Brussels, February 2024

BSA | The Software Alliance's
Response to the European Commission's Call for Evidence on the Second Application Report of the EU General Data Protection Regulation

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global enterprise software industry, welcomes the opportunity to provide input for the second report of application of the EU General Data Protection Regulation (GDPR). The business-to-business (B2B) software industry is at the forefront of the development of cutting-edge innovation, including cloud computing, privacy and security solutions, data analytics, and artificial intelligence (AI). Our member companies' software-enabled technologies increasingly rely on data and, in some cases, personal data, to function and provide insights to our customers to enable their businesses. As a result, the protection of personal data is an important priority for BSA members, and we recognize that it is a key part of building customer trust.

As the European Commission conducts its second evaluation, it is important to assess **if the GDPR continues to achieve its goal** of effectively harmonizing data protection laws throughout the EU and beyond for two reasons: first, so that consumers know and trust what privacy controls they have, regardless of where they are; and second, so that businesses know what their obligations are, which not only improves the EU single market but also advances trust, digital transformation and innovation in Europe.

Benefits of GDPR Application

Within EU and EEA countries[2], the GDPR has brought valuable harmonization of applicable rules and increased transparency of data handlers' responsibilities. Since May 2018, the GDPR has raised general **public awareness** of privacy and focused the **attention of organizations**, including non-profits and SMEs, that were not necessarily accustomed to dealing with data protection requirements. It has also given Data Protection Authorities (DPAs) the tools to monitor and enforce compliance, including requirements for international data transfers.

The GDPR has adopted a **risk-based and technology-neutral approach to data protection requirements,** which allows organizations to ensure compliance while adapting their practices and safeguards to the

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, PagerDuty, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] References to the EU in the submission are to be read to also mean EEA countries.

Avenue des Arts 44
1040 Brussels
Belgium

www.bsa.org
EU Register of Interest Representatives 75039383277-48

most-suited approach given their business model, activity and risk profile. The GDPR's principle of accountability has raised awareness among companies on the importance of evidence based GDPR compliance. It has streamlined the unification of privacy operations across industries, providing greater insight into where personal information is collected, used, and accessed. The GDPR not only helped organizations (especially, smaller companies) to better understand processing activities within their entities and better manage data flows, but also improved the regulatory readiness of the industry.

The GDPR has become a global point of reference at a time when many countries are developing or updating their privacy laws and regulations, based on standards pioneered in the GDPR. Very importantly, the GDPR enshrined **free movement of personal data** as a crucial pillar of the EU acquis, supporting digitalization and streamlining data processing, thus facilitating the digital transformation of the economy. The overarching goals of the GDPR – to **provide high levels of data protection and to ensure free movement of data** – are continuously essential to privacy laws worldwide. The principles that underpin the GDPR have been foundational to privacy legislation for decades and across economies. Offering these principles to all customers globally helps foster trust and transparency and contributes to reaching global convergence across privacy frameworks. BSA welcomes the leading role that the European Commission is taking on the global scene to support the emergence of "modern data protection regimes […] designed to afford individuals a high level of protection while facilitating data flows in a way that maximizes economic opportunity and consumer interests[3]." The EU has a critical role to play to encourage international privacy best practices and interoperability of privacy systems.

Challenges of GDPR Application

BSA concurs with the European Data Protection Board (EDPB)[4] that it is **premature to revise the legislative text of the GDPR** at this point in time (less than 6 years after its entry into force) and welcomes **continued discussion with BSA members** to enhance the practical application of the GDPR.

BSA offers its feedback based on our member companies' practical experience of GDPR implementation and highlights areas that could benefit from further attention from the European Commission, the European Data Protection Board and national data protection authorities.

Priority issues to be addressed in the second GDPR application report include:

I. **Consistency mechanism should be improved to reduce fragmentation in the Member States and advance harmonization.**
II. **International data transfers toolbox should be strengthened to support global data flows.**
III. **Contractual and business relationships in a B2B environment should be addressed to further advance digital transformation and ensure smooth application of risk-based approach.**
IV. **The GDPR and other data related legislation should be coherent to help foster innovation and new technologies.**

[3] https://eeas.europa.eu/delegations/india/53963/node/53963_zh-hans?Consumers_to_the_Ministry_of_Electronics_and_Information_Technology_%28MeitY%29=
[4] Contribution of the EDPB to the report on the application of the GDPR under Article 97: edpb_contributiongdprevaluation_20231212_en.pdf (europa.eu)

I. Consistency mechanism should be improved to reduce fragmentation in the Member States and advance harmonization.

The consistency mechanism has been an important improvement introduced first in the Directive 95/46 and then further developed in the GDPR. The European Data Protection Board (EDPB) and national data protection authorities (DPAs) should play an important role to ensure that the GDPR is interpreted and enforced in a harmonized manner across the Member States, that individuals benefit from a coherent application of data subjects' rights and redress mechanisms, and that reversely, companies have the guidance they need to reach compliance while being able to tailor their compliance programs to their specific situation and needs. In that regard, BSA acknowledges a timely proposal for the GDPR Enforcement Regulation[5], currently discussed by the EU institutions.

