Brussels, April 2020

BSA | The Software Alliance's feedback on the implementation of the EU General Data Protection Regulation.

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, welcomes the opportunity to provide feedback on 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. 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 Commission conducts its evaluation, it is important to assess if the GDPR is working as intended to successfully harmonize 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 improves the EU single market.

Within EU and EEA countries[2], the GDPR has brought valuable harmonization of applicable rules and increased transparency of data handlers' responsibilities. It 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 effectively 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 most-suited approach given their business model, activity and risk profile. It also importantly enshrines free movement of personal data as an important pillar of the EU acquis.**

The GDPR has become a global point of reference at a time when many countries are developing or updating their privacy laws and regulations, emulated by the GDPR. The overarching goal of the GDPR –

[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, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cadence, Cloudflare, CNC/Mastercam, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

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

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

to provide high levels of privacy protection – is 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.

BSA offers this feedback based on member companies' practical experience of GDPR implementation and highlights areas that could benefit from further attention from the European Commission and DPAs. BSA concurs with the European Data Protection Board (EDPB)[4] that it is premature to revise the legislative text at this point in time and welcomes continued discussion with its members to further improve the GDPR in practice.

COVID-19 test case

The difficult times stemming from the COVID-19 pandemic are challenging our societies in unprecedented ways. They are also testing the GDPR against unpredictable yet very real situations and have highlighted among others the high-level of adoption of software technologies across economies and communities, including technologies that facilitate the ability of companies and employees to work remotely and technologies that enable contract tracing applications that are currently being developed. BSA members are taking responsible action to address the COVID-19 crisis in an number of ways, including by providing free access to their services; advice and help regarding remote work; helping track and disseminate information on the spread of the virus; supporting medical research efforts and the production of personal protective equipment; preventing the spread of malicious campaigns including email spam, malware, and ransomware; and partnering with governments to keep people safe.[5]

Some of these activities require by nature processing of sensitive personal data, including in the employment context. This triggers the application of additional GDPR provisions, to which Member States can add specific conditions under Article 89. This situation has highlighted the need for a harmonized approach to data protection, as companies and public authorities use data in connection with urgent efforts to combat the pandemic and to adapt to pandemic remediation measures. For example, the narrow interpretation adopted by some DPAs to limit legal grounds for processing of sensitive data to explicit consent creates uncertainty for companies seeking to use data to help address these dramatic circumstances (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.

[3] https://eeas.europa.eu/delegations/india/53963/node/53963_zh-hans?Consumers_to_the_Ministry_of_Electronics_and_Information_Technology_%28MeitY%29=

[4] EDPB "Contribution of the EDPB to the evaluation of the GDPR under Article 97"

[5] https://www.bsa.org/covid19

Consistency mechanism & European Data Protection Board

The consistency mechanism has been an important improvement introduced by the GDPR over the Directive 95/46. The EDPB should play an important role to ensure that the GDPR is interpreted and enforced in a harmonized manner across Member States, that individuals benefit from a coherent application of 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.

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 a risk not to follow the more conservative DPA as they may not respect the one-stop-shop principle. As noted above, we have seen this lack of harmonization arise particularly in the context of COVID.

The EDPB guidelines on GDPR provisions are a useful reference but additional guidance in some areas would be appreciated. As many guidelines were adopted after the end of the two-year transition period (with some still to be finalized, for example on codes of conduct and certifications), well-intended companies face uncertainty on the exact nature of certain requirements and DPAs' interpretations. Specifically, updated guidance on the definition of controller/processor should bring further clarity on role classification, particularly important in the context of complex processing operations. Companies that need to establish whether to conduct a balancing test, for instance in the context of data protection impact assessments (DPIAs), would benefit from uniformity and guidance on DPIA thresholds and triggers. Local differences created by the opt-in and opt-out lists (Article 35 (4) and (5)) bring harmonization risks. More 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.

International data transfers

Cross-border data flows are necessary for companies to operate globally and to provide services to their customers, across sectors and geographies.[6] The GDPR provides a list of mechanisms that can be used by 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 continue using the full range of existing GDPR-compliant data transfer mechanisms, such as: adequacy decisions (including on the EU-US Privacy Shield framework or Privacy

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

Shield); certifications; codes of conduct; Binding Corporate Rules (BCRs); and Standard Contractual Clauses (SCCs). These mechanisms are critical to support global data flows and are built with strong safeguards.

BSA supports the Commission's work on adequacy and believes it 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 April 2020, the EU had finalized 13 adequacy decisions, including for commercial transfers to the United States through the Privacy Shield. As of April 2020, more than 5,300 companies from across the US are using the Privacy Shield, including at least 18 BSA members. More than 70 percent of the companies certified are small- or medium-sized businesses, across industries. BSA encourages the European Commission to finalize rapidly its adequacy proceedings with South Korea and with the UK to ensure EU-UK data transfers are not disrupted once the UK effectively becomes a third country.

EU lawmakers developed the 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 European Union. In this case, the GDPR puts the burden on companies to apply strong safeguards when using the clauses, 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[7], approximately 88% of companies transferring data out of the EU rely on SCCs, while 60% use Privacy Shield.

However, both the SCCs and the Privacy Shield are currently challenged before European Courts, raising significant concerns about the viability of both mechanisms and suitable alternatives.[8] **Were SCCs and/or Privacy Shield to be invalidated, it would not only cause massive disruption to economic operators in Europe and beyond, it would also deprive Data Protection Authorities from important tools to enforce EU individuals' rights under the GDPR.** It is critical for EU policymakers to continue to work with partner countries and stakeholders on short-term alternative and long-term solutions. BSA therefore welcomes the EC's firm commitment to defending both the Privacy Shield and SCCs as critically important transfer mechanisms which should be upheld, and to prepare revised SCCs to bring them fully in line with the GDPR.

Article 46 of the GDPR foresees additional tools to provide the necessary safeguards such as BCRs, codes of conduct and certification mechanisms. 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 should look to dedicate sufficient resources to facilitate these processes. Updated guidance on the approval process, the identification of lead supervisory authority and transferring BCRs in light