indicate that data protection measures require continuous adjustment. Existing Standard Contractual Clauses (SCCs) had to be replaced by the new EU Standard Contractual Clauses by the end of December 2022, creating additional compliance and implementation requirements for many companies.

In 2024, 71 percent of companies reported that they had fully or largely implemented the GDPR — the highest figure in the time series. At the same time, 28 percent still regarded the requirements as only partially implemented or not yet implemented at all. These figures highlight two key findings: data protection has become firmly established across the economy, but even ten years after the GDPR became applicable, compliance remains an ongoing task.

1.2 Effort for Data Protection

Which of the following statements best describes your organisation's data protection efforts since the GDPR came into force in 2018?



Base: All surveyed companies with at least 20 employees | Totals may not equal 100 percent due to rounding | "Don't know/no answer" responses not shown | Source: Bitkom Research

Figure 2: Effort for data protection since the introduction of the GDPR

Greater maturity, greater effort

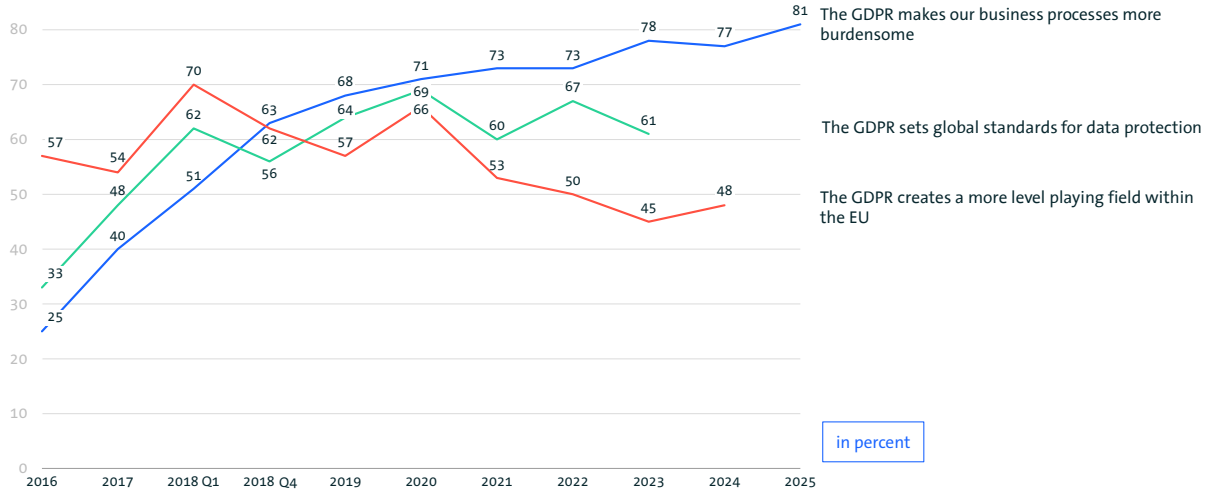
Implementing the GDPR is not a completed project for companies, but an ongoing aspect of day-to-day business operations. Despite increasing experience in data protection compliance, the perceived level of effort has not declined — quite the opposite. The share of companies reporting an increase in effort since the introduction of the GDPR rose from 71 percent in 2020 to 84 percent in 2024. At the same time, the proportion of companies stating that the effort had remained the same or decreased fell from 28 percent to just 16 percent.

The figures show that greater maturity in data protection does not automatically result in relief for companies. On the contrary, the practical implementation of the GDPR often leads to increasing requirements relating to documentation, processes, contracts, technical and organisational measures, and the continuous assessment of new legal and technological developments. As a result, data protection compliance is becoming more professionalised while remaining highly resource-intensive.

The current assessment of the effort associated with data protection further underlines this trend: in 2025, a total of 97 percent of companies rated the effort required for data protection compliance as high, with 44 percent describing it as "very high" and 53 percent as "fairly high" ↗Study report "Data Protection in the German Economy".

1.3 Perceptions of the GDPR since 2016

To what extent do you agree with the following statements about the GDPR?



Base: All surveyed companies with 20 or more employees | Responses "Strongly agree" and "Somewhat agree" combined | In 2016 and 2017, the statement read: "... will make our business processes more complex" | Source: Bitkom Research

Figure 3: Statements on the Effort Caused by the GDPR (2016-2025)

Data protection is increasingly perceived as a source of complexity

Companies increasingly perceive the GDPR as a factor that makes business processes more burdensome. Even before it became applicable, a growing share of companies expected the new Regulation to increase complexity. In 2016, 25 percent agreed with this statement, rising to 51 percent by the first quarter of 2018. Following the GDPR's entry into application in May 2018, the figure increased significantly, reaching 63 percent in the second quarter of 2018. Since then, this perception has become increasingly entrenched. By 2025, 81 percent of companies stated that the GDPR makes their business processes more burdensome.

At the same time, the GDPR has for many years been regarded as an international benchmark for data protection regulation. Between 2018 and 2023, at least 56 percent of companies consistently agreed with this statement, with approval peaking at 69 percent in 2020. Companies therefore fundamentally recognise the GDPR's international significance.

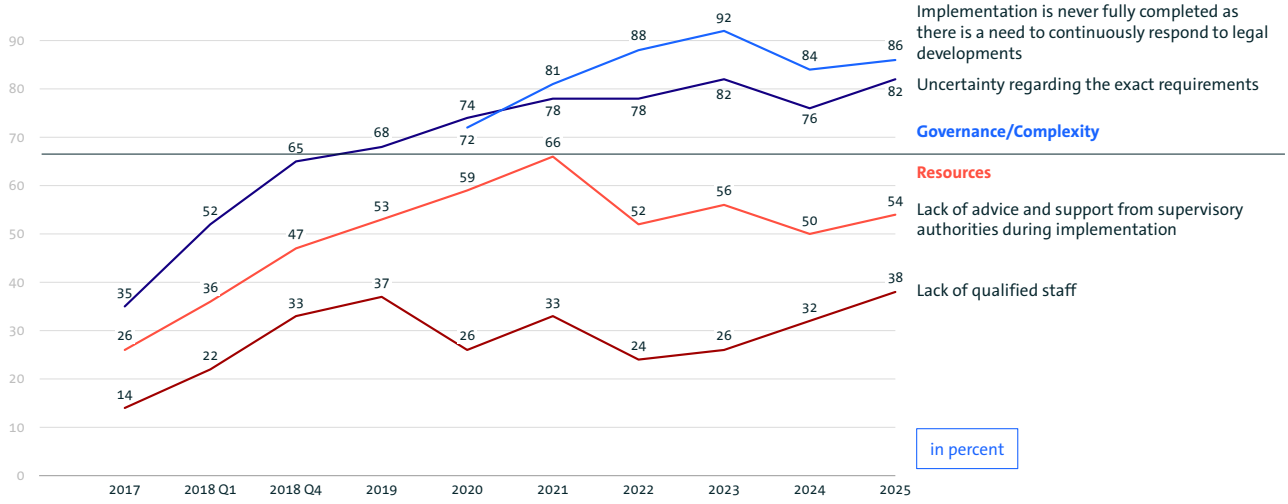
Assessments of the GDPR's impact within the EU are more mixed. Initially, the GDPR was strongly associated with more level competitive conditions across the EU: 70 percent agreed with this statement in the first quarter of 2018 and 63 percent in the second quarter. In the years that followed, however, agreement declined significantly, falling to just 48 percent by 2024. This suggests that while companies recognise the general benefits of a harmonised European data protection framework, in practice they continue to perceive differences in implementation, legal uncertainty and considerable compliance effort.

Overall, the findings show that, from the perspective of many companies, the GDPR remains an important regulatory framework with international influence. At the same time, in day-to-day business operations it is increasingly associated with additional complexity, increasingly burdensome processes and limited efficiency gains.

