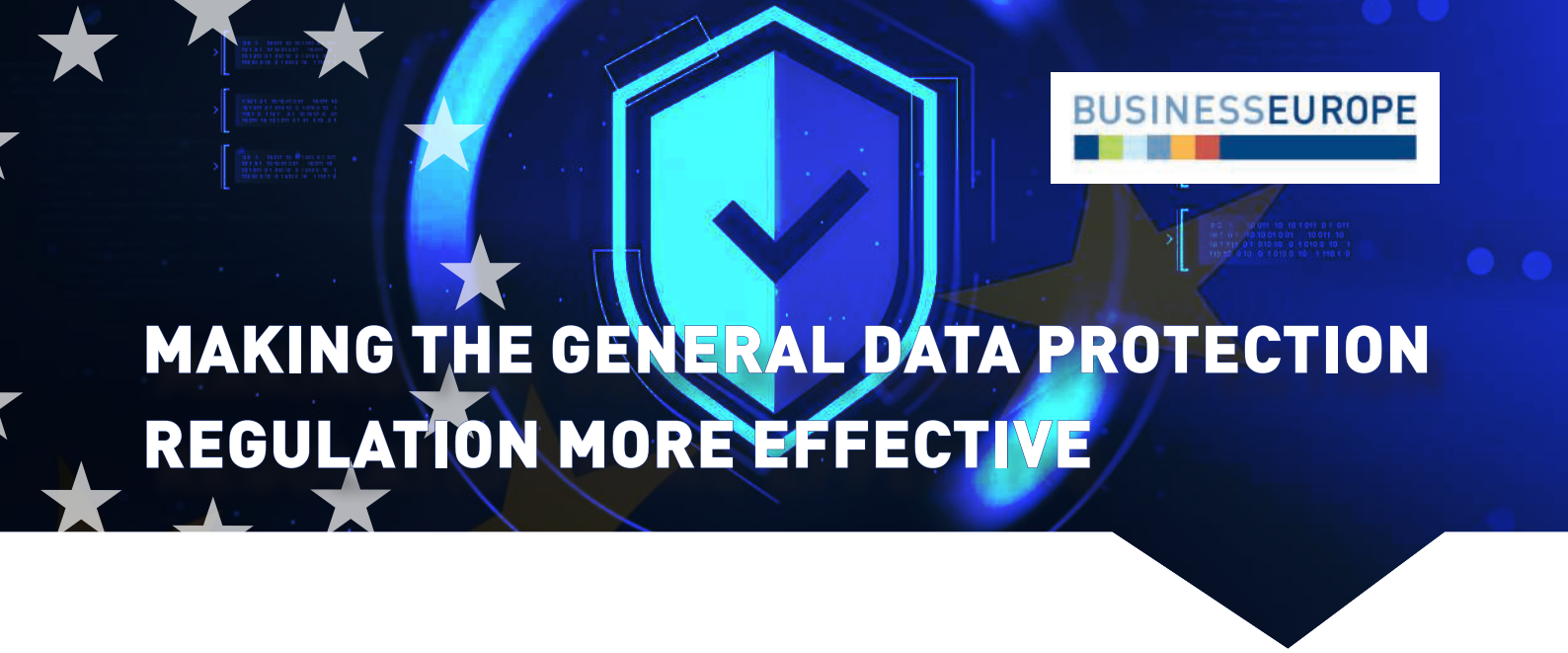

MAKING THE GENERAL DATA PROTECTION REGULATION MORE EFFECTIVE

KEY MESSAGES

Make the GDPR truly risk-based: The GDPR should truly prioritise real risks over routine low-risk processing, using a proportionate approach that supports innovation, compliance, and respect for fundamental rights and freedoms.

Enable access to data for Artificial Intelligence (AI) and European innovation: Clarify that pseudonymised and lowrisk data may be used for R&D and AI development, and reduce the barriers created by today's broad definition of personal data and rigid purpose limitation.

Cut unnecessary administrative burdens: Excessive documentation and reporting obligations consume vast resources, and are unduly and disproportionately costly[1], without improving privacy outcomes.

Make data subject rights compliance workable: Rights remain essential and must be effectively protected. At the same time, their exercise should not be abusive or result in a disproportionate workload. Obligations should be clarified, simplified, and aligned with risk.

Simplify international data transfers: The EU should take more responsibility at systemic level through additional adequacy decisions and clearer guidance, thus reducing the heavy burden now placed on individual companies.

WHAT DOES BUSINESSEUROPE AIM FOR?

