EUROCHAMBRES

GDPR SIMPLIFICATION PROPOSALS

General Data Protection Regulation Simplification Proposals

Chambers of commerce and industry call for the reaffirmation of a risk-based approach as the guiding principle in the interpretation and application of General Data Protection Regulation (GDPR). The rather conservative interpretation, coupled with lack of harmonisation and consistent application of GDPR has created significant challenges for businesses, with dangerous repercussions on business operations and innovation. Chambers suggest the following simplification measures in order to foster legal certainty, reduce excessive administrative burdens, and better align data protection with practical business realities.

Since its introduction in 2018, the GDPR has fundamentally reshaped the data privacy landscape across the EU, setting a global benchmark for the protection of personal information. However, while the regulation has been lauded for strengthening individuals' rights and harmonising data protection standards, it has also imposed significant administrative burdens on businesses operating within the European Union. Businesses of all sizes have faced complex compliance requirements, including extensive record-keeping, detailed documentation of data processing activities, and ongoing obligations to monitor and report on their data practices.

These administrative demands have been particularly challenging for small and medium-sized enterprises (SMEs), which often lack the resources and expertise to efficiently manage the intricate regulatory landscape. The cost and effort required to comply with GDPR have, at times, diverted attention and resources away from core business activities, stifled growth, and even discouraged some firms from expanding their operations.

Most importantly, while chambers of commerce support several targeted amendments, they believe many meaningful improvements can be achieved without a complete overhaul of the GDPR. They do not support a full-scale revision, as this could create significant business uncertainty. In this context, chambers would like to highlight the main causes of administrative burden for businesses and suggest the following improvements:

Reason for administrative burden	Suggested improvements
Chapter 2, Article 6(1) - Lawful grounds for processing Businesses still grapple with legal uncertainty around the appropriate legal basis for processing personal data, particularly regarding necessity for the performance of a contract and legitimate interest. The uncertainty often leads to an overuse of consent, despite other legal bases being	Regulators should provide clear, practical guidance on the application of legal bases, especially "performance of a contract" and "legitimate interest", to reduce uncertainty and prevent the default overreliance on consent. The European Commission should encourage DPAs to recognise, support and reinforce the use of legitimate interest and

more suitable. Regulators exacerbate this by limiting options beyond consent, overlooking individuals' consent fatigue and ignoring the risk-based organisational accountability inherent to other legal bases, better suited for innovative data processing.	contractual necessity where appropriate, reflecting the risk-based accountability model of the GDPR rather than a consent-centric approach. Additionally, it should be clarified that pseudonymised data may be considered non-personal data for third-party recipients who have no access to, or legal means of obtaining, the re-identifying information.
Chapter 3, Article 13 – Information obligations Art 13 et seq. and the high requirements also set by the supervisory authorities lead to extensive data protection information that is mostly not read. The documentation, information and verification obligations are proving to be too bureaucratic for many businesses. In the case of low-data processing or data processing with a low or normal risk, the comprehensive documentation, information and verification obligations are disproportionate and not appropriate to the risk.	In keeping with the risk-based approach, in certain low-risk scenarios, the obligation for SMEs to proactively provide information should be replaced with a right for customers to request it. In other words, while full information must be made available upon request, SMEs should not be required to automatically disclose details that hold limited practical relevance for the data subject in low-risk contexts.
Chapter 3, Article 15 - Data Subjects' Access Requests (DSARs) Due to heightened GDPR awareness and the expanding data economy, businesses are increasingly allocating resources to handle Data Subjects' Access Request (DSARs). Mapping and consolidating data from various systems and sources is extremely costly and time-consuming, especially with pseudonymised or unstructured data. The volume and complexity of required disclosures, such as legal bases, retention periods, or extensive rights explanations, are often disproportionate to the actual risk and interest to the customer. The scope of the right to information is not clearly regulated. To many businesses it is not completely clear which documents must be handed over in the event of a "right to a copy of data". For example, the question arises as to whether data that the person	Regarding the outcome of the CJEU case C-203/22 Dun & Bradstreet Austria, new guidelines on the way to provide "meaningful information about the logic involved" according to article 15, §1, GDPR could be very useful to businesses. Full practical guidance and templates similar to the ones provided by the EDPB on CCTV in 2019 (Guidelines 3/2019 on processing of personal data through video devices) would help businesses simplify their compliance with right of access in the context of increased use of complex algorithms or AI systems. As guidance and case law have further broadened the scope of DSAR and the level of detailed information to provide to data subjects, applying proportionality could help businesses to meet these challenges in line with GDPR principles.