Nevertheless, BSA is concerned that some DPAs are not fully committed to the consistency mechanism and still seek to assert their own jurisdiction, approaching GDPR compliance and enforcement differently. As a result, **regardless of the country of establishment for GDPR purposes, companies still have to cater to specific DPAs and their pronouncements on GDPR, which undermines the purpose of a pan-European Regulation.** For example, if one DPA issues more conservative guidance than the DPA of a company's main establishment, it is still a risk not to follow the more conservative DPA's approach, even though it is not the approach of a lead supervisory authority.

Thus, a harmonized privacy regime across the EU is not always a reality due to **different and sometimes conflicting views of the DPAs** or due to the **use of specific derogation clauses in the GDPR**, for example:

- Amid the COVID-19 crisis, BSA members observed a peak in the lack of harmonization among various Member States, particularly concerning **special categories of personal data**. For example, the narrow interpretation adopted by some DPAs to limit legal grounds for processing of special categories of personal data to explicit consent created uncertainty for companies seeking to use data to help address the COVID-19 crisis (including, at the very least, to ensure the safety of their employees) while continuing to abide by the necessary requirements for sensitive data processing. In this context, clarity and harmonization are paramount, and it is important to clarify that *public interest and legitimate interest could serve as legal basis for processing of sensitive data, within the framework of the current GDPR provisions*. In addition, to support a harmonized approach towards the processing of special categories of personal data, the regulators could outline best practices for a lawful processing of special categories of data[6].

- Regarding **data protection impact assessments** (DPIAs) for high-risk activities, which can be a helpful tool for businesses, the powers granted under Article 35(5) of the GDPR to DPAs to create their own list of processing operations subject to DPIAs has caused irregular approach to DPIAs at the EU level. In this regard, there are processing activities that could be subject to DPIAs in one Member State but not in another (i.e. Ireland's DPA and Germany's DPA consider the processing of genetic data as subject to DPIAs when at least one of the WP 248 guideline's criteria is met, whereas Spain's DPA considers any processing involving genetic data as subject to a DPIA irrespective of its purpose). A uniform approach regarding DPIAs should be adopted for all Member States.

[5] Proposal for a Regulation laying down additional procedural rules relating to the enforcement of GDPR - European Commission (europa.eu)
[6] Some useful research on this is available, for example: https://fpf.org/blog/workplace-discrimination-and-equal-opportunity/

- Absence of updated guidance on **anonymization** divides DPAs' approach to anonymization. Some DPAs (e.g. France's DPA) consider that the reidentification must be practically impossible for data to be anonymized, and other DPAs (e.g. Ireland's DPA) consider that the anonymization exists when the risk of reidentification is reduced to a minimum. Guidelines 05/2014 should be updated to respond to the need for a uniform anonymization standard in the EU, especially as the generative AI and other technologies emerge. Anonymization guidance should ideally adopt a practical standard to be implemented across all the EU Member States. In addition, anonymization should not be regarded as a processing activity that needs a legal basis, as it removes the possibility to identify data subject, or at least it should be covered by a "legitimate interest" processing ground under the current GDPR rules, as it is *per se* in the interest of the data subject.

- National DPAs' approach towards **IP addresses** differ in Member States. In the case C-582/14 Breyer v. Bundesrepublik Deutschland[7], the European Court of Justice considered that IP addresses are not always "personal data" subject to the GDPR. The court explained that dynamic IP addresses constituted personal data only if the processor of the IP address could link the IP addresses to an individual. Unfortunately, several DPAs have rejected the relative approach explained in the before-mentioned judgment and believed that IP addresses should always be considered personal data (e.g. decisions of Austria's DPA in December 2021, France's DPA in February 2022, Italy's DPA in June 2022). Only a very few DPAs followed the approach of the Breyer case (e.g. decision of Spain's DPA in December 2022). Therefore, guidelines (if not legal clarification of the GDPR) that IP addresses should not be considered personal data when they cannot be linked by an entity to a real person would help to address this problem. If this issue is not clarified, IP addresses in some Member States would continue being considered personal data in all cases, which would subject IP address to the GDPR's data transfer restrictions. This would be very problematic since both the functioning of the global Internet and advanced cybersecurity services depend on the cross-border processing of IP addresses. In addition, this could lead to further fragmented application of these GDPR provisions.