2 Challenges in Implementing the GDPR

2 Challenges in Implementing the GDPR

From your perspective, what are or have been the biggest challenges in implementing data protection requirements such as the GDPR in your company?



Base: All surveyed companies with 20 or more employees | Item "Implementation is never truly complete" not surveyed between 2017 and 2019 | Multiple responses possible | Source: Bitkom Research

Figure 4: Biggest challenges in implementing data protection regulations

Complexity remains high, while challenges are shifting

The greatest challenges companies face in relation to data protection continue to lie in the management, organisation and ongoing adaptation of their data protection processes. This is particularly evident in companies' assessment that GDPR implementation is never truly complete, as organisations must continuously respond to technological and legal developments. This figure already stood at 72 percent in 2020, rose to 92 percent by 2023 and remained at a very high level of 86 percent in 2025. Data protection is therefore clearly perceived as a permanent task rather than a one-off implementation project.

Uncertainty regarding the precise requirements also remains a major challenge. Even before the GDPR became applicable, this uncertainty increased significantly — from 35 percent in 2017 to 65 percent in the second quarter of 2018. Since then, the figure has remained consistently high, reaching 82 percent again in 2025. This demonstrates that, even after years of practical experience, considerable difficulties remain in interpreting and applying data protection requirements.

At the same time, the nature of resource-related challenges is changing. A lack of guidance and support from supervisory authorities was cited particularly frequently as a challenge during the first years following the introduction of the GDPR. The figure rose from 26 percent in 2017 to 66 percent in 2021. Since then, it has declined, but at 54 percent in 2025 it remains a significant issue. At the same time, the shortage of qualified staff is once again becoming more important. Following fluctuating figures in previous years, 38 percent of companies cited a lack of skilled personnel as a challenge in 2025 — the highest level in the time series. The findings therefore point to a shift in priorities. In addition to external guidance and clearer regulatory requirements, internal resources, expertise and data protection know-how are increasingly becoming the focus of attention.

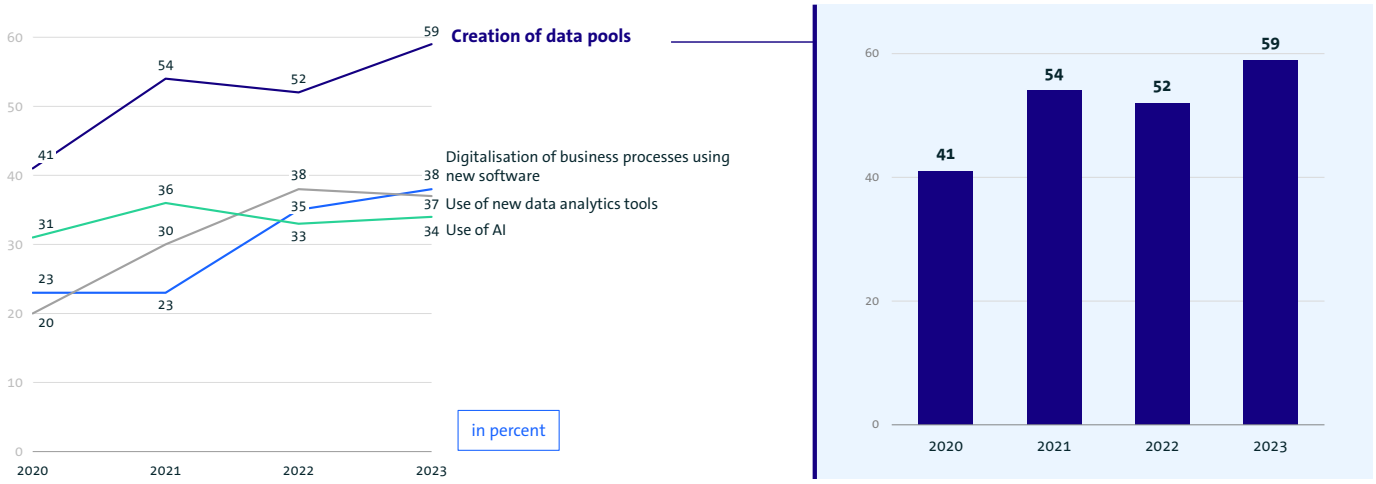
Overall, the findings show that the challenges associated with data protection have not diminished, but rather evolved over time. Companies must continuously monitor legal developments, interpret regulatory requirements, adapt internal processes and ensure the availability of sufficiently qualified personnel.

3 Innovation vs. Data Protection

3 Innovation vs. Data Protection

3.1 Data Protection Requirements and Failed Innovation Projects

In the past 12 months, have there been cases in which innovative projects in your company were abandoned or not initiated due to data protection requirements?



Base: All surveyed companies with 20 or more employees | Responses "Yes – due to specific GDPR requirements" and "Yes – due to uncertainty in dealing with GDPR requirements" combined | Source: Bitkom Research

Figure 5: Failure of innovative projects due to data protection regulations

Data protection requirements are increasingly perceived by companies as an obstacle to data-driven innovation projects. This is particularly evident in the creation of data pools. In 2020, 41 percent of companies reported that such projects had failed due to data protection requirements or had not been pursued at all. By 2025, this figure had risen to 59 percent.

The share of affected companies also remains high across other digital and data-driven initiatives. In the digitalisation of business processes using new software, the figure increased from 23 percent in 2020 and 2021 to 38 percent in 2023. A significant increase can also be observed in relation to the use of new data analytics tools — from 20 percent in 2020 to 37 percent in 2023. Regarding the use of artificial intelligence, the proportion has consistently remained at a high level of between 31 and 36 percent since 2020.

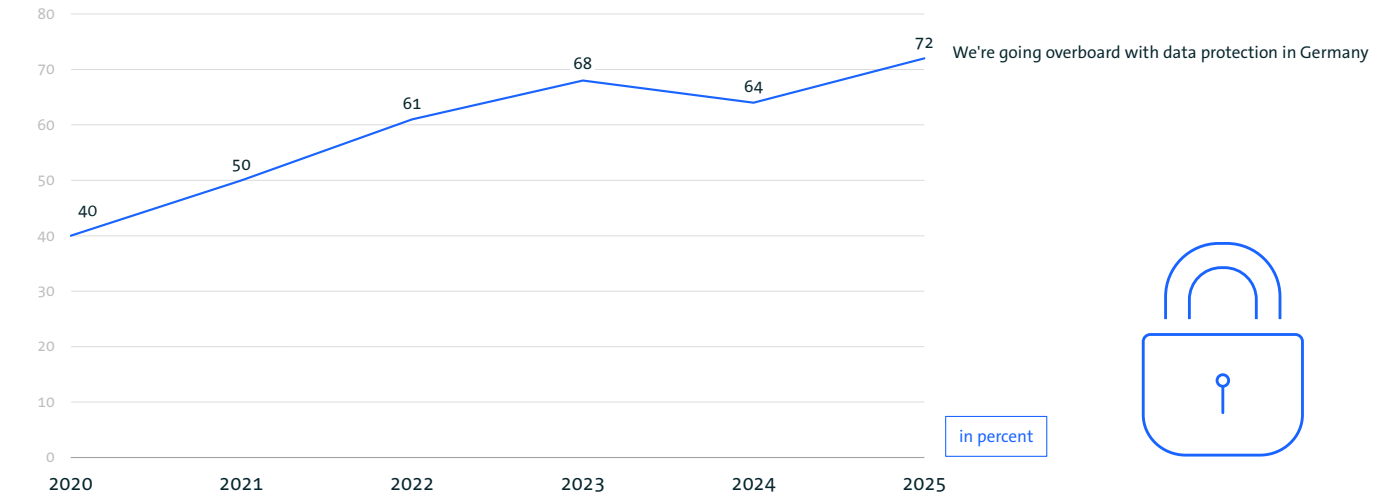
The findings show that data protection requirements are increasingly perceived as a barrier to innovation, particularly where new business models, more efficient processes or AI applications depend heavily on the large-scale use of data. The issue is therefore less about individual project types than about a broader structural tension. Companies want to make greater use of data, but in practice they frequently encounter legal uncertainty, documentation obligations and extensive requirements relating to consent, purpose limitation and data minimisation.