requesting information already has must also be handed over. The person already has knowledge of this and it is contrary to the purpose of the right to information to have to provide a copy of this data again.	Businesses should be exempt under the "right to information" from providing data that the person requesting information already has available and is accessible. In addition, the broad interpretation of what constitutes an "abuse of rights" should also be interpreted more narrowly.
Chapter 3, Article 22 - Automated individual decision-making, including profiling With the last case law of the CJEU (case C-634/21 SCHUFA Holding (Scoring)) and the step-by-step entry into force of the AI Act, businesses need more guidance to apply the rules regarding automated individual decision making. The current guidelines on automated decision making and profiling date back to WP 29. They were last revised on 6 February 2018.	Clear and practical guidance, including concrete examples, would be very valuable. For instance, it would be helpful to illustrate best practices for effective human oversight when using AI tools to process personal data, ensuring compliance and responsible intervention throughout the process.
Chapter 4, Article 24 - Responsibility of the Controller Article 24 requires controllers to implement appropriate technical and organisational measures, taking into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". This is in accordance with recital 76, in which the assessment of risk should consider "the likelihood and severity of risk to the rights and freedoms of natural persons," and that risk should be evaluated in light of the nature, scope, context, and purposes of processing.	Chambers emphasize the importance of national and European regulators consistently applying the GDPR's risk-based approach and principle of proportionality. In practice, there is often a disproportionate focus on the mere possibility of harm, with insufficient attention to the likelihood and severity of risks, and how these vary across sectors and business operations.
Chapter 4, Article 25 - Controller/processor obligations, security, DPO, Data Protection by Design The obligations laid out in this article requires equal implementation rigor regardless of the size of a company and the sensitivity of data.	Article 25 should be formally revised to require explicit risk-tiering based on data sensitivity, the scale of processing, and organisational capacity. In addition the European Commission should introduce SME-specific technical standards for key safeguards, including anonymization techniques, access controls, and breach

	detection systems, ensuring that compliance measures are both effective and proportionate to the risks involved. A robust monitoring mechanism should be established, obliging national DPAs to report (for example biennially) on SME compliance costs and the effectiveness of these simplified measures, thereby ensuring continuous improvement and accountability in supporting SMEs data protection efforts.
Chapter 4, Article 30 (5) – Exemption of record-keeping obligations for SMEs Omnibus IV proposes replacing art. 30(5) with the following wording: "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or organisation employing fewer than 750 persons, unless the processing it carries out is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35." Recital 10 explains that, in this context, processing special categories of personal data that is necessary for carrying out obligations and exercising rights in the field of employment, social security and social protection law, as referred to in Article 9(2)(b) of Regulation (EU) 2016/679, should not require records of processing to be kept. Chambers welcome these changes and it is positive that SMCs are now exempt from the record-keeping obligation and in particular that this exemption has been made more accessible to SMEs. However, as the other GDPR obligations, such as accountability and transparency, remain fully applicable, the suggested modification to Article 30(5) could have a very limited practical effect. For instance, to comply with the transparency principle, controllers must provide data subjects with up-to-date privacy policies. How can the data controller have up-to-date privacy policies if it does not, at some point, have an up-to-date inventory of its data	Reducing record-keeping obligations for SMEs must necessarily be accompanied by a simplification in the information, accountability and transparency obligations imposed on SMEs, otherwise the simplification of Art. 30 (5) could have a very limited practical effect. All these adjustments must be geared towards paying greater attention to the risk-based approach and eliminating existing legal uncertainties. Recital 13 of the GDPR, which recognizes the special situation of SMEs, has hardly played a role in practice to date.

processing activities? Yet such an inventory is a record of processing activities. Therefore, even if a controller were exempt from the obligation to maintain a record of processing activities, they would still need to do so in order to draft and update their privacy policies and thus inform data subjects. The same reasoning applies to the accountability principle. How can a data controller comply with the accountability principle if they are unable to demonstrate that they are aware of the data processing activities they perform? Therefore, it would need to have evidence, or at least an inventory, of the data processing it performs.	
Chapter 4, Article 33 – Data Incident Reporting Requires extensive reporting to the data protection supervisory authority in case of any data incidents within 72 hours. This holds also over weekends and on public holidays, often resulting in fines for failure to report on time.	Chambers of commerce suggest that the reporting obligation should be limited only to data incidents with a high risk to the rights and freedoms of data subjects. There is a need for a standardised and clear definition within GDPR of the term “risk”. Businesses should be able to assume that the personal data breach does not result in a risk to the rights and freedoms of natural persons. The previous interpretations of the European supervisory authorities do not allow for a clear differentiation. No 72-hour reporting period over weekends and on public holidays.
Chapter 4, Article 35 - Data Protection Impact Assessments (DPIAs) Article 35(1) mandates that a DPIA must be carried out when a type of processing, especially using new technologies, "is likely to result in a high risk to the rights and freedoms of natural persons," taking into account the nature, scope, context, and purposes of the processing.	Create one Data Protection Impact Assessment (DPIA) template, common guides and common risk assessments that are applicable to all member states. Consider limiting the reporting obligations of DPIAs to the minimum content requirements laid out in article 35.
Chapter 4, Article 40 and 42 – Codes of Conduct and Certificates	Urgent action is needed for DPAs to review their very stringent requirements on such codes of conduct and collaborate with

