



# **GDPR changes: Reducing bureaucracy for SMEs and SMCs**

Bitkom on the European Commission's  
consultation on the adaptation of Regulation  
(EU) 2016/679 (EU General Data Protection  
Regulation)

## At a glance

# GDPR changes: Reducing bureaucracy for SMEs and SMCs

## Initial position

In May 2025, the EU Commission proposed amendments to the GDPR to relieve small and medium-sized enterprises and small mid-caps of bureaucratic obligations. Among other things, risk-based exemptions for the documentation of processing activities and greater flexibility in rules of conduct and certifications are planned.

## Bitkom rating

The planned simplifications are an important signal for small and medium-sized enterprises. In practice, however, they clearly do not fulfil the objective of providing noticeable relief. Reforms should be more risk-based and practical – without fundamentally calling into question the stable regulatory framework of the GDPR.

## The most important takeaway

### ■ Risk-based exemption from documentation requirements

Exempting smaller companies from the obligation to keep a record of processing activities makes sense, but the term 'high risk' must be clearly defined and interpreted uniformly in order to avoid legal uncertainty.

### ■ Inclusion of small mid-caps

Excluding smaller companies from the obligation to maintain a record of processing activities makes sense, but the term 'high risk' must be clearly defined and interpreted uniformly in order to avoid legal uncertainty.

### ■ Further need for reform

Additional measures are required for real relief, such as standard templates, clearer rules on data subject requests, better integration with new EU laws, and practical guidelines instead of structural changes.

## Bitkom number

### 94 percent

of German companies describe the current data protection effort as high (according to a study by [Bitkom Research](#)).

94%

of German companies describe the current data protection effort as high (according to a study by [Bitkom Research](#))

# Content

<b>1</b>	<b>Introduction</b>	<b>4</b>
	<b>Risk-based documentation requirement: Article 30(5) GDPR</b>	<b>4</b>
	<b>Extension to small mid-caps and Articles 40 and 42 of the GDPR</b>	<b>5</b>
	<b>Limited relief in practice</b>	<b>5</b>
	<b>Employee -based approach vs. risk-based approach</b>	<b>6</b>
	<b>Further need for reform and recommendations</b>	<b>7</b>
	Reducing bureaucracy through a risk-based approach.	7
	Greater focus on actual criticality rather than company size	7
	Improving Manageability of Data Subject Requests	8
	Consents: Adjustments and Clarifications for Greater Practical Applicability	8
	Expansion of Legal Bases and Introduction of Broad Consent	8
	Better stakeholder Involvement in EDPB Guideline development	9
	Legal Certainty	9
<b>2</b>	<b>Conclusion</b>	<b>10</b>

# 1 Introduction

On 21 May 2025, the European Commission proposed initial amendments to the General Data Protection Regulation (GDPR) as part of the so-called Omnibus IV package. The aim is to reduce the administrative burden on small and medium-sized enterprises (SMEs) and small mid-caps (SMCs), thereby strengthening their competitiveness.

Bitkom welcomes the EU Commission's efforts to reduce bureaucracy and implement a risk-based approach in the GDPR. Relieving smaller organisations of certain documentation obligations, provided their data processing does not entail a high risk, is a step in the right direction. However, it is only a very small step with limited effect. This can therefore only be the beginning.

## **Risk-based documentation requirement: Article 30(5) GDPR**

Specifically, the Commission's proposal states that companies with fewer than 750 employees will be exempt from the obligation to maintain a record of processing activities under Article 30 of the GDPR. However, this exemption will not apply to companies that carry out processing operations likely to pose a 'high risk' to the rights and freedoms of data subjects. This extends the previous blanket exemption for SMEs with fewer than 250 employees.

Bitkom fundamentally supports this risk-based approach. Exempting smaller companies from certain bureaucratic obligations is a positive step, provided the specific data processing operations do not pose any significant data protection risks. This frees up resources for investment in innovation and growth.