Clarity, proportionality, and a cooperative regulatory approach can make the GDPR a source of empowerment rather than a constraint. Grounded in real-world practicality, it can evolve into a framework that truly balances protection and innovation.

[1] According to the 2024 Draghi report on competitiveness, GDPR compliance costs may reach EUR 500,000 for SMEs and EUR 10 million for larger organizations.

CONTEXT

Europe has successfully raised the bar on data protection, embedding respect for personal data across the economy. Companies of all sizes have been investing, adapting, and acting in good faith to comply. Yet while awareness is strong, practical consistency and maturity in implementation are still evolving[2].

Legal uncertainty and fragmented enforcement slow innovation. The combination of differing interpretations, complex compliance requirements, and the threat of heavy sanctions creates hesitation rather than rejection of the rules among businesses. Data protection and the freedom to conduct business are not competing goals, but the perception that efforts in compliance are never enough can inadvertently discourage innovation and limit Europe's digital competitiveness[3].

Action is needed for clarity, and coherence. Moving from fragmentation to alignment among national Data Protection Authorities (DPAs), the European Data Protection Board (EDPB), businesses and citizens will reinforce trust and unlock innovation.

The proposed Digital Omnibus changes related to the General Data Protection Regulation represent a meaningful step in the right direction. Below, we share views broadly aligned with the approaches recently proposed by the Commission, and offering some suggestions for improvement.

DEFINITION OF PERSONAL DATA AND RISK-BASED APPROACH (ARTICLES 4.1; 5, 24, 33, 34 AND RECITALS, 24, 26)

The broad scope creates disproportionate burdens, and hinders innovation since the definition, legal bases, and purpose limitation taken together significantly restrict collection, sharing and use of data. A clarification should also address the legal status of pseudonymised and anonymised data, reflecting the Court of Justice of the EU (CJEU) reasoning in Case C-413/23 P that whether a person is identifiable depends on the processing context, the means reasonably likely to be used by the data recipient rather than only by the controller, and the actual risk of re-identification.

Strengthening the risk-based approach for data processing is essential to reduce the burden on businesses. Accountability obligations, like documentation and organisational measures, and reporting obligations for low-risk and mundane processing activities may be excessive in relation to the context and potential risk to data subject's rights.

Moreover, principles of data protection require modernisation to reflect technological developments and contemporary data processing methods: particularly, purpose limitation, storage limitation, data minimisation, and the unlimited accountability of the controller, which increasingly conflict with large-scale data processing and AI-driven operations.

---

[2] The Fundamental Rights Agency (2024; 2020) notes that awareness of data protection rights does not necessarily translate into understanding, as evidenced by the high number of "trivial or unfounded" and "petty and repetitive" complaints received by Data Protection Authorities.

[3] Regulatory complexity, legal uncertainty, and compliance risk are identified in the Draghi competitiveness report as factors that can weaken innovation incentives, particularly for smaller firms. Supporting evidence from Finland shows that GDPR implementation reduced pharmaceutical and biotechnology R&D spending by up to 39 percent within four years, with the strongest effects among firms operating exclusively under the EU regulatory regime. Consistently, the European Innovation Scoreboard identifies a share of firms with no inclination to innovate.

SUGGESTED IMPROVEMENTS:

- Clarify the use of pseudonymised/anonymised data as to when it can be treated as non-personal data in line with the CJEU Case C-413/23 P, in Article 4 and consistently in Recital 26 by establishing an approach based on the entity processing the data and the means it actually has at its disposal.
- Article 5 must reaffirm the risk-based nature of the Regulation and its balance of data protection and innovation in the economy, with a corresponding reflection in Article 24. Further processing for archiving, research[4], statistical, or public-interest purposes should be explicitly treated as automatically compatible, removing the need for a separate Article 6(4) assessment, which often adds unnecessary red tape. This ensures efficiency while keeping all Article 89(1) safeguards in place to protect data subjects' rights.
- An adaptation of the applicable requirements according to the level of risk would also enhance overall coherence with the AI Act, which clearly differentiates the obligations applicable to an AI system based on the level of risk associated with it.
- Heighten the threshold for data breach reporting, so only high-risk breaches are covered, and consider merging Articles 33 and 34. Such an evolution would help avoid excessive notification of minor incidents, which provide limited value for supervisory authorities, while allowing resources to be focused on significant risks.

E-PRIVACY DIRECTIVE AND THE GDPR

Aligning parts of the e-Privacy Directive with the GDPR would be beneficial for the recognition that certain uses of data can help service providers to improve and maintain quality without unnecessarily burdening users with frequent consent requests. Such framework would continue to safeguard personal data, while offering a clear, structured approach for responsible data use.