Codes of conduct and certifications were designed as accountability tools for specific sectors and processing activities. However, they have been underutilized despite their benefits of promoting consistent data protection approaches, enabling compliance, and reducing DPAs' workload.	stakeholders through simplified approval processes to address sector-specific challenges, risks, and best practices.
Chapter 5, Article 44 ff - Data transfers outside EU/EEA Following the CJEU Schrems II Judgment and even after the EU-US Data Privacy Framework, the European Commission and regulators have taken a strict stance on international data transfers to countries lacking EU adequacy agreements. Despite costly Transfer Impact Assessments, organisations are nevertheless required to eliminate all risks of unauthorized access to European personal data, regardless of the nature of the data, the likelihood of access by foreign governments and the severity of the potential harm. This strict approach thus obliges businesses to implement additional measures beyond Standard Contractual Clauses and Binding Corporate Rules. This poses challenges, particularly for smaller entities, urging for a more balanced, risk-based approach in line with GDPR principles. The vast majority of companies (e.g., 88% in Germany according to a survey conducted by the German Chamber of Commerce and Industry (DIHK) in 2023) is unable to independently assess the level of data protection in third countries and therefore cannot be liable for the protection of data transferred internationally.	The European Commission should develop robust international standards and provide clear, stable guidance on the level of data protection in third countries. This includes ensuring that adequacy decisions are comprehensive, transparent, and not subject to sudden changes that could disrupt business operations. Transfer Impact Assessments (TIAs) should be risk-based, distinguishing between low-risk data, such as non-sensitive business contact details, and high-risk data so that rigorous safeguards are applied only where truly necessary. To support organisations, particularly SMEs, the European Data Protection Board (EDPB) should maintain standardised, sector-specific TIA templates and checklists, making the assessment process more practical and consistent across the EU.
Chapter 8, Article 82 – Compensation for breaches of GDPR There are major uncertainties regarding the right to compensation. Even though the European Court of Justice has now clarified individual questions, it is still unclear in practice under what conditions and to what extent compensation can be claimed for breaches of the GDPR. This leads to	Introduction of a materiality threshold in relation to damage under GDPR. The requirements are too narrow.

incalculable risks that burden and inhibit the economy (barrier to investment).	

Additional suggestions

A. Legal Basis within GDPR for data processing for AI

A robust legal framework is essential for the data economy. This framework should provide clear, competitive, and internationally harmonised conditions that enable data processing while simultaneously safeguarding the legitimate interests of both citizens and businesses. **Chambers therefore advocate for the establishment of a clear legal basis, either within the GDPR or through dedicated regulations, for all stages of data processing involving AI, as well as for the legally secure use of data rooms.**

When developing such regulations, it is crucial to ensure coherence and consistency with existing laws. The frequent use of the phrase “The GDPR remains unaffected” in new EU data regulations creates significant legal uncertainty. If new regulations for the data economy are to be based on the GDPR, any existing ambiguities within the GDPR itself must first be resolved. Therefore, **chambers call for the creation of explicit legal provisions that address all stages of AI-driven data processing** and ensure the secure and lawful use of data rooms.

B. Specific provisions on business transfers

The GDPR lacks specific provisions addressing data protection in the context of business transfers, especially asset deals, making legal compliance uncertain for private companies. In order to ensure legal clarity a dedicated legal basis should be introduced within the GDPR to cover personal data processing in the context of business transfers.

Eurochambres – the association of European chambers of commerce and industry – represents more than 20 million businesses through its members and a network of 1700 regional and local chambers across Europe. Eurochambres is the leading voice for the broad business community at EU level, building on chambers' strong connections with the grass roots economy and their hands-on support to entrepreneurs. Chambers' member businesses – over 93% of which are SMEs – employ over 120 million people.

Previous positions can be found here: bit.ly/ECHPositions

Contact:
Eurochambres Policy Advisor for Digitalisation – Single Market
Ms Lara Condell, Tel. +32 2 282 08 85, condell@eurochambres.eu

Eurochambres Press and Communication Manager
Mrs Karen Albuquerque, Tel. +32 2 282 08 72, albuquerque@eurochambres.eu

Eurochambres Press Contact
Ms Agatha Latorre, Tel. +32 2 282 08 62, latorre@eurochambres.eu

@Eurochambres
www.eurochambres.eu