We, the representatives of the business community, are unanimously calling for the re-affirmation of a risk-based approach as the guiding principle in the interpretation and application of the General Data Protection Regulation (GDPR). This could be done by focusing on harmonisation of interpretation of the existing regime through a constructive dialogue between regulators, including data protection authorities, and the industry.

Committed to make data protection as a cornerstone of our operations, economic players across all sectors have invested many resources in their compliance efforts since the entry into force of the GDPR. Beyond a mere compliance exercise, businesses acknowledge how GDPR has been pivotal in strengthening data protection across the EU and recognise the competitive advantage deriving from data protection to ensure long-term trustworthy relationships with data subjects. However, a rather conservative interpretation of the GDPR, coupled with a lack of harmonisation and consistent application, has created important challenges for businesses, despite their commitment and significant investments, with dangerous repercussions on business operations and innovation.

In this context, **we stress the need for national and European regulators to consistently apply the risk-based approach and the proportionality principles enshrined in the GDPR**. Over the past six years, we have increasingly observed the adoption of a conservative approach whereby regulators have espoused a strict interpretation of the law. Contrary to the GDPR's original spirit, this approach seems only to consider the existence of a potential harm, and it overlooks the likelihood and severity of the risks and how they vary across sectors and business operations. We thus perceive that data protection has become an absolute right, in contradiction with the GDPR's ambition of reconciling it with other public policy objectives and fundamental rights, including the right to conduct a business, as set out in Recital 4 of the GDPR and arising from the European Data Strategy[1].

This re-alignment must be accompanied by a **reinforcement of the regulator's mission to support economic actors**, especially SMEs, in protecting personal data through technical and organisational measures that are more tailored to the risks of their processing activities and their specific sector. As regulators cannot be expected to have extensive sectoral expertise, it is fundamental to ensure a constructive and structured dialogue with stakeholders (both individual companies and sectoral associations). In the context of guidelines, for instance, this dialogue should occur as early in the process as possible, always underpinned by workshops or hearings before both national Data Protection Authorities (DPAs) and the European Data Protection Board (EDPB). This dialogue should also assist regulators to better understand business dynamics as well as the importance and impact of data in business models and strategies.

Businesses often face legal uncertainty in their efforts to comply with the GDPR, which is further exacerbated by significant levels of fragmentation in how risks to individuals should be assessed which makes it harder for companies to conduct their business in multiple EU countries while remaining in compliance with data protection rules. This is reflected, for instance, in the ambiguity resulting from the diverse range of Data Protection Impact Assessments (DPIA) templates and guides available in

[1] Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence; https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273

different Member States which would benefit from better harmonisation at EU level and common risk assessments.

Against this background, there are other key areas where economic players across all sectors agree about the need for an overhaul in the application of the GDPR's risk-based approach and proportionality principle.

- **Codes of Conduct & certifications**. Codes of conduct and certifications under Articles 40 and 42 of the GDPR 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. Urgent action is needed for DPAs to review their very stringent requirements on such codes of conduct and collaborate with stakeholders through simplified approval processes to address sector-specific challenges, risks, and best practices.

- **Legal bases for processing data:** 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 more suitable. Regulators exacerbate this by limiting options beyond consent, lastly reflected in the EDPB's draft guidelines on the ePrivacy Directive[2]. This overlooks individuals' consent fatigue and ignores the risk-based organisational accountability inherent to other legal bases, better suited for innovative data processing.

- **International data transfers:** 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.

- **Data Subjects' Access Request (DSAR):** Due to heightened GDPR awareness and the expanding data economy, businesses are increasingly allocating resources to handle DSARs. Mapping and consolidating data from various systems and sources is extremely costly and time-consuming, especially with pseudonymized or unstructured data. As recent guidance[3] and case law[4] have further broadened DSAR scope and level of detailed information to provide to data subjects, applying proportionality could help businesses to meet these challenges in line with GDPR principles.

- **Documentation and information obligations:** To date, the exemption from keeping records of processing activities has no practical relevance. Not only does every employer inevitably handles special categories of data to comply with legal obligations (e.g. for tax purposes) as part of the employment relationship, but every small business processes customer data daily (i.e. not occasionally). Thus, hardly any company in Europe is eligible for the exemption. The risk-based approach needs to be applied accordingly in this case and regarding related information obligations, taking especially into account the core activity of the company.

---

[2] Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive; https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en

[3] Guidelines 01/2022 on data subject rights - Right of access; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en

[4] CJEU (1st Chamber), 26 Oct. 2023, C-307/22

- **Pseudonymisation & anonymisation:** Six years post-GDPR enactment, data controllers still lack common tools and criteria for pseudonymised and anonymized data processing. Though this should have been one of the first priorities of regulators, the current overly restrictive risk-based approach often renders pseudonymised/anonymised data useless, discouraging investment in privacy protecting technologies. Regulators must define GDPR boundaries, specifying operational anonymization methods and conditions for safe data reuse through pseudonymization.

All these considerations delay businesses' approval for all types of data processing, from low-risk processing with an operational imperative to innovative data processing with comprehensive data protection safeguards, and they can negatively affect individuals' access to key services. The one-size-fits-all and maximalist approach, coupled with complicated interpretations of the GDPR provisions, is slowing down companies' advances in innovation and the deployment of new technologies. This also risks jeopardising the promises of new initiatives under the European Data Strategy and the AI Act whose logical interaction with data protection requires a clear application of the risk-based approach on their interplay with the GDPR. As the GDPR and AI act respond to fundamentally different principles and purposes, some provisions overlap: these conflicting obligations will have to be clearly identified to avoid additional compliance difficulties. The complexity of the legal framework must not contribute to fuel a vicious circle which would gradually erode the capacity and willingness of economic players in all sectors to innovate.

Without questioning the imperative to protect personal data, the undersigned associations therefore stress the need for a paradigm shift in the current interpretation of the GDPR to revamp the risk-based approach as the guiding principle of the GDPR. Innovative economic players are unanimous in their call for such an adjustment in order to establish **a sustainable model for the use of data** with a necessary balance of the right to the protection of personal data with others' fundamental rights and public policy objectives.

On behalf of the business community, we remain committed to constructive dialogue and collaboration with EU institutions, bodies, and data protection authorities.