- **Children's consent –** providing Member States with discretion to define the age of a "child" brought an irregular approach as to what is considered a child under the GDPR (e.g. 13 year old can consent in Portugal whereas in Germany they need to be 16). This poses various compliance challenges for organizations, especially SMEs.

- Article 37(4) of the GDPR has empowered Member States' data protections laws to further extend the **scenarios where a data protection officer (DPO) must be appointed**. Where some countries (e.g. Portugal) have chosen not to go beyond the scenarios in Article 37(1)(a)-(c), others have foreseen additional scenarios where a DPO must be mandatorily appointed (e.g. Spain foresees up to 16 additional scenarios). This creates inconsistent requirements across Member States.

- Clearer **standards for calculation of administrative fines** and **uniform categorization of GDPR infringements** across EU Member states would be helpful for companies. Standards should focus on the proportionality of fines and in guaranteeing consistency across Member States. Categorization of GDPR infringements by Member States is irregular, i.e. failure to notify a data breach on time (Article 33(1) of the GDPR) or to internally document a breach (Article 33(5) of the

[7] 62014CJ0582 (europa.eu)

GDPR) is considered a "minor" breach in Spain and a "serious" breach in Portugal. The same data breach would therefore be subject to different fines in various Member States.

- BSA members have experienced that there is no universal **mode of cooperation and communication between businesses and the DPAs**. As such, DPAs' responsiveness, openness to cooperate and advice industry varies from Member State to Member State. Some DPAs are very responsive and cooperative, while others do not respond to requests for advice neither by phone, nor in writing, or take a very long time to respond.

In light of the above, fragmentation creates unequal interpretation of the GDPR across Member States. This significantly affects global companies operating in multiple Member States, as they need to introduce amendments to their business services to ensure they meet any additional or differentiating national requirements even to satisfy EU obligations. ***Therefore, not only should the EDPB issue more targeted and centralized guidance that promotes harmonized application of the GDPR's obligations, but the DPAs should also be granted sufficient human recourses to effectively advice and guide businesses, as well as provide timely responses to inquiries.***

In addition, **better coordination between the EDPB and the DPAs** is very important. Sometimes, the DPAs issue national guidance that contradicts the EDPB guidance. For example, the Spanish DPA has amended its cookie guidelines in January 2024, raising questions about the concept of free consent as explained in the EDPB guidelines. This potentially contradicts the EDPB guidelines. Therefore, it would be beneficial to compare the EDPB's guidance with those of DPAs' to ensure a uniform application of the GDPR across the EU. In addition, **continued alignment between the EU's DPAs and the UK's Information Commissioner's Office** even in a post-Brexit environment continues to be very important for companies operating in both jurisdictions.

The **EDPB guidelines** on GDPR provisions serve as a valuable reference, assisting in both preventing fragmentation and responding to it, especially when they include examples reflecting real cases and real-world situations. As many EDPB guidelines were adopted after the end of the two-year transition period, well-intended companies were facing and still face uncertainty on the exact nature of certain requirements and local fragmented DPAs' interpretations. Additional EDPB guidance in some areas would still be welcomed, specifically, in response to all the above mentioned fragmentation areas. In addition, core guidance pertaining to cloud-based examples or multi-party contracting examples could be helpful as well as clarification on reporting thresholds for data breach notifications, as 72-hour notification period can be too short to properly assess incidents and restricts the ability of companies to provide meaningful notifications.

Overall, the EDPB would benefit from being better connected to companies across-sectors and geographies to **take into account industry views**. The work of the EDPB could be more transparent and include more structured and improved ways to dialogue with stakeholders.

II. International data transfers toolbox should be strengthened to support global data flows.

Cross-border data flows are necessary for companies to operate globally and to provide services to their customers, across sectors and geographies.[8] The GDPR provides a list of mechanisms that can be used by

[8] https://www.globaldataalliance.org/downloads/GDAeverysector.pdf

organizations to comply with the Regulation's general principles and specific requirements when transferring personal data outside the EU and EEA. Different organization types and business models require the use of different transfer mechanisms that are not interchangeable. **It is important that businesses be able to use the full range of existing GDPR-compliant data transfer mechanisms**, such as: adequacy decisions (including on the EU-US Data Privacy Framework or EU-US DPF); certifications; codes of conduct; Binding Corporate Rules; and Standard Contractual Clauses. These mechanisms are critical to support global data flows and are built with strong safeguards.