However, it is important that the term 'high risk' is clearly defined and interpreted uniformly. The planned reference to Article 35 of the GDPR suggests that the focus is on processing activities that require a data protection impact assessment.

Nevertheless, it is unclear whether a single high-risk processing operation would necessitate maintaining the entire register, or if only this specific activity would require documentation. The wording of the regulation should be clarified to avoid legal uncertainty.

Otherwise, the new provision risks becoming ineffective. Many companies, including those with fewer than 750 employees, have at least a few 'high-risk' processes. They would therefore still have to keep a record of their processing activities, greatly limiting the scope of the relief. Companies would still need to collect and evaluate information on their processing operations to determine whether their activities pose a high risk. This largely corresponds to the status quo and only marginally reduces bureaucracy.

Furthermore, it should be noted that, in their role as controllers in complex data processing networks (e.g. outsourced services or data supply chains), larger companies will continue to require comprehensive documentation from their service providers and partners, even if they fall below the threshold. This is in order for the larger

companies to fulfil their own accountability obligations under Article 5(2) of the GDPR. In practice, this could significantly undermine the intended relief for SMEs and SMCs and even lead to the indirect continuation of documentation obligations.

## **Extension to small mid-caps and Articles 40 and 42 of the GDPR**

Bitkom expressly welcomes the fact that the exemption provision in Article 30(5) of the GDPR will apply to small mid-caps as well as traditional SMEs in future. These companies, which are defined as firms with up to 750 employees, an annual turnover of no more than €150 million, and a balance sheet total of no more than €129 million, often outgrow their SME status yet are not yet considered to be large enterprises. Therefore, it is logical to grant them similar relief to that granted to SMEs, given that they face comparable challenges in many cases.

In addition, Article 40 of the GDPR (codes of conduct) should be amended to ensure that the specific needs of SMEs are considered when developing industry codes of conduct in future. Bitkom welcomes this and points out that the codes of conduct approved by the supervisory authorities do not currently offer sufficient legal certainty, as they are not legally binding. Class actions and individual court rulings can call these codes into question, leading to years of legal uncertainty. There is a fundamental need for the legal upgrading of approved rules of conduct. Those who comply with them should at least be protected from heavy fines and claims for damages. As a rule, compliance with the codes of conduct should give rise to a presumption of legality. Regarding Article 42 of the GDPR (certification) it should be noted here that data protection certification mechanisms and seals should be tailored to the situation of SMEs. This will ensure that new compliance tools, such as codes of conduct and certificates, are designed to be practical and manageable for medium-sized companies.

In the past, such instruments often focused on large companies or traditional SMEs. Bitkom welcomes the fact that the intermediate group of small mid-caps is now explicitly included.

## **Limited relief in practice**

Despite these positive approaches, Bitkom points out that these are relatively minor changes that will only provide limited relief for companies in practice. The planned relaxation of the documentation requirement only applies in cases where there is no high-risk data processing, which is unlikely to be the case in most instances, as explained above. Many companies that formally fall below the 750-employee threshold will nevertheless have to keep a record of processing activities due to the nature of their data processing.

In addition, GDPR compliance involves more than just maintaining a record of processing activities.

The truly time-consuming obligations, such as detailed mapping of all processing operations, creating a Data Protection Impact Assessment (DPIA) and ongoing review

of technical and organisational measures, remain unchanged. Even if no formal record of processing activities is required for low-risk operations, companies must continue to fulfil these tasks in order to meet the requirements of the GDPR.

Overall, the proposed amendments fall short of expectations. Companies had hoped for more comprehensive simplifications, such as standard templates for common processing activities and clearer guidelines for low-risk processes.

While the selective adjustments proposed are welcome, they are insufficient to significantly reduce data protection bureaucracy.