As a result, data protection is increasingly becoming a factor affecting both competitiveness and innovation. The more economic value creation depends on data, the more important it becomes to implement data protection requirements in a legally certain, practical and innovation-friendly manner.

3.2 Majority sees Overregulation in Data Protection

To what extent do you agree with the following statement?

”We’re going overboard with data protection in Germany”



Base: All surveyed companies with 20 or more employees | Combined figures for ”Strongly agree” and ”Somewhat agree” | Source: Bitkom Research

Figure 6: Perception of Privacy Regulation

The perception that data protection is excessively regulated in Germany has increased significantly in recent years. In 2020, 40 percent of companies agreed with the statement that «we are going overboard with data protection in Germany”. By 2025, this share had risen to 72 percent — the highest level recorded to date.

Particularly striking is the sharp increase between 2020 and 2023. Within just three years, agreement rose from 40 percent to 68 percent. Following a slight decline to 64 percent in 2024, the figure increased significantly again in 2025. This suggests that the perception that data protection regulation in Germany is excessive has not only become more established, but has further intensified.

This finding is consistent with the broader pattern observed in the previous results: companies increasingly perceive data protection requirements as complex, burdensome and restrictive to innovation. The high level of agreement with the statement regarding excessive data protection therefore reflects less a fundamental rejection of data protection itself and more growing criticism of the practical design, interpretation and implementation of the regulatory framework in Germany.

4 Supervisory Authorities

4 Supervisory Authorities

Supervisory authorities play a key role for companies in the practical implementation of data protection requirements.

The use of, or requests for, support from supervisory authorities has remained at a high level for several years. In both 2022 and 2023, 82 percent of companies reported having sought or used support from supervisory authorities, while the figure stood at 80 percent in 2024. This demonstrates that the demand for guidance, interpretative assistance and practical support remains high, and that supervisory authorities are regarded as important points of contact.

At the same time, the support received is viewed critically. In 2023, only 36 percent of companies stated that they were satisfied with the support they had received, while 63 percent were dissatisfied. Dissatisfaction also predominated in previous years, standing at 66 percent in 2021 and 56 percent in 2022. Increased use of support services therefore does not automatically translate into higher levels of satisfaction. Instead, a clear tension emerges: companies are increasingly seeking support, but often do not perceive it as sufficiently practical or helpful for implementation.

A closer look at the assessment of individual aspects reinforces this picture. On the positive side, the guidance provided is generally perceived as constructive and approachable. In 2023, 59 percent of companies agreed with this statement, compared with 65 percent in 2022. Processing speed has also improved compared with 2021. At that time, 29 percent stated that their request had been handled promptly; by 2023, this figure had risen to 41 percent. Nevertheless, the overall results remain cautious. Particularly notable is the decline in the share of companies reporting that they had access to a competent contact person at the supervisory authority — from 47 percent in 2021 to 38 percent in 2023.

The support provided by supervisory authorities appears to offer only limited assistance for data-driven innovation projects. In 2023, 34 percent of companies stated that they had been able to implement innovative, data-driven projects more quickly with the support of supervisory authorities. While this represents an increase compared with 27 percent in 2021, it remains below the 40 percent recorded in 2022. Particularly in light of the widespread perception of data protection requirements as an obstacle to data pools, data analytics and AI projects, this finding suggests that companies expect supervisory authorities to provide more practical and innovation-friendly guidance.

The reasons why companies do not seek or use support have also changed over time. Traditional barriers to access are becoming less significant. The share of companies unaware that support was available declined from 26 percent in 2021 to just 7 percent in 2024. Fear of dealing with supervisory authorities also decreased significantly — from 18 percent in 2021 to 8 percent in 2024. This points to increased visibility of support services and a decline in general apprehension. At the same time, however, qualitative concerns are becoming more important. The proportion of companies rating the quality of the support provided as inadequate rose from 25 percent in 2021 to 44 percent in 2024. At the same time, 25 percent of companies in 2024 stated that they had heard about negative experiences from other companies — the highest figure in the time series.

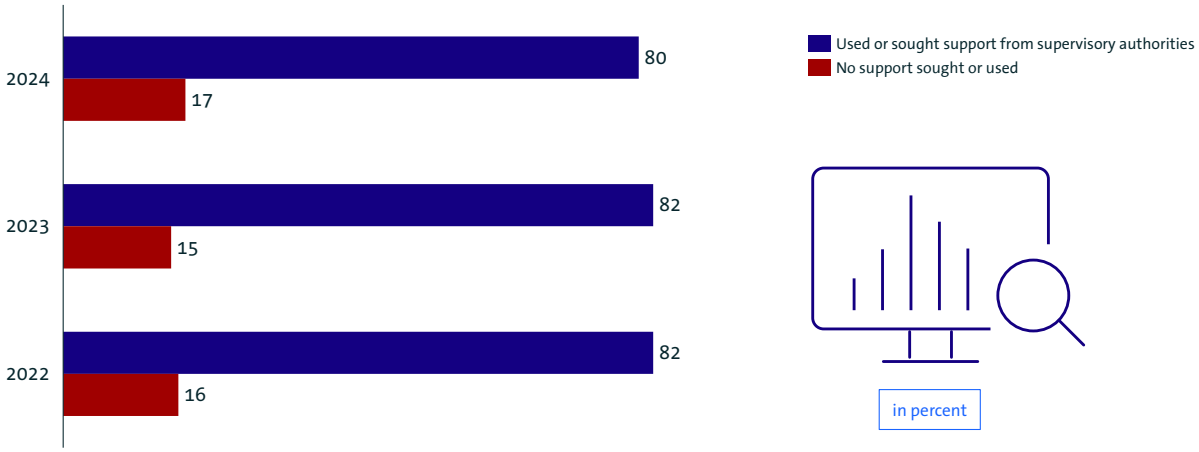
Although the perception that supervisory authorities are not interested in finding practical solutions declined from 34 percent in 2021 to 24 percent in 2024, a considerable proportion of companies remain sceptical about the practical value of the support provided.

Overall, the findings paint an ambivalent picture: supervisory authorities are increasingly being used as sources of support, yet many companies believe that the assistance provided does not meet their expectations. The focus is shifting away from a lack of awareness or fear of authorities and increasingly towards concerns regarding quality, practical relevance and solution-oriented guidance.

For the continued implementation of the GDPR — and especially for data-driven innovation — it is essential that supervisory authorities are perceived not only as enforcement bodies, but increasingly as reliable, competent and practical partners for guidance and orientation.

4.1 Utilisation of Support from Supervisory Authorities

Have you sought or used support from supervisory authorities in recent years in order to implement data protection requirements?