BSA supports the European Commission's work on **adequacy decisions** and believes this authority should be used more broadly. However, the process that determines whether a country is adequate remains too time consuming and should be accelerated: as of February 2024, the EU had finalized 16 adequacy decisions, including for commercial transfers to the United States through the EU-US Data Privacy Framework. As of February 2024, more than 2,600 companies from across the US have self-certified for the EU-US DPF, including BSA members. Many of the companies certified are small- or medium-sized businesses, across industries.

BSA encourages the Commission to expand and speed-up adequacy decisions, considering their positive impact to economy, and the growing digital trade between the EU and third countries. Thus, BSA embraces the EDPB's recommendation[9] to the Commission to *develop, expand and multiply adequacy negotiations with third countries* (in particular, the ones that play an important role in the global digital economy and to which a particularly large amount of personal data is transferred from the EU) and international organizations (whose legal frameworks are essentially equivalent to that of the EU). Some BSA members expressed particular interest for the Commission to advance adequacy negotiations with other countries, including South Africa, Brazil, UAE, or Australia. In addition, BSA companies want to make sure that the EU-US DPF is a reliable permanent solution for transferring data between the EU and the United States and that it will stand the test of the European Court of Justice.

Among other data transfer mechanisms in the GDPR, EU lawmakers developed **Standard Contractual Clauses (SCCs)** so that organizations could transfer data to all the other countries whose regimes may not be recognized as essentially equivalent to that of the EU. In this case, the GDPR puts the burden on companies to apply strong safeguards when using the SCCs, so that data is protected at high levels wherever it travels. SCCs are an essential part of the day-to-day operations of companies across Europe, to transfer data with affiliates, vendors, customers and suppliers. BSA surveyed its members and found that 100% of respondents use SCCs; 70% rely on them as their principal transfer mechanism; 50% have more than one thousand contracts in place. According to a 2019 IAPP-EY report[10], approximately 88% of companies transferring data out of the EU rely on SCCs.

BSA welcomes the European Commission's work in 2021 updating and revising the SCCs, and bringing them in line with the GDPR. BSA members recognize the positive impact of the updated SCCs. For example, Modules 1-4 of the updated SCCs have helped BSA members regulate relationships that were not covered in the previous SCCs (e.g. regarding P2P or P2C transfers). Clauses 14 and 15 of the updated SCCs have also ensured that the SCCs remain in line with the latest case law of the European Court of Justice (e.g. Schrems II judgment and the transfer impact assessment requirements stemming from this judgment).

[9] EDPB "Contribution of the EDPB to the report on the application of the GDPR under Article 97": edpb_contributiongdprevaluation_20231212_en.pdf (europa.eu)

[10] IAPP-EY Annual Governance Report 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/

However, BSA members' experience exposed some **challenges remaining in the updated SCCs**:

- Insufficiencies and areas of uncertainty remain with respect to *transfer impact assessments* (TIAs). Clause 14 of the SCCs require exporter/importer carry out an in-depth *study of the legal framework of the territory* where the Importer is located. This triggers increased efforts in external resources to examine foreign legislation. Some importers (i.e. SMEs) may not have the resources to undertake this obligation. In addition, these increased efforts may not be sufficient to address in enough detail the entire legal framework of a territory, as there is no guidance/threshold that allows exporter/importer to understand when a TIA will be considered enough/satisfactory for a DPA. Although EDPB recommendations on supplementary measures have helped, uncertainty as to when a TIA will be considered sufficient before the eyes of a DPA still remains. In addition, the wording in Clauses 14 and 15 of the SCCs raise disputes in contract negotiations about who is responsible for conducting the TIA and whether the TIA needs to be shared with the other party.

- Likewise, this is another area of potential fragmentation as DPAs have recognized *additional measures* going beyond the non-exhaustive list of technical, organizational and contractual measures set forth in the EDPB's supplementary measures guidance, i.e. solution of France's DPA involving a proxy server which avoids direct contact between a user's terminal and Google's server. It is however unclear whether the supplementary measures recognized/proposed by one DPA would be also recognized in all EU Member States.

Binding Corporate Rules (BCRs) are a tool of significant importance for companies, including some BSA members but their review and adoption processes are burdensome and lengthy for both companies and DPAs. DPAs and EDPB should dedicate sufficient resources to facilitate these processes. BSA welcomes the updated EDPB's guidance on the BCRs for controllers, and encourages publication of the EDPB's guidance on the BCRs for processors.