A key problem is that all companies are currently bound by numerous data protection obligations. In addition to the record of processing activities, these include extensive documentation requirements, such as logging consents and contracts for order processing, as well as reporting obligations, such as the mandatory notification of supervisory authorities and data subjects in the event of a data breach.

Processing requests for information and other data subject requests pursuant to Art. 15 et seq. GDPR also requires considerable personnel resources, particularly when a high volume of requests are received, complex data collections must be searched or requests for information are asserted as ancillary claims, for example in the context of dismissal protection proceedings. Furthermore, confirming the identity of the person making the request and protecting the personal data of third parties that may be mixed with the personal data of the person who made the request presents practical challenges. While these obligations remain unaffected by the current proposal, they place an enormous burden on companies in their day-to-day operations.

High documentation costs, for example for the processing activities register or data protection impact assessments, tie up resources that companies urgently need for innovation and digital transformation. Against this backdrop, it is clear that more far-reaching measures are required than the selective adjustments proposed.

However, Bitkom also points out that, although the planned relief measures are tailored to SMEs and SMCs, larger companies face many of the same data protection challenges. Companies with complex data processing operations, particularly those in highly regulated sectors such as healthcare and Industry 4.0, have similar needs for administrative relief and legal clarity. Any targeted reform should therefore focus on the entire SME sector. While we recognise the importance of relief for SMEs, other companies should not be excluded. Reforms should apply to all companies within the scope of the GDPR, as limiting them exclusively to SMEs would pose risks to the supply chain and to accountability.

## **Employee -based approach vs. risk-based approach**

Bitkom is critical of the rigid focus on employee numbers as a criterion for simplification. While the planned increase in the threshold to 750 employees may suit many growing companies, this criterion is inadequate.

Company size does not automatically correlate with data protection risk. For example, a company with 50 employees may process highly sensitive personal data on a large

scale, thereby posing a high risk, while a company with 500 employees may only carry out minor, routine data processing. Therefore, the rigid threshold of 750 employees appears arbitrary and inappropriate.

Bitkom recommends focusing more on the type of data processing and associated risks than on company size. A genuine risk-based approach would involve reducing obligations where the risk of a particular data processing activity is low, regardless of a company's size.

Furthermore, the term 'likely high risk' requires clarification. The definition of what constitutes high risk under Article 35 of the GDPR should be as clear as possible and based on objective criteria. Legal clarification would be welcome, for example in the form of specific examples, to specify when it is necessary to keep a record of processing activities even if the threshold is not reached. Without such clarification, there is a risk of differing interpretations across Member States, which would undermine the desired reduction in burden as companies would face legal uncertainty and numerous enquiries from authorities once again.

## **Further need for reform and recommendations**

Bitkom sees the Commission's proposals as a step in the right direction, but only as a beginning. To provide targeted relief for companies, further adjustments to the GDPR and its implementation are necessary. From the perspective of the digital economy, the following points should be addressed in particular:

### **Reducing bureaucracy through a risk-based approach.**

A consistent, risk-based approach to data protection is a key starting point for reducing the burden on companies. Obligations should be reduced for data processing activities that pose only a low risk to the rights and freedoms of data subjects. This would allow small and medium-sized enterprises (SMEs), and small mid-caps (SMCs) in particular, to allocate their human and financial resources more effectively towards innovation and growth. At the same time, a targeted focus on risky processing operations would maintain the high level of data protection.

### **Greater focus on actual criticality rather than company size**

In our view, it is insufficient to focus solely on company size, for example by setting a threshold of 750 employees. Company size is not a reliable indicator of actual data protection risk. Smaller companies can process sensitive data on a large scale, while larger companies may carry out low-risk processes routinely. Bitkom therefore recommends aligning the requirements more closely with actual data processing activities. The decisive factor should be whether a specific processing activity poses a risk to the rights and freedoms of data subjects. All companies – regardless of their size – should be exempt from administrative compliance requirements for low-risk processing operations without such implications. This would better reflect the actual protection needs of data subjects and enable more targeted relief.