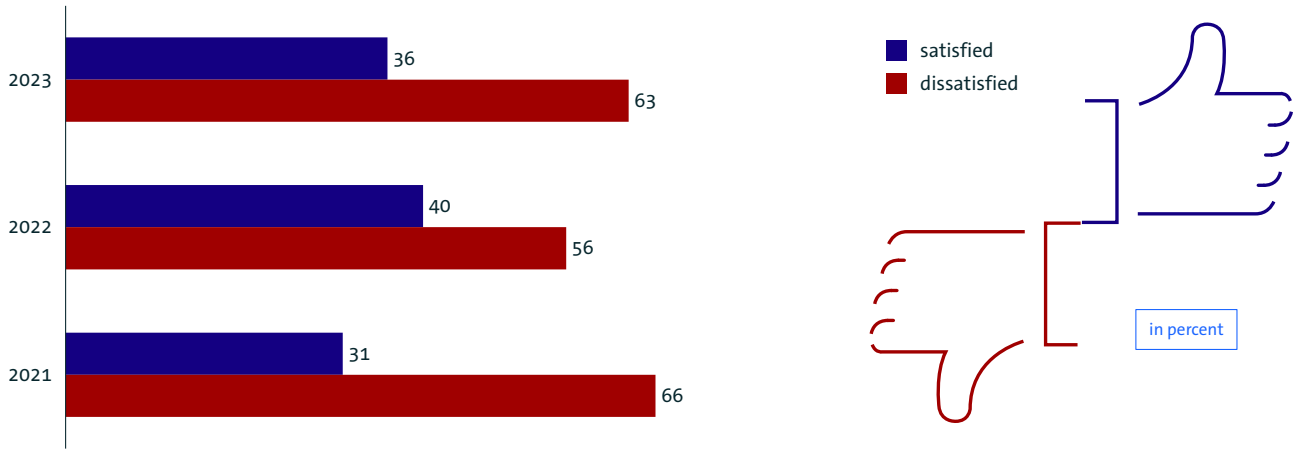


Base: All surveyed companies with 20 or more employees | Source: Bitkom Research

Figure 7: Use of Regulatory Authorities' Support

4.2 Satisfaction with Support from Supervisory Authorities

How satisfied are you with the support your company has received?

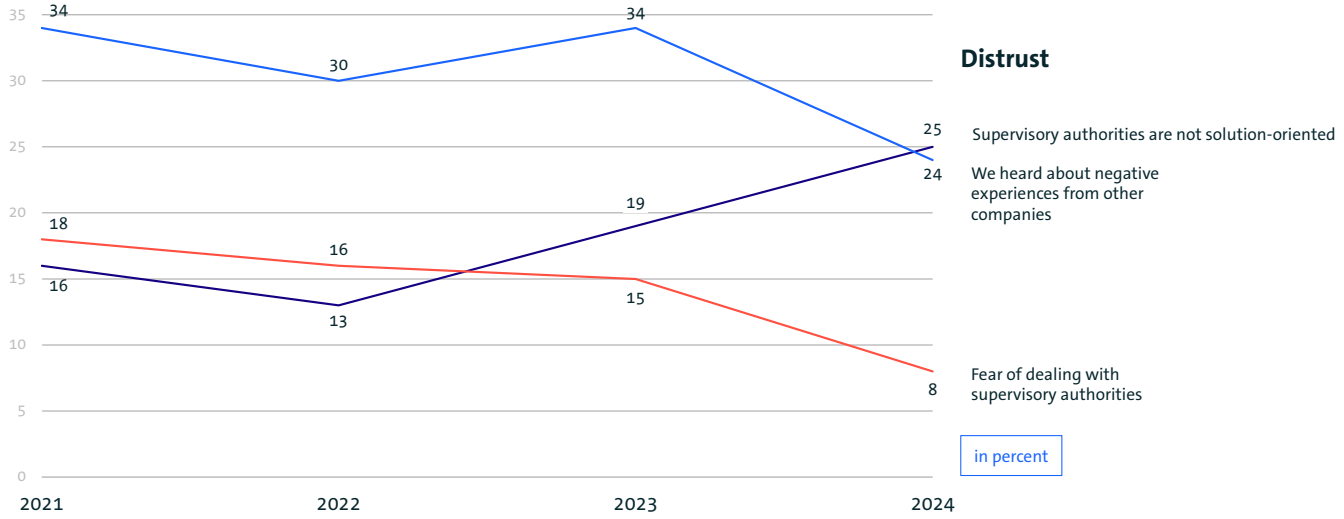


Base: Surveyed companies with 20 or more employees that have used support from supervisory authorities | Totals may not equal 100 per cent due to rounding | "Don't know/no answer" responses not shown | Source: Bitkom Research

Figure 8: Satisfaction with assistance from regulatory authorities

4.3 Distrust of Supervisory Authorities

Why did you not seek or use support from supervisory authorities?

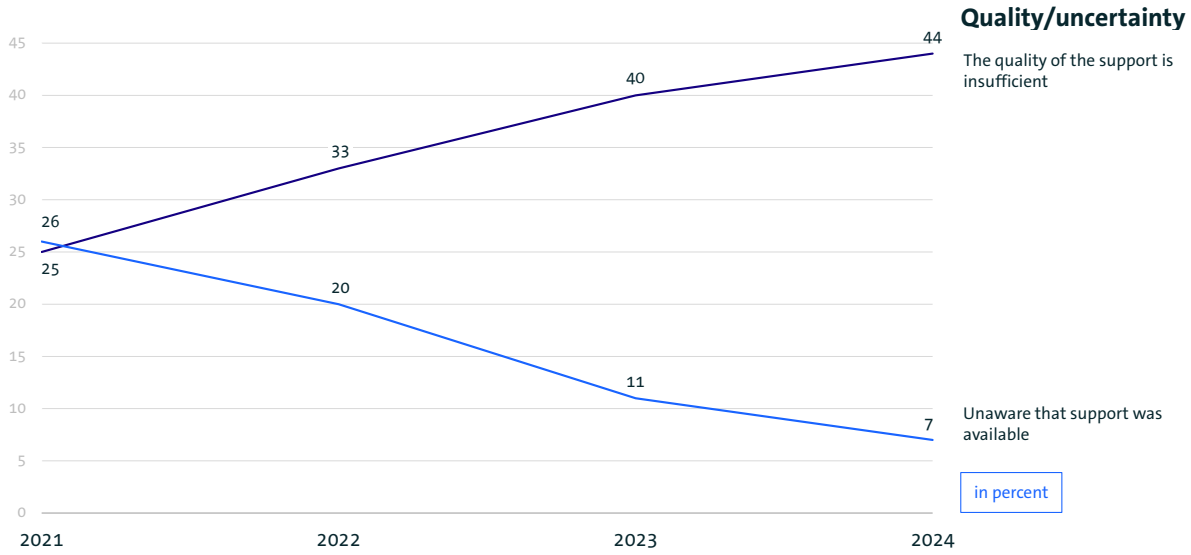


Base: Surveyed companies with 20 or more employees that did not seek or use support from supervisory authorities | Multiple responses possible | Source: Bitkom Research

Figure 9: Reasons for not using assistance: Distrust

4.4 Supervisory Authorities: Quality and Legal Uncertainty

Why have you not sought or used support from supervisory authorities?

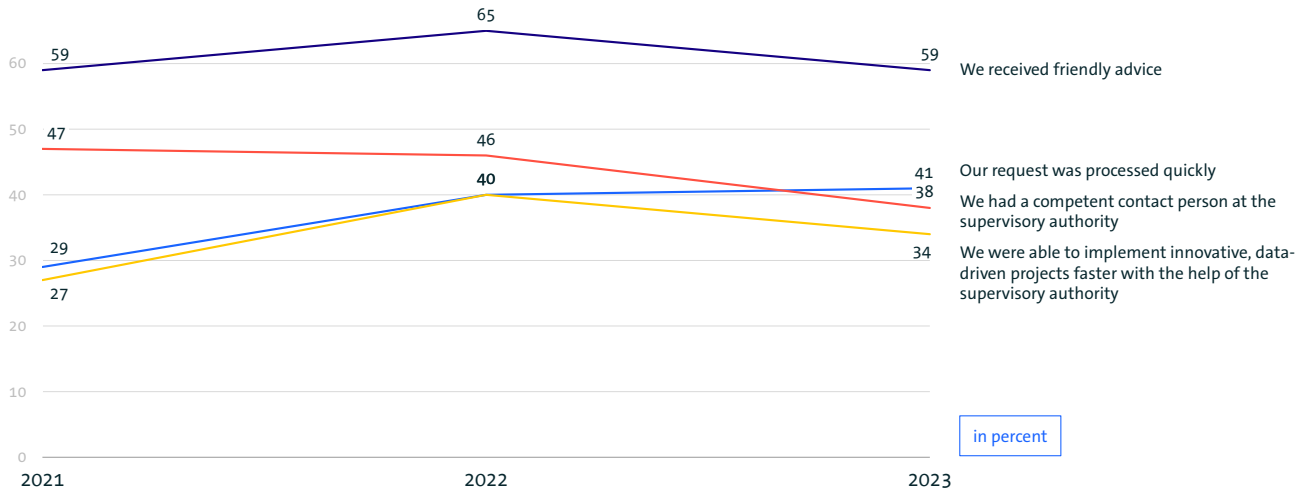


Base: Surveyed companies with 20 or more employees that did not seek or use support from supervisory authorities | Multiple responses possible | Source: Bitkom Research

Figure 10: Reasons for Not Using Assistance: Quality/Unclarity

4.5 Assessment of Support Provided by Supervisory Authorities

To what extent do you agree with the following statements regarding the support your company received from supervisory authorities?