While national codes of conduct may raise some practical usage concerns for global companies, BSA members believe that the **European Codes of Conduct** could be a strong and valuable compliance tool. The European codes of conduct strengthen compliance with the GDPR and enhance trust among users and DPAs due to their pan-European scope. These codes undergo a specific review by all EU DPAs, with the issuance of an opinion by the EDPB at the conclusion of the procedure. Its adoption procedure makes the European codes of conduct a very valuable compliance tool which oversees application of the GDPR and reinforces trust. However, codes of conduct usually take years to be drafted and approved due to the complex requirements to be met and therefore the stakeholders are often discouraged to launch them. Drafting a code of conduct requires extensive consultation and exchanges among the stakeholders and it can take a very long time to align all parties. Among the challenges are also the differentiating interpretation of the provisions of the GDPR by various stakeholders. As a result, to this day, codes of conduct, as well as certification mechanisms remain largely theoretical, hindering those willing to invest in such programs and thereby impacting public trust. Therefore, we would like to see the Commission actively promoting the creation and adoption of codes of conduct that can serve as adequate and independent transfer mechanisms.

BSA supports initiatives that make use of Article 46 of the GDPR to create **additional tools** to help address business needs in a legally and operationally sound manner, in line with the accountability principle. BSA members would welcome further certifications, including as they leverage existing international

standards such as the Service Organization Control (SOC) 2[11] and ISO security standards, which are both recognized certifications on the B2B customer side as well. However, any such tool shall not include protectionist data localization requirements as they do not improve data protection.

The misconception that **data localization** leads to better data protection is extremely dangerous. Data localization undermines the goals of the GDPR, which aim to ensure a high level of data protection and facilitate the free flow of data. BSA members' experience and recent research[12] show that GDPR-induced data localization threatens the ability to achieve integrated management of cybersecurity risks and limits the ability to employ state-of-the-art cybersecurity measures that rely on cross-border data transfers to make them as effective as possible. This also clashes with the controller's and processor's obligation of Article 32 of the GDPR to "develop appropriate technical and organizational measures to ensure a level of security appropriate to the risk", "taking into account the state of the art". In addition, data localization undermines information sharing within industry and with government agencies for cybersecurity purposes, which is generally recognized as vital[13] to effective cybersecurity. Thus, building on the GDPR's existing Recital 49, which rightly recognizes cybersecurity as a legitimate interest for processing, the EDPB could *issue guidance that acknowledges the importance of data transfers for cybersecurity purposes and clarifies that such transfers are consistent with the GDPR, in particular where they are deemed necessary to fulfil the obligations of controllers and processors under Article 32 of the GDPR.* All in all, ***a unified response by the EDPB and the European Commission expressing opposition to occasional calls by some DPAs to localize data should help promote the goals of the GPDR.***

III. Contractual and business relationships in a B2B environment should be addressed to further advance digital transformation and ensure smooth application of risk-based approach.

B2B software companies enable their customers' software-based operations in multi-layered environments. By offering trusted and responsible solutions for their customers' data processing needs, BSA members enable their customers to in-turn service their own clients across industry sectors. For the purposes of the GDPR, **BSA members often act as a processor, handling personal data on behalf of and pursuant to the instructions of a controller**. The customer/controller has its own compliance with the GDPR which varies depending on the types of data they collect and store, and the purposes for which they use it, and potentially additional sector-specific legislation relevant to data protection. Without much insight into how the controller uses their products and services, B2B software companies need to ensure they are meeting the controller's needs and are making available to them the tools and measures necessary for them to comply with the GDPR and any other relevant legislation.

The updated SCCs' provisions, governing the controller-processor relationship would gain from additional clarity to make the application of them as practical as possible, in particular in a cloud computing environment. Therefore, **BSA offers concrete suggestions below to address specific implementation challenges in B2B environments regarding the SCCs**:

- *Audit right requirements*: SCCs prescribe an audit right for the B2B customer (i.e. data exporter) which could be interpreted as an on-site audit (Clauses 8.9 of Modules 2 and 3). For most

[11] See ENISA's CCSL - Cloud Certification Schemes List: Cloud Computing Certification Schemes List - CCSL | Shaping Europe's digital future (europa.eu)
[12] Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures by Peter Swire, DeBrae Kennedy-Mayo, Drew Bagley, Avani Modak, Sven Krasser, Christoph Bausewein :: SSRN
[13] Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu)

processors (i.e. data importers in SCCs), it may be impossible to provide on-site audits given the number of customers most processors have. In addition, the scope of such audits may also involve accessing data and systems that other controllers similarly utilize from a software company, which would be in direct conflict with certain confidentiality agreements. It would be beneficial to clarify that processors are able to comply with the SCCs audit requirement by offering to make compliance certifications/third party audit reports available to the customer or offer to provide necessary information through other virtual means, in a tiered fashion where possible.

- *List of sub-processing agreements:* Clause 9(a) of Modules 2 and 3 requires that the data exporter keeps a list of sub-processing agreements and the data importer shall specifically inform the data exporter in writing of any intended changes to that list. This concept of listing may have made sense in an environment of cloud services delivered on premise. Now, however, the multi-layer environment in which B2B cloud companies tend to operate makes it operationally challenging to keep such a list and update it, which in practice is also no longer a cause of rejection by customers.