- Move the "cookie rule" from the ePrivacy Directive to the risk-based framework of GDPR, or "whitelist" low-risk, essential activities (e.g., security monitoring, software updates, anti-fraud, and first-party analytics).

CLARITY ON LAWFUL BASIS FOR PROCESSING (ARTICLES 6 AND 9)

Lawfulness of data processing activities has been a point of tension over the years. Subsequent legal acts in the digital sphere have treated different legal bases as to clarify which one is more suitable for particular activity, thus creating confusion as to whether the legal bases are ranked or not. In addition, certainty is necessary, especially for further processing for example for AI training, or other emerging technology developments.

SUGGESTED IMPROVEMENTS:

- Clarify in the GDPR that companies have a clear legal basis in Article 6, such as legitimate interest; research grounds, for training AI models and systems.

[4] Including one that would support innovation, technological development, and R&D activities of the private sector. The GDPR Recital 33 allows for broader consent of certain areas of scientific research. Business R&D often uses the same methodologies, experimentation, and has contributed to major breakthroughs, and should also more explicitly benefit from such broader consent.

- Reaffirm "legitimate interest" for AI training and clarify rules to ease the processing of data that has been manifestly made public by individuals.
- Reflection in Article 9 on balanced processing of special categories of data in line with technological developments, such as AI, would be necessary, for example by introducing carefully scoped exceptions that allow use of sensitive data for AI, while underpinning safeguards to protect individuals' rights. This approach would balance technological progress with fundamental data protection principles.

DATA SUBJECT RIGHTS: PRACTICAL CHALLENGES AND MISUSE (ARTICLES 12 TO 15)

Data subject rights are often perceived as absolute, and not as relative to other persons rights, freedoms and legal obligations. This creates unrealistic expectations, especially regarding access and erasure, or rejection of request. The scope of uncertainty on what must be disclosed is high. Identification challenges to verify data subjects' requests persist. Yet, any non-compliance by business is portrayed as intentional, which fuels negative perceptions, and discourages engagement, particularly among SMEs.

Data subject requests are a large administrative burden, time-consuming and costly. Moreover, the volume of data subject rights requests has been increasing significantly each year, to the point of becoming difficult to manage for many organisations, particularly for SMEs, which often lack the resources to handle such requests effectively. This imbalance led to the misuse of data protection rights for purposes unrelated to safeguarding personal data, exposing controllers to heightened legal and reputational risks. A growing risk of misuse of these rights can thus be observed, where they are used: (i) as leverage in litigation to obtain evidence, for instance in employment disputes; (ii) as a means of exerting pressure on companies through repeated or coordinated requests from activists; or (iii) as a reputational or image-related tool without any direct connection to the genuine protection of personal data.

SUGGESTED IMPROVEMENTS:

- Clarify that the rights are not absolute, especially to avoid intrusive monitoring obligations and ensure the balance with other persons' rights.
- The possibility to reject a request on grounds that its purpose is abusive (e.g., manifestly unfounded or excessive, especially if the request is made for purpose other than data protection) can be considered. Data subjects must cooperate in this process of clarifying the purpose of the request.[5]
- Unfounded, abusive, misused, and excessive requests should be further defined in guidelines issued by the European Data Protection Board (EDPB).
- Consider less information obligations under Articles 13–15 where more proportionality is needed.

[5] Suggestion, Article 12 (5): Information supplied under Articles 13 and 14, as well as any communications or measures taken under Articles 15 to 22 and 34, must be provided to the data subject at no cost. However, if a request cannot reasonably be met, is clearly unfounded or excessive, particularly when repeated, or would require a disproportionate effort in light of the actual risk or alleged harm, the controller may either charge an appropriate fee reflecting the administrative effort needed to provide the requested information, communication, or action, or refuse to comply with the request after asking the data subject to clarify the purpose and the specific processing activities concerned.

AUTOMATED DECISION-MAKING (ARTICLE 22)

The application of Article 22 GDPR regarding automated decision-making is often interpreted narrowly. Some data protection authorities claim that automated decisions cannot be considered "necessary" simply because humans have historically performed such tasks. They draw the conclusion that automated decision-making is not permissible and that an effective consent according to Article 22(2)(c) and Article 7(4) can only be given if the data subject has the opportunity

to choose processing by a human being from the beginning. However, such a narrow interpretation of what can be considered necessary would prevent businesses and consumers from fully accessing the benefits new technology. This restrictive reading often prevents digital solutions, such as online contracts or automated tasks processing (i.e., automated claims processing).