Base: Surveyed companies with 20 or more employees that received support from supervisory authorities | Combined figures for "Strongly agree" and "Somewhat agree" | Source: Bitkom Research

Figure 11: Evaluation of the guidance provided by regulatory authorities

5 International Data Transfers

5 International Data Transfers

International data transfers remain an integral part of business operations for many companies.

This is particularly evident in relation to the United States. In 2021, 52 percent of companies transferred personal data there; by 2023, this figure had risen to 64 percent, before standing at 61 percent in 2025. The United States therefore remains by far the most important third country for transfers of personal data outside the EU.

The United Kingdom has also become increasingly important as a third country following Brexit. The share of companies transferring personal data there rose from 35 percent in 2021 to 43 percent in 2025. India likewise recorded a significant increase, rising from 13 percent in 2021 and 2022 to 24 percent in 2025.

The findings show that, despite ongoing debates surrounding digital sovereignty and legal uncertainty, international data flows are not declining. Companies remain deeply integrated into globally interconnected value chains, cloud infrastructures, software ecosystems and international service relationships. As a result, the need for reliable, legally certain and practical frameworks for international data transfers is becoming increasingly important.

Standard Contractual Clauses (SCCs) remain the primary legal basis for transfers of personal data to the United States. Their use has remained consistently high since 2016 and, in 2025, 80 percent of companies reported relying on them. Although this represents a decline compared with 2023, when 94 percent of companies used SCCs, they continue to be by far the most important mechanism for transfers to the United States. This reflects the role of SCCs as a pre-approved transfer mechanism for data transfers to countries outside the European Economic Area (EEA).

The EU–US Data Privacy Framework established a new legal basis for transfers to the United States in 2025, but it has not yet achieved the practical significance previously held by the Privacy Shield. While the Privacy Shield was used by 42 percent of companies in 2019, the EU–US Data Privacy Framework stood at 21 percent in 2025. This suggests that many companies continue to rely on established instruments such as SCCs despite the new adequacy decision — possibly because the Framework applies only to participating or certified US companies. Other legal bases also continue to play a role, although to a significantly lesser extent.

Binding Corporate Rules (BCRs) were used by 23 percent of companies in 2025, representing a decline compared with previous years. Consent as a legal basis was cited by 12 percent of companies in 2025, roughly in line with the level recorded in 2021. Overall, the findings show that the legal framework governing transfers to the United States remains fragmented. Companies continue to combine different transfer mechanisms, although SCCs remain the backbone of practical implementation.

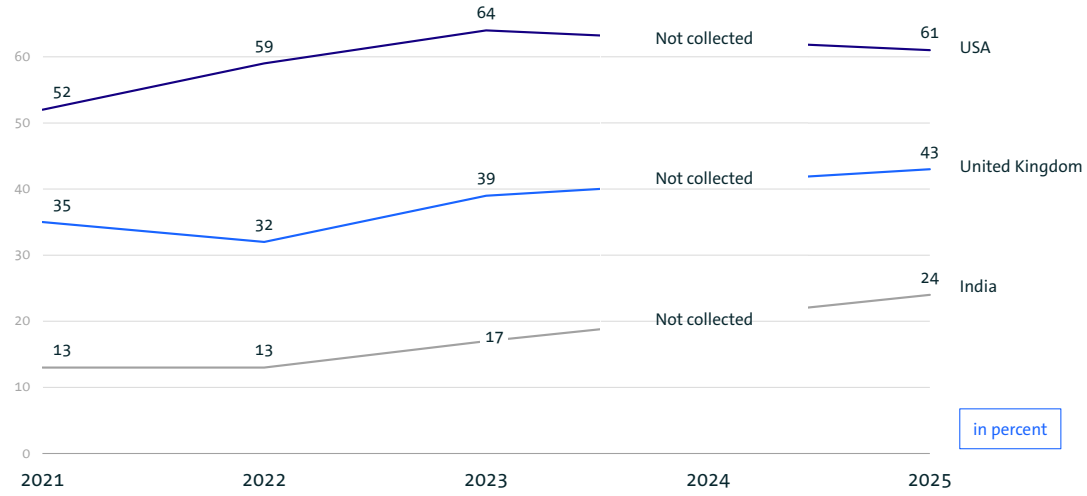
At the same time, political pressure is increasing significantly. The share of companies calling for policymakers to establish sustainable political solutions for international data transfers rose from 32 percent in 2021 to 71 percent in 2025.

Companies are therefore increasingly viewing international data transfers not merely as a compliance issue, but as a strategic issue affecting competitiveness and business location attractiveness.

Overall, the findings reveal a clear area of tension: international data flows remain indispensable for modern business operations, while their legal safeguarding continues to be perceived as complex and legally uncertain.

5.1 International Data Transfers Outside the EU

To which non-EU countries does your company transfer personal data?

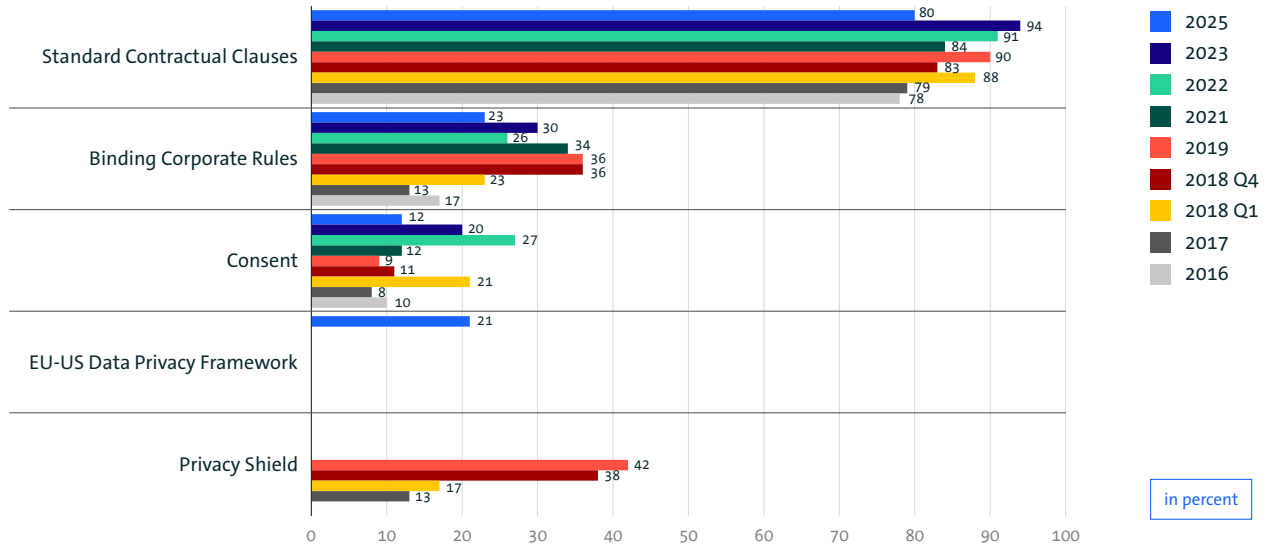


Base: Companies with 20 or more employees that transfer personal data outside the EU | Multiple responses possible | Source: Bitkom Research

Figure 12: International Data Transfers Outside the EU

5.2 Legal Bases for Data Transfers to the United States

On what legal basis does your company currently transfer personal data to the United States?