- *Obtaining data exporter's instructions*: SCCs require processors to only process the personal data in compliance with customer's instructions (Clause 8.1 of Modules 2 and 3). While we agree with this understanding of the role and obligations of data processors, it is important to clarify that the applicable agreement between processor and customer serves as customer's instructions for the processing of customer personal data, that processing initiated by users of the SaaS service will be deemed customer instructions, and that additional or alternate instructions may be separately documented and agreed upon in writing. Without such clarity, this language could pose a risk for processors if such instructions have not been expressed in a clear enough manner to the processor.

- *Obligation to notify about unauthorized access*: SCCs require processors to promptly notify the customer about a data breach, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (Clause 8.6(c) of Modules 2 and 3). This can pose a challenge for processors in the sense that processors may not have the visibility to be aware of such access. One way to address this issue could be to clarify that the obligation to notify is limited to instances in which the processor knows or should have known about such access. Adding a materiality or harm qualifier would also improve consistency with notification requirements in the GDPR.

Many software applications are now being operated as services from a cloud-based architecture (Software-as-a-Service or SaaS). EDPB Recommendations 01/2020 have had a significant negative impact on SaaS providers, who often need to access data in the clear to provide their services (especially, regarding the Use Case 6 of the Recommendations). According to this use case, where: (i) a controller transfers personal data to a cloud service provider; (ii) the cloud service provider needs to access to the data in the clear to execute the tasks; and (iii) the power grant to public authorities of the cloud service provider's country to access the transferred data goes beyond what is necessary and proportionate, the EDPB considers that the current state of the art is incapable of envisioning an effective technical measure to prevent this access. In this respect, according to the Recommendations, transport and data-at-rest encryption do not constitute sufficient supplementary measures. A similar scenario follows in Use Case 1 of the Recommendations, which requires encryption keys to be under the control of the exporter (or a trusted entity located in an adequate jurisdiction). This is equally problematic for SaaS providers. As they need to access data in the clear during the provision of its services, they would equally need access to the data-at-rest key. The mentioned use cases have negatively impacted SaaS providers and their provided

services, which depend on access to data in the clear. Considering the nature of SaaS services, the fact that the EDPB Recommendations were published 3 years ago and that alternative protections (i.e., cache only keys or contractual guarantees from SaaS providers) can achieve the same or similar levels of protection, it would be ***important to consider updating EDPB Recommendations 01/2020 to ensure that they do not unnecessarily restrict SaaS/Cloud services***.

BSA members are supportive of the **risk-based approach** that underlies the structure of the GDPR. However, they have identified various challenges related to the practical application of this approach:

- Several DPAs and EDPB have exhibited a tendency to question the applicability of the risk-based approach, particularly concerning *Chapter V of* the GDPR. We perceive a risk in the overly restrictive interpretation of the Schrems II judgment, suggesting that the risk-based approach no longer applies to data transfers under Chapter V of the GDPR. This creates a potentially dangerous gap between the risk-based approach, a core principle of the GDPR, and its practical interpretation by the EDPB.

- Implementing *privacy by design*, especially in the context of data transfers, poses challenges. Many provisions, such as those related to transfer impact assessments and standard contractual clauses (SCCs), necessitate a case-by-case assessment, making automation and the implementation of a risk-based approach particularly challenging.

- Some requirements introduced by the *principle of accountability* (i.e. records of processing activities) can be administratively burdensome for both, controllers and processors, without necessarily adding corresponding benefits for the data subject.

Regarding implementation of data **subject rights** under the GDPR, the experience of BSA members and, particularly, their business customers (data controllers) emphasizes the importance of maintaining a balance between the rights of the data subject and the interests of the controller and processor. However, several challenges persist, undermining this delicate balance:

- *Right to access personal data* (Article 15 of the GDPR) is being used by some data subjects to acquire more information than was originally intended by the GDPR. This goes for both employees and for consumers who might be motivated by something unrelated to personal data, but are exercising the right of access hoping that this could help them achieve what they are looking for. Also, experience of some companies shows that over the past years, data subjects' access requests have been used by lawyers to obtain information outside of the litigation process. In addition, there are cases when data subjects exercise *right to erasure* (Article 17 of the GDPR) to have data deleted to cover up their fraudulent activity. In both cases, the data subjects can be difficult to communicate with and often will not accept rejection to implement the request in case companies refuse to provide access to all data or to delete data. This creates a disbalance between data subjects' rights and data controllers' interests and it should be addressed by EU regulators.