## **Improving Manageability of Data Subject Requests**

Processing data subject requests, particularly access requests under Article 15 of the GDPR, involves considerable effort for many companies. Complex data structures, high case volumes, and abusive requests often result in disproportionate burdens in practice. Bitkom therefore supports measures that make it easier to deal with manifestly unfounded or excessive requests. This could be achieved through legal clarifications, deadlines, limits, or standardized processes, without weakening the overall rights of data subjects.

## **Consents: Adjustments and Clarifications for Greater Practical Applicability**

In practice, consent has often become the default mechanism for legitimising data processing, even in cases where it is legally or practically inappropriate. Therefore, we need to make the scope of consent more realistic, while also clarifying and making the requirements for its effectiveness more practical.

In many situations, such as where there is a structural imbalance (e.g. in employment relationships), in complex or continuously changing processing contexts, or in data processing involving only minor intrusions, consent is not an effective means of ensuring data protection. Furthermore, the requirements of voluntariness, informed consent and revocability are not easily translatable to international scenarios.

It would be desirable to provide a legal clarification regarding consent under Article 9(2)(a) of the GDPR, particularly by introducing illustrative examples of permissible processing purposes. Additionally, the possibility of exempting certain low-risk processing activities from existing consent requirements should be examined. This would make consent easier to understand and more legally secure, while ensuring the rules are applied proportionately. It would also be beneficial to introduce a risk-adapted consent model that allows for lower requirements in terms of the form and depth of consent for less sensitive or pseudonymised data, for example in the context of research projects subject to ethical review. Differentiation based on processing risk would better reflect the actual need for protection.

Consents given in accordance with the laws of third countries should be recognised as valid for data collection, provided subsequent processing within the EU complies with GDPR requirements. Retrospective verification of consent forms from third countries should not be necessary. This would facilitate global data flows while maintaining the European level of data protection.

Overall, consent as a legal basis should be considered more carefully and not used universally as a default solution. A more flexible, risk-based approach could help to strike a better balance between data protection and data availability.

## **Expansion of Legal Bases and Introduction of Broad Consent**

The existing legal bases under the GDPR are increasingly reaching their limits in the context of innovative technologies and data-intensive applications. Bitkom therefore



advocates expanding the legal basis for processing pseudonymised data in particular. In order to ensure national and European competitiveness, the innovation potential of new technologies must be utilised and the legal security of their application must be promoted. One option could be a new legal basis that specifies when certain protective mechanisms apply, such as mandatory data protection impact assessments, transparency obligations and opt-out options. However, it should be clarified how such a new legal basis would operate in practice, in particular whether it would apply to low- or high-risk processing activities. To ease compliance burdens, the Commission should consider identifying certain categories of processing activities where a legitimate interest can be presumed. In these cases, administrative requirements such as Legitimate Interest Assessments (LIAs) or, in some instances, DPIAs would not be required.

Additionally, consideration should be given to incorporating the concept of ‘broad consent’ into general data protection legislation. Recital 33 of the GDPR provides a potential framework for granting consent for multiple purposes that are not yet fully specified but are compatible. This would make research- and innovation-driven data processing more legally secure and efficient. However, such an approach should only be implemented if the Commission simultaneously provides clear guidelines specifying which processing activities are covered, in order to avoid compliance uncertainties for companies.

Furthermore, ways of facilitating the processing of pseudonymised data should be examined. Simplified legal bases could be considered, provided that strong safeguards (e.g. mandatory DPIAs) and transparency obligations, along with a right to object for data subjects, are in place. While Article 6(4) of the GDPR offers some starting points, its complexity makes it difficult to apply in practice.

## **Better stakeholder Involvement in EDPB Guideline development**

For the GDPR to be applied in a practical and business-friendly way, the interpretation of the European Data Protection Board (EDPB) is of central importance. Bitkom suggests refining the process of creating guidelines, opinions and recommendations by involving stakeholders before draft texts are prepared, for instance through public consultations or expert discussions. This would improve the quality of the documents, enhance their practicability and increase their acceptance.

