verbraucherzentrale
Bundesverband

DOCUMENTATION AS A PILLAR OF RISK ASSESSMENT AND ACCOUNTABILITY

Opinion by the Federation of German Consumer Organisations (vzbv) on the European Commission's proposals for the simplification of the GDPR's record-keeping obligations for SMEs and small mid-cap companies

21. May 2025

RELEVANCE FOR CONSUMERS

> Consumers are affected daily by the processing of their personal data – for example, by their physician or lawyer. If such organisations are no longer required to maintain systematic records of their processing activities, a central basis for identifying risks to the rights of data subjects at an early stage will be missing. This would undermine the ability to prevent misuse or data breaches. The obligation to maintain records therefore directly enhances security for consumers and constitutes a prerequisite for their effective exercise of data protection rights.

BACKGROUND

The European Commission is planning an amendment to Article 30(5) of the General Data Protection Regulation (GDPR), under which the obligation to maintain a record of processing activities would no longer apply to certain organisations, provided that the processing of personal data does not pose a likely high risk to the rights and freedoms of the data subjects. The assessment of whether such high risk exists shall be guided by the Article 29 Working Party's Guidelines on Data Protection Impact Assessment.[1]

This exemption is intended not only for small and medium-sized enterprises (SMEs) with up to 250 employees, but is proposed to be extended to small mid-cap companies with up to 750 employees and a total balance sheet not exceeding 129 Million Euro and an annual net turnover not exceeding 150 Million Euro.

GENERAL REMARKS

vzbv regards these proposals with fundamental scepticism. The GDPR constitutes a central pillar of European digital regulation. It was adopted after years of intensive negotiations among legislators, civil society, industry and academia. It repre-

[1] Article 29 Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev.01), 2017, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711, 06.05.2025.

sents a balanced regulatory framework that has been assessed in previous evaluations by the European Commission as effective, future-proof and proportionate. The European Commission's **evaluation reports** as well as the stakeholder feedback submitted in that context **have revealed no need for structural reform**. Rather, they emphasised the appropriateness of the GDPR's principles and rules. According to these reports, future efforts should focus on coherent interpretation and enforcement, not on deregulation.[2]

vzbv expresses particular concern that the proposed adjustments risk opening the door to further erosions of the GDPR. In the political debate, for instance, proposals have been advanced by the German Federal Government to exempt SMEs entirely from the scope of the GDPR.[3] This illustrates that any amendments could be used as an opportunity to question the carefully balanced framework of the GDPR, potentially leading to a fundamental erosion of the European level of data protection.

ON THE SPECIFIC PROPOSALS

From a substantive perspective, it is important to underline that the documentation of processing activities constitutes a **central element of effective data protection management**. Data protection risks cannot be assessed in a static manner but only contextually and dynamically. Risks emerge from the specific constellation of the processing operation, which may change at any time.[4] Proper documentation therefore serves not only as a means of accountability but primarily as a tool for the structured identification, analysis, evaluation and mitigation of risks. Without initial and ongoing documentation, there is an acute danger, that companies misjudge whether a high risk is present. If the proposals were implemented, physicians or lawyers, for example, may in principle no longer be required to maintain a record of processing activities.[5]

Beyond that, documentation serves as an indispensable **framework for reflection and structuring** within the controller or processor, particularly for SMEs. It enables these organisations to systematically identify, categorise and translate the data protection requirements into appropriate organisational processes. Only by structuring the purposes of processing, legal bases, retention periods, data subject rights and the technical and organisational measures employed can companies archive sound understanding of their data-processing operations and the respective legal obligations. The planned abolition of the record-keeping obligation for SMEs and small mid-cap companies – covering approximately 99 percent of all European companies – entails a significant risk that such entities will no longer feel compelled to actively and systematically engage with their data protection responsibilities. It may foster the impression that systematic, documented and verifiable data protection practices are merely optional, thereby sending a fatal signal regarding the binding nature of data protection standards.

---

[2] European Commission: Second Report on the application of the General Data Protection Regulation, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0357, 06.05.2025.

[3] Coalition Agreement between CDU, CSU and SPD, 2025, p. 65, https://www.cdu.de/app/uploads/2025/04/Koalitionsvertrag-%E2%80%93-barrierefreie-Version.pdf, 06.05.2025.

[4] Article 29 Working Party: WP 248 rev.01, 2017, p. 13f

[5] According to Recital 91 GDPR and WP 248 rev.01 (p. 12), the processing of personal data relating to patients or clients by an individual physician, other healthcare professional or lawyer may not constitute a high risk, as such processing is not considered to be on a large scale.

Moreover, documentation represents one of the core pillars of the **accountability** principle, Article 5(2) GDPR. It is the primary instrument through which data controllers and processors can demonstrate that they actively and systematically implement data protection requirements. This concerns not only the assessment of risks and legitimate interests but also the transparent presentation of the technical and organisational measures adopted, purpose limitation, data minimisation and storage limitation. Therefore, for data protection supervisory authorities, records of processing activities constitute an indispensable basis for their audits. Only structured records enable authorities to identify high-risk processing operations, conduct targeted inspections and adopt **effective regulatory measures**.

> Instead of adopting blanket exemptions for certain companies, the European legislator should focus its efforts on supporting small enterprises through targeted awareness-raising, training programmes and technical tools for record-keeping. Abandoning essential documentation obligations would mark a step backwards in the development of a responsible digital regulatory framework.

Contact

Federation of German Consumer Organisations –
Verbraucherzentrale Bundesverband e.V. (vzbv)
Team Digital and Media
digitales@vzbv.de
Rudi-Dutschke-Straße 17, 10969 Berlin, Germany

vzbv is registered in the German Lobby Register and the European Transparency Register. You can access the relevant entries here and here.