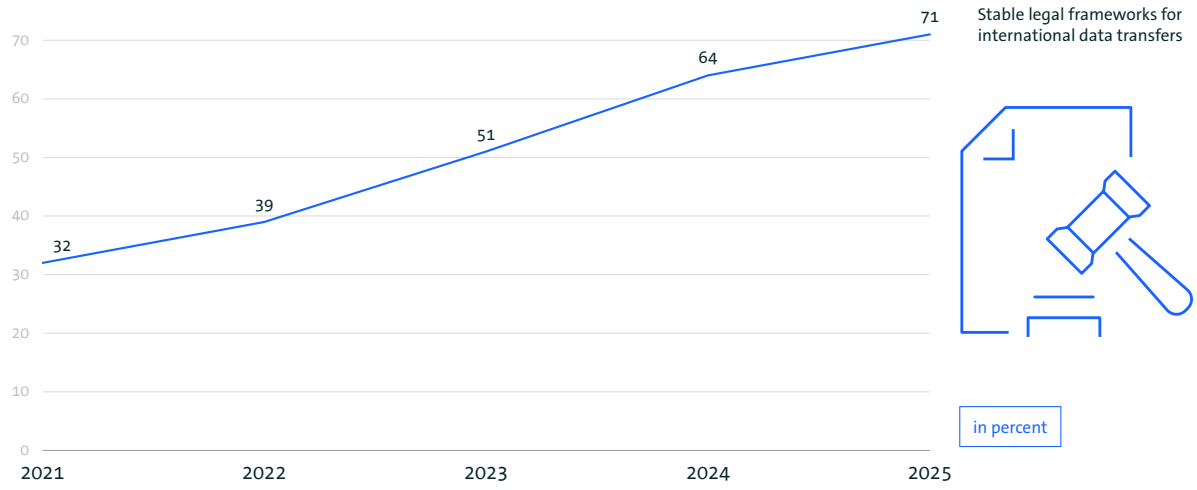


Base: Surveyed companies with 20 or more employees that transfer personal data to the United States | Multiple responses possible | Source: Bitkom Research

Figure 13: Legal Basis for Data Transfers to the USA

5.3 International Data Transfers: Expectations for Policymakers

What measures do you expect policymakers to take regarding data protection?



Base: Surveyed companies with 20 or more employees | Multiple responses possible | Source: Bitkom Research

Figure 14: Expectations of politics concerning international data transfer

6 GDPR and Artificial Intelligence

6 GDPR and Artificial Intelligence

European data protection is increasingly perceived as an advantage — while at the same time creating challenges for the practical development and deployment of AI. The relationship between data protection and artificial intelligence therefore presents a mixed picture.

On the one hand, a growing number of companies view European data protection rules as an advantage for AI development in Germany and Europe compared with international standards. The share increased from 48 percent in 2023 to 53 percent in 2024 and reached 59 percent in 2025.

At the same time, the proportion of companies perceiving European data protection as a disadvantage declined from 46 percent in 2023 to 36 percent in 2025.

At first glance, this suggests that companies increasingly regard European data protection as a differentiating factor. Data protection can strengthen trust, increase acceptance of AI applications and serve as a mark of quality for European AI. Particularly when handling sensitive data, operating in regulated sectors or developing B2B applications, high data protection standards may represent a competitive advantage.

At the same time, further findings indicate that this potential advantage has so far only been realised to a limited extent in practice.

In 2025, 69 percent of companies stated that data protection makes it difficult to train AI models on sufficient data — a significant increase from 42 percent in 2023 and 50 percent in 2024.

Concerns regarding competitive disadvantages also remain high: in 2025, 63 percent of companies stated that data protection encourages companies developing AI to relocate outside the EU. In addition, 57 percent said that data protection restricts the use of AI within the EU. This apparent contradiction can therefore be understood as reflecting a tension between strategic expectations and practical implementation.

Many companies evidently see significant potential in European data protection as an international competitive advantage.

In the practical development of AI, however, companies often experience data protection requirements as an obstacle — for example when accessing training data, ensuring the legally compliant use of large datasets or developing data-intensive business models.

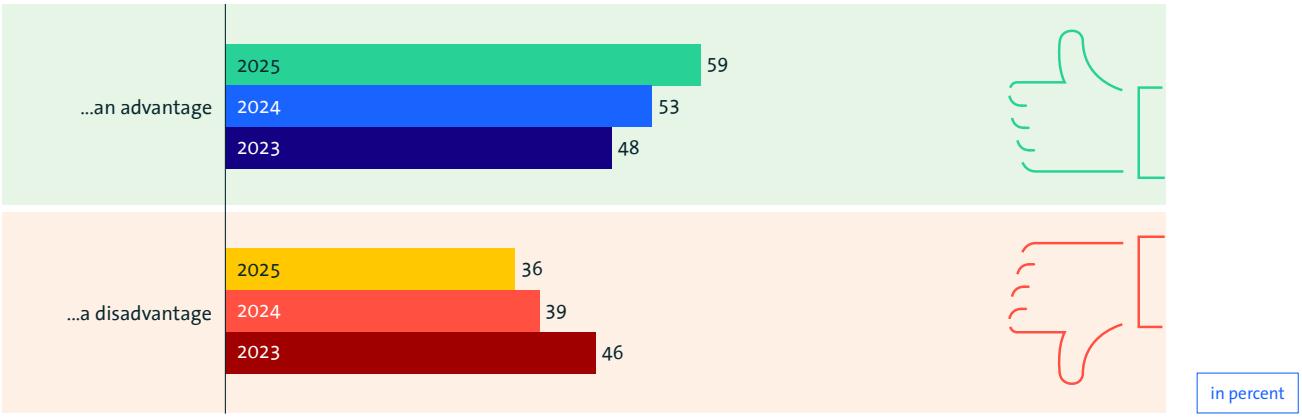
At the same time, data protection is increasingly viewed positively in relation to legal certainty. The proportion of companies stating that data protection provides legal certainty for the development of AI applications rose from 44 percent in 2023 to 58 percent in 2025. Data protection is therefore perceived not only as a burden, but also as an important framework for guidance and legal certainty.

This illustrates the central ambivalence: data protection can create trust and legal certainty, while simultaneously being perceived as a barrier to data availability, scalability and international competitiveness.

Overall, the findings show that, from the perspective of the surveyed companies, European data protection is neither clearly an advantage nor clearly a disadvantage for AI development. It is increasingly perceived as a strategic quality promise, while at the same time remaining a significant competitive factor in practical implementation.yet remains a significant competitive factor in practical application.

6.1 AI Development and European Data Protection

Compared internationally, European data protection rules are, for the development of AI in Germany and Europe, ...