Furthermore, the EDPB's role should evolve from that of an ex-post body to that of a cooperative innovation facilitator. One possible approach would be to establish an «EDPB Innovation Forum» to bring companies, research institutions and supervisory authorities together at an early stage, enabling legally compliant innovation and providing regulatory support for new technologies.

## **Legal Certainty**

The creation of a legally secure and practical framework for the use of personal data would provide reassurance to consumers and businesses. The GDPR contains many vague legal terms which are sometimes interpreted differently by various stakeholders

(such as courts and supervisory authorities), which creates legal uncertainty for businesses. When interpreting the GDPR, it is important to strike a balance between the interests of consumers and the economy — a one-sided interpretation hinders economic innovation and is detrimental to consumer-oriented services. Therefore, when revising the GDPR, a primary goal should be to clarify the legal terms in order to enable data protection.

It is equally important to ensure a uniform interpretation across all Member States in order to avoid legal uncertainty caused by differing interpretations.

Any reform considerations for the GDPR should be measured and take practical realities into account. Since the regulation came into force, companies have adapted to the existing framework and established processes, making significant investments in data protection compliance in the process.

The aim of any further development should therefore be to address specific challenges in a targeted manner, while ensuring that the core principles of the GDPR and the achieved level of harmonisation and legal certainty remain intact. While targeted adjustments and clarifications – whether through guidelines or legislative measures – can be useful, they must always be assessed for practical applicability and systemic compatibility.

## 2 Conclusion

Bitkom welcomes the EU Commission's initiative to simplify the GDPR in a targeted manner, particularly the provision of risk-based relief for small and medium-sized enterprises (SMEs) and small mid-cap companies (SMCs). Proposals such as limiting certain documentation obligations and extending SME exemptions to additional company sizes are important initial steps in the right direction.

However, from Bitkom's perspective, these measures alone are insufficient to reduce the bureaucratic burden of data protection in a sustainable way. Companies of all sizes continue to devote significant personnel and financial resources to extensive documentation and reporting obligations, often without generating proportional added value for data protection.

Therefore, a more risk-based, practical data protection framework should be the objective. Obligations should align with the actual risk of specific data processing activities, regardless of company size, while unnecessary complexity should be avoided. Reforms should be carefully and selectively designed. Bitkom notes that deep structural changes or a comprehensive reopening of the GDPR could jeopardise the level of legal certainty and harmonisation achieved so far.

Further improvements should therefore take place within the existing legal framework wherever possible, through centrally coordinated EU Commission guidelines, clearer interpretation standards and practical relief for low-risk processing. Where legislative

adjustments are necessary, they should be precise and compatible with the existing system, without undermining the established foundation of the regulation.

The changes initiated so far can serve as a meaningful starting point, but they must not mark the end of reform efforts. Reform efforts should also focus on synchronising the GDPR with digital legislation such as the DGA, Data Act and AI Regulation. Existing overlaps and contradictions create legal uncertainty and additional costs for companies. In the coming weeks, Bitkom will develop concrete proposals aimed at alleviating the burden on companies while ensuring that the GDPR – and thus the protection of data subjects – remains fit for the future, even with regard to new technologies.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

#### Published by

Bitkom e.V.  
Albrechtstr. 10 | 10117 Berlin

#### Contact person

Isabelle Stroot | Policy Officer Data Privacy  
P +49 30 27576-228 | [i.stroot@bitkom.org](mailto:i.stroot@bitkom.org)

Elena Kouremenou | Policy Officer Data Privacy  
P +49 30 27576-425 | [e.kouremenou@bitkom.org](mailto:e.kouremenou@bitkom.org)

#### Responsible Bitkom Committee

WG Data Privacy

#### Copyright

Bitkom 2024

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.