- While the EDPB Guidelines 01/2022 include sections explaining the concepts of *manifestly unfounded and excessive*, there is a need for further clarification. For instance, "manifestly unfounded" is defined as when data subject's access request requirements are "clearly and obviously not met when applying an objective approach". The Guidelines insist on ensuring that the content and scope of the request are analyzed prior to determining if a request is "manifestly unfounded". However, it should be clarified whether current uses of data subject's access

requests (e.g. obtaining advance disclosure in litigation) can be considered "manifestly unfounded". Lastly, requiring data subjects to issue a statement confirming the bona fide belief of his/her request, as implemented in other more recent EU laws (i.e. Article 16(2)(d) of the Digital Service Act) should be considered, as means to impede/mitigate manifestly unfounded requests with the intention to harm a controller (i.e. fake/false data subject requests). In terms of "manifestly excessive", EDPB 01/2022 clarified controllers should assess "whether a reasonable interval has elapsed". Although factors, such as nature of the data, purpose of processing, type of request are explained, the *Guidelines should provide more objective criteria (i.e. approximate time intervals) to further guide the controllers*.

- In addition, some Member States (i.e. Ireland) provide for a *list of data subject access right exemptions* in their data protection law, whereas others (i.e. Spain) do not. Absence of written data subject access right exemptions further generates uncertainty and fragmentation across the EU. As a result, disclosure of data will be provided to data subject depending on the Member State where it exercises his/her data subject access right.

- In a series of judgements, the European Court of Justice has substantially raised the bar for controllers to comply with data subject's access to data requests. It would be helpful if regulators could seek for a reasonable balance and also give attention to the impact that data access requests could have on controllers and their organizations, recognizing *limits to what may be reasonably expected from a controller.* Another concern is the conflict of confidentiality rights (especially in an employment context) and privacy rights (e.g. relationship between the European Convention on Human Rights and, e.g. Barbulescu vs Romania case in the European Court of Human Rights, and the GDPR).

- EDPB Guidelines 01/2022 address *requests made via third parties (proxies);* however, the scope is limited to ensuring that controllers have evidence that proxies hold the legal representation of a data subject. In practice, most proxies require controllers to register in their respective platforms and respond to the requests within the proxy's interface. This delays response time periods (i.e. because only one user can be registered per controller, or because a controller receives requests from different proxies). *EDPB guidance should consider alternatives (i.e. proxies engaging with Controller's data subject right procedures, where applicable), to ensure resource optimization*.

- Experience of the companies also shows a need for guidance on procedures for data subject request management when *multiple data subject's rights requests* are received in a quick succession (i.e. request for deletion followed by access request).

- In addition to addressing the mentioned challenges and concerns in targeted EDPB guidelines, some measures could be introduced to *facilitate the response of data subject requests*. For example, online tools or user-friendly procedures could harmonize the receipt of uniform and consistent data subject requests, i.e. ensuring a request meets minimum requirements and thus avoiding controllers having to reach out to the data subject for additional information. These tools/procedures could ensure requests are being dealt with in an efficient manner.

In addition, experience of BSA members shows that the *GDPR sets the bar too high regarding data sharing and the secondary use of publicly available information.* The principles for secondary use should also apply to the scraping of publicly available data. Under the GDPR provisions, the original purpose and the secondary purpose must be set by the same controller. Thus, it might be implied that publicly available

data may not be re-used by a different controller. GDPR should recognize that individuals have made a lot of data available in the public domain and that a secondary use might well be compatible with the original purpose (even if set out by different controllers).

IV. GDPR and other data related legislation should be coherent to help foster innovation and new technologies.

The GDPR has provided a reinforced privacy framework to continue to protect the rights and freedoms of data subjects in light of emerging technologies and latest technological advancements. Importantly, the GDPR does not approach its requirements only from the perspective of protecting personal data; as the EDPB has made clear, the GDPR also serves the purpose of protecting other fundamental rights, including preventing discrimination and the right to human autonomy.

As the EU and international policy and regulatory landscape applicable to emerging technologies evolves, it is important to consider how the GDPR applies to new technologies such as AI and machine-learning to ensure the EU's approach remains consistent and do not create unnecessary burdens that would stifle European innovation. **The principles endorsed by the new EU (draft) legislation should stem from and be in line with the GDPR**. Also, it is important for the EDPB and the DPAs to continue working on recommendations and guidance in order to ensure smooth application of the GDPR provisions to the emerging technologies.

The EDPB, the DPAs, and the legislators should pay particular attention to the following elements:

- **The interplay between the GDPR and emerging AI regulation**, e.g. AI and its model collection vs principles of minimization, transparency and accuracy in the GDPR, or the interplay between generative AI and Article 22 of the GDPR. Establishing common principles that align the requirements of the GDPR and the draft EU AI Act could be beneficial for achieving harmonized compliance.