SUGGESTED IMPROVEMENTS:

- GDPR's Article 22 should be reformed and aligned so that compliance with the due diligence obligations in the AI Act enables a legally compliant use under GDPR, provided a legitimate interest is pursued.

PRIOR CONSULTATION AND DPIA GUIDANCE (ARTICLES 35 AND 36)

Article 36 requires prior consultation only when a "Data Protection Impact Assessment" DPIA identifies a high risk that cannot be mitigated, and some DPAs interpret their guidance role as limited to these non-mitigatable high-risk cases. This leaves controllers, especially those using highly innovative technologies, facing regulatory uncertainty, and unable to seek support until risks are already severe, leading to delays and uneven compliance. Yet Article 57 makes clear that DPAs must promote awareness of risks, rules, safeguards, and controller obligations more broadly. Such a narrow interpretation does not help with proactive oversight.

Furthermore, current DPIA practices can sometimes become routine "tick-box" exercises, particularly when requirements are rigid or interpreted inconsistently across authorities, which makes it harder for organisations to focus on genuinely high-risk processing.

SUGGESTED IMPROVEMENTS:

- Articles 35 and 36: The DPIAs requirements will also benefit from risk-based clarification, and prior consultation to the supervisory authority on a voluntary basis should be permissible not only for reactive situations, but also, for example, where the results of the impact assessment are not conclusive.
- Streamlining DPIA requirements and harmonising templates would also help reduce complexity of internal processes and cut administrative burden for businesses.

INTERNATIONAL DATA TRANSFERS (ARTICLES 44 - 47)

International data transfers have not been smooth, especially for smaller players. The conclusion of adequacy decisions with different jurisdiction has not been at the speed that would allow scale and certainty for expanding business operations abroad.

SUGGESTED IMPROVEMENTS:

- A thorough assessment of the international data transfers challenges under the GDPR must be conducted, and the process reformed.
- Clarify that the risk-based approach (Articles 24 and 32) applies also to the measures for data transfers to third countries (Chapter V).
- Simplify the validation process of Binding Corporate Rules (Article 47).
- Create a positive presumption for intra-group transfers where a group self-certifies adherence to appropriate safeguards. Assessment of a third country's laws should focus on the actual likelihood of public authorities accessing EU persons' data.

REGULATORY COOPERATION AND PROCEDURAL CERTAINTY (ARTICLES 51 - 57)

The Helsinki Commitments already outline valuable principles for transparency, stakeholder engagement, and predictability in European Data Protection Board (EDPB) and national data protection authorities (DPAs) cooperation. To ensure these remain stable and consistently applied over time, it would be helpful to explore whether some procedural guarantees, such as clearer consultation practices, feasibility assessments, transparency, could be reflected at the legislative level. This would strengthen trust, reduce uncertainty for stakeholders, and ensure continuity of the practice.

SUGGESTED IMPROVEMENTS:

- The process of EDPB guidelines could be amended to include feasibility checks ahead of adoption, engage stakeholders from the beginning, and include transparency requirements on how stakeholders' input has been treated (the Helsinki statement).
- Article 57 should more clearly state that DPAs have a responsibility to guide controllers and processors on data processing activities beyond only non-mitigatable high-risk cases, reinforcing cooperation and strengthening the
- protection of data subjects.
- The principle of proportionality, already stated in recitals, must be made explicit in the main text to guide enforcement by DPAs.

BUSINESSEUROPE

BusinessEurope is the leading advocate for growth and competitiveness at the European level, standing up for companies across the continent and campaigning on the issues that most influence their performance. A recognised social partner, we speak for enterprises of all sizes in 36 European countries whose national business federations are our direct members.

Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic
Denmark	Denmark	Estonia	Finland	France	Germany
Germany	Greece	Hungary	Iceland	Iceland	Ireland
Italy	Latvia	Lithuania	Luxembourg	Malta	Montenegro
Norway	Poland	Portugal	Rep. of San Marino	Romania	Serbia
Slovak Republic	Slovenia	Spain	Sweden	Switzerland	Switzerland
The Netherlands	Türkiye	Türkiye	Ukraine	Ukraine	United Kingdom

Avenue de Cortenbergh 168
B - 1000 Brussels, Belgium
Tel: +32(0)22376511 / Fax: +32(0)22311445
E-mail: main@businesseurope.eu

WWW.BUSINESSEUROPE.EU

EU Transparency Register 3978240953-79