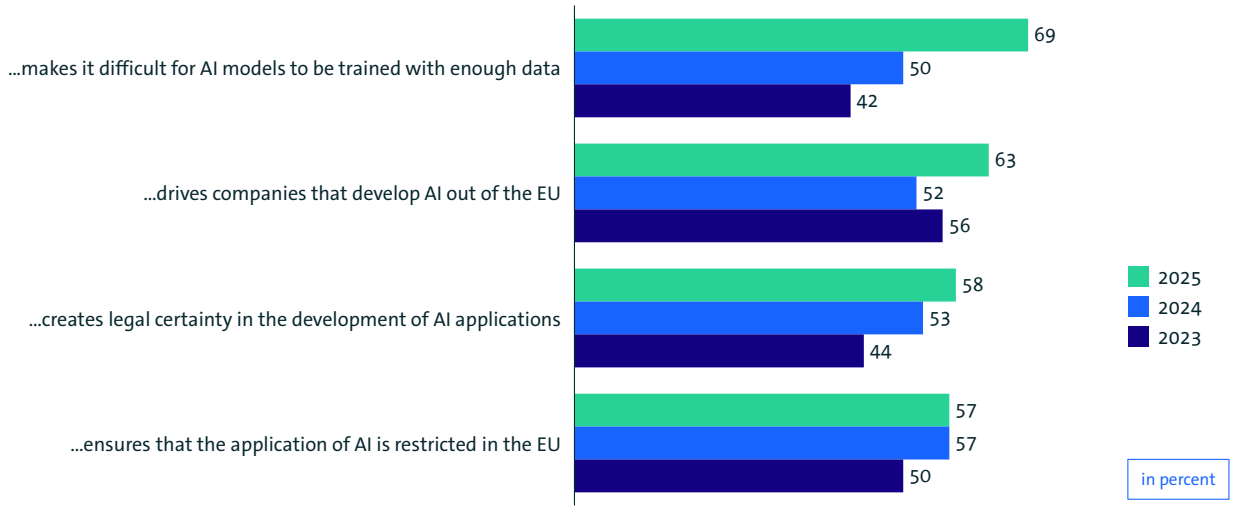


Base: Surveyed companies with 20 or more employees | Totals may not equal 100 per cent due to rounding | "Don't know/no answer" responses not shown | Source: Bitkom Research

Figure 15: AI Development and European Data Protection

6.2 Impact of Data Privacy Regulations on AI Development

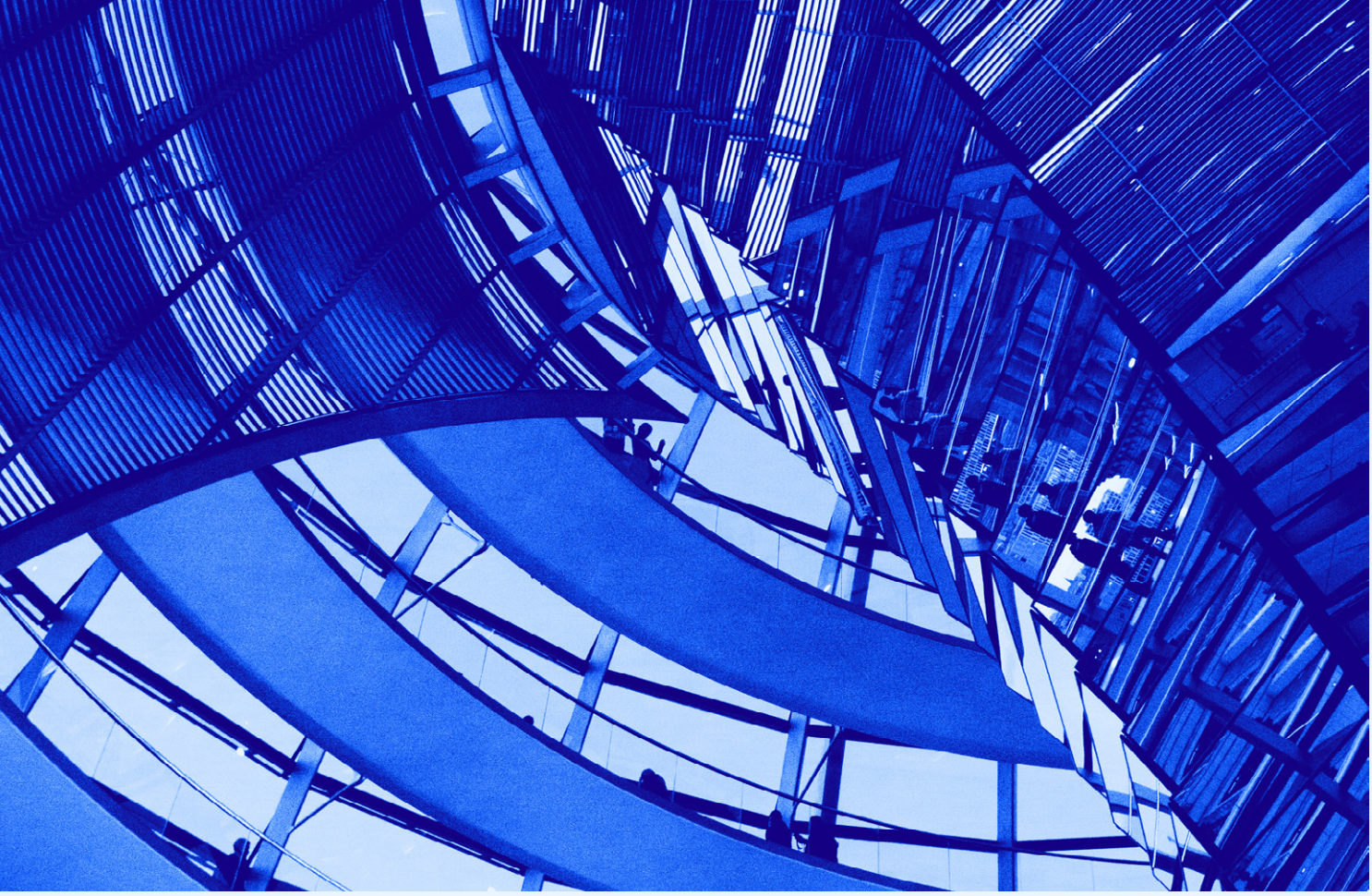
To what extent do you agree with the following statements about data protection?



Base: All surveyed companies with 20 or more employees | Combined figures for "Fully applies" and "Rather applies" | Source: Bitkom Research

Figure 16: Impact of data protection regulations on AI development

7 Reform of the GDPR



7 Reform of the GDPR

Make Data Protection Effective, Reduce Burdens on Businesses and Enable Innovation

Ten years after its adoption, the GDPR has become firmly embedded in companies' day-to-day operations. At the same time, for many businesses, implementation remains an ongoing challenge.

By 2024, 71 percent of companies reported that they had fully or largely implemented the GDPR. At the same time, perceptions regarding compliance effort, complexity and barriers to innovation remain clear. The practical application of the GDPR continues to represent a significant and ongoing challenge for businesses.

The need for reform does not arise from a single finding, but from the interaction of several developments. The effort associated with data protection compliance has increased since the introduction of the GDPR, business processes are increasingly perceived as more burdensome, the interpretation of regulatory requirements remains uncertain for many companies, and data-driven innovation projects are frequently hindered in practice. The survey findings therefore indicate where reform efforts should focus — particularly in creating greater legal certainty, strengthening risk-based approaches, reducing formal obligations for low-risk processing activities, improving conditions for data-driven innovation and ensuring more harmonised implementation of the GDPR across Europe.

The objective is not to weaken data protection as a fundamental right. On the contrary, data protection remains a key prerequisite for trust in the digital economy. However, in order to remain effective in the future, data protection rules must become more practical, more risk-based and more innovation-friendly. Reform should therefore reduce burdens where formal requirements do not provide additional protection benefits, while at the same time ensuring robust safeguards where genuinely high risks to individuals arise.

From Bitkom's perspective, the current reform approach under the Digital Omnibus addresses important issues. In particular, it is right to focus on resolving specific implementation and application problems without reopening the GDPR as a whole.

The proposed reforms can contribute to greater legal certainty, stronger harmonisation and a more risk-based application of data protection law. However, it is essential that the reform process is consistently refined throughout the legislative process so that the intended relief measures genuinely reach businesses in practice and are not undermined by vague terminology, broad exceptions or additional documentation obligations.

A central area of reform is **the consistent focus on risk**.

While the GDPR already contains risk-based elements, in practice many obligations apply largely irrespective of whether specific processing activities actually pose a high risk to individuals. This particularly affects documentation and accountability obligations, transparency requirements and internal review procedures.