- **The need for a uniform position on anonymization practices**, as discussed in this submission. Guidelines 05/2014 should be updated to respond to the need for a uniform anonymization standard in the EU, especially as the generative AI and other technologies emerge.

- The rules, recommendations and guidelines for emerging technology, including SaaS and cloud services, **should not be unnecessarily and unproportionally restrictive**.

Regarding the interplay between the GDPR and new legislative initiatives, BSA and BSA members encourage the legislators and enforcement authorities to **ensure a consistent approach that supports responsible innovation.**

Key focus areas for legislators and enforcement authorities regarding the interplay between the GDPR and the draft **EU Artificial Intelligence Act** (draft AI Act):

- *Biometric data.* It will be important to ensure a consistent approach in case law is maintained between the draft AI Act and the GDPR on the definition of "biometric data".

- *Data minimization and data governance.* In many cases, the more information that is ingested by an AI model, the more accurate the AI model will be. However, this could raise tensions with the minimization principle of the GDPR. It will be therefore be important to understand how the principle of minimization will interact with the obligation to ensure training, validation and testing data sets remain representative, free of errors and complete (Article 10 of the draft AI Act).

- *Processing of Special Categories of Data where necessary to ensure bias monitoring, detection and correction of high-risk AI systems.* Another important interaction between the AI Act and the GDPR revolves around the use of special categories of data. Article 10(5) of the draft AI Act allows for the processing of special categories of data (as defined in the GDPR) by providers of high-risk AI systems when it is "strictly necessary for the purposes of ensuring bias monitoring, detection and correction". Article 10(5) of the draft AI Act however says this processing is "subject to appropriate safeguards for the fundamental freedoms of natural persons". It will be important to understand whether this provision will create a specific and additional condition for processing or whether providers of high-risk AI systems will have to rely on an Article 9(2) of the GDPR regarding processing of special categories of data for the above purpose. In the case of the latter, it will be important to understand what condition of Article 9(2) of the GDPR will be considered appropriate by the DPAs.

- *Automated decision-making and profiling*. The Guidelines on automated individual decision-making and profiling should be updated to reflect how automated decision-making interplays with new technologies (i.e. generative AI). Consideration should be given to examples of key factors that can "similarly significantly" affect data subjects in relation to AI decisions. Additionally, the Guidelines' section on Article 22(1)(b) of the GDPR (performance of a contract) should be updated to reflect whether it is possible to rely on AI beyond the example that is currently available (use of automated means for recruitment processes).

Key focus areas for legislators and enforcement authorities regarding the interplay between the GDPR and the **EU Data Act:**

- The rules and enforcement regarding personal and non-personal data processing should provide more legal clarity for controllers and processors. For example, *mixed data sets* (with personal and non-personal data) are treated as personal data under the GDPR, while non-personal data sets are subject to other data transfer rules as per the Data Act.

- *Prevention of dual enforcement*. It is important for all stakeholders to understand how enforcement actions under both regulations (the GDPR and the Data Act) will be addressed and how dual enforcement (i.e. an infringement being subject to Data Act and GDPR fines) will be prevented.

Key focus areas for legislators and enforcement authorities regarding the interplay between the GDPR and the **Digital Services Act:**

- *Notice and action mechanism and minimization principle*. Recital 50 of the Digital Services Act (DSA) states that the notice and action mechanisms "should allow, but not require, the identification of the individual or the entity submitting a notice". On the other hand, Article 16(2)(c) of the DSA states that hosting service providers shall enable and facilitate the submission

of notices containing "the name and email address of the individual or entity submitting the notice". It will be important to understand how Recital 50 and Article 16(2)(c) of the DSA will interplay with the GDPR. In particular, if a hosting provider can oblige a recipient of a service to provide his/her name and email address when submitting a notice and action, and if affirmative, how will this interplay with the principle of minimization enshrined in Article 5 of the GDPR.

Finally, BSA recognizes a particular role for **privacy- and confidentiality-preserving technologies** such as *Privacy Enhancing Technologies* (PETs) and *Privacy-Preserving Machine Learning* (PPML). Pseudonymous datasets with state-of-the-art technical and organization measures can support privacy and confidentiality, and hence BSA recommends further exploring when and where these solutions can offer alternative or complementary solutions to e.g. anonymization techniques. Using such solutions can foster innovation, including machine learning that is used to advance societal goals.

Closing remark

BSA thanks the European Commission for providing the opportunity to comment on these important matters. For further information please do not hesitate to contact Irma Gudziunaite, Director, Policy – EMEA, irmag@bsa.org.