For companies, this means that even low-risk standard processing activities often involve substantial formal and administrative effort. A modernised GDPR should therefore align the scope and intensity of such obligations more closely with the actual level of risk involved. This would allow resources to be focused more effectively on areas where data protection concerns are genuinely significant.

The study findings support this conclusion. When 84 percent of companies report that their data protection workload has increased since the introduction of the GDPR, and 86 percent state that implementation is never truly complete, this points to a structural and ongoing compliance burden. Reform efforts should therefore not merely adjust individual obligations, but systematically assess whether the balance between regulatory effort and actual protective benefit remains proportionate.

The need for reform is particularly evident in the context of data-driven innovation and artificial intelligence. Companies increasingly regard European data protection as a potential competitive advantage in international markets.

By 2025, 59 percent of companies stated that data protection represents an advantage for AI development in Germany and Europe. At the same time, 69 percent reported that data protection makes it difficult to train AI models on sufficient data, while 63 percent believed that data protection encourages companies developing AI to relocate outside the EU.

This tension illustrates that the objective of combining high data protection standards with trust and international competitiveness has not yet been sufficiently realised in practice.

> Data protection can become a quality feature of European AI — but only if companies are provided with legally certain and practical ways to use data for the training, development and deployment of AI systems.

There is therefore a need for **legally certain foundations for data-driven innovation**. The proposed clarification that the development and operation of AI systems can generally rely on the legal basis of legitimate interests represents an important step forward. However, this approach must apply consistently across the European Union, must not be undermined by national derogations or additional consent requirements, and should be designed in a technology-neutral manner. Data-intensive innovation is not limited to today's AI systems. Data-driven applications are also emerging in areas such as healthcare, mobility, energy, cybersecurity, public administration and product development, all of which require a clear, reliable and innovation-friendly legal framework.

More clarity is also needed regarding whether data can be considered **personal data** in a specific context. In practice, there is often uncertainty as to whether data is actually identifiable for a particular recipient or whether identification would only be theoretically possible for other actors. A **more precise and context-based interpretation of the concept of personal data** could reduce burdens on companies while ensuring that protection remains focused on genuinely relevant risks.

In addition, anonymisation, pseudonymisation and modern privacy-enhancing technologies should receive stronger legal recognition. This would create greater incentives for companies to anonymise or pseudonymise data and could thereby improve the effectiveness of data protection in practice. Such measures can significantly reduce risks for individuals, but they often involve substantial technical, organisational and legal effort for companies. In order for these investments to be worthwhile, companies require reliable criteria regarding when data is considered anonymous, under which conditions pseudonymisation is recognised as a risk-reducing measure, and which technical procedures can be used with legal certainty.

Greater legal recognition of such protective measures would not weaken data protection; rather, it would help make data protection more effective in practice. Companies would have a clear incentive to make data processing more privacy-friendly if this also resulted in greater legal certainty and proportionate relief from subsequent compliance obligations.

Another key area for reform concerns the rules governing **cookies and access to terminal equipment**. Current practice results in an overwhelming number of consent requests without necessarily improving the level of data protection. Instead, users experience consent fatigue, while companies face considerable compliance costs. Aligning the GDPR and ePrivacy framework therefore offers an opportunity to fundamentally simplify the current system.

Low-risk processing activities — such as audience measurement, fraud prevention, IT security or context-based advertising — should not generally be subject to consent requirements. Instead, as with other processing activities, they should be capable of relying on appropriate legal bases such as legitimate interests.

Machine-readable preference signals do not solve this underlying problem. On the contrary, they risk creating additional technical and legal complexity.

International data transfers also remain a long-term political challenge. The United States continues to be the most important third country for transfers of personal data outside the EU, with 61 percent of companies transferring personal data there in 2025. At the same time, 71 percent of companies called for policymakers to establish sustainable solutions for international data transfers.

This demonstrates that global data flows are an economic reality, while their legal safeguarding remains burdensome and legally uncertain. Reform should therefore strengthen political solutions that ensure high data protection standards while also enabling international cooperation, cloud usage and digital business models.

Finally, greater **harmonisation and a stronger practical orientation in regulatory oversight** are needed.

Companies now frequently seek support from supervisory authorities. In 2024, 86 percent reported having sought or used such support. At the same time, however, the findings show that satisfaction remains limited and that concerns regarding quality and practical relevance persist.

Reform should therefore not only adjust substantive rules, but also harmonise their practical application. EU-wide criteria for data protection impact assessments, standardised reporting formats for personal data breaches and clearer guidance could all contribute to this goal — provided that such measures remain concise, understandable, practical and do not create additional bureaucracy.

Several **concrete reform priorities** can be derived from the survey results.

- First, a more consistent risk-based approach is needed so that low-risk processing activities do not trigger the same level of formal effort as high-risk processing.
- Second, clearer and more harmonised guidance is required in order to reduce legal and interpretative uncertainty.
- Third, data-driven innovation and AI development must be enabled within a legally certain framework.
- Fourth, technical safeguards such as anonymisation and pseudonymisation should receive stronger regulatory recognition and support.
- Fifth, more harmonised and practice-oriented supervision is needed, alongside sustainable political solutions for international data transfers.

Overall, the study findings show that the GDPR has firmly embedded data protection within the business community, but it has not made compliance simpler. Many companies accept data protection as an important framework for trust in the digital economy, yet regard its practical implementation as too complex, too uncertain and too burdensome.

In 2025, 72 percent of companies agreed with the statement that «we are going overboard with data protection in Germany". This criticism is directed not at data protection itself, but at an implementation practice that too often prioritises formal requirements over actual risks. Reform of the GDPR should therefore pursue three key objectives:

- greater legal certainty,
- stronger risk orientation, and
- greater capacity for innovation.

Data protection rules must remain robust where data processing poses high risks to privacy and informational self-determination. At the same time, where processing activities are low-risk, socially beneficial or economically necessary, companies require practical and proportionate flexibility.

Only in this way can the GDPR continue to create trust over the next decade while simultaneously enabling digital value creation, AI development and international competitiveness in Europe.

8 Methodology

Surveys 2016-2025 | Overall Economy

Client	Bitkom
Methodology	Computer-assisted telephone interview/Computer Assisted Telephone Interview (CATI)
Population	Companies in Germany with at least 20 employees
Target Individuals	Management, Board of Directors, Chief Information Officers or Data Protection Officers, Head of Legal Department, Lawyers or Compliance Officers
Sample Size	n=509 (2016); n=507 (2017); n=505 (2018 Q1); n=505 (2018 Q4); n=502 (2019); n=504 (2020); n=502 (2021); n=503 (2022); n=502 (2023); n=605 (2024); n=603 (2025)
Survey Period	↗Dataverse
Weighting	Representative weighting of the dataset based on the current Company Register of the Federal Statistical Office
Statistical Margin of Error	+/- 5 percent or +/- 4 percent (from 2024)

Susanne Dehmel
Member of the Executive Board for Law & Security
susanne.dehmel@bitkom.org
↗ LinkedIn

Isabelle Stroot
Head of Data Protection Law & Policy
i.stroot@bitkom.org
↗ LinkedIn

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

Scientific Direction
Bettina Lange

Contact Person
Susanne Dehmel
Isabelle Stroot
Elena Kouremenou

Editorial Team
Alissa Geffert

DOI (German version)
10.64022/2026-DGVO

Ten years after preparations for the GDPR began, data protection has become an established part of companies' organisational routines. At the same time, surveys conducted by Bitkom Research between 2016 and 2025 show that the compliance burden remains high, legal uncertainty persists, and data-driven innovation is increasingly coming under pressure. Marking the tenth anniversary of the GDPR, this report takes stock of the Regulation from a business perspective. Based on long-term survey data, it analyses the development of data protection in companies — from the implementation of regulatory requirements to the impact on innovation, international data transfers and artificial intelligence.

DOI (German version)
10.64022/2026-DSGVO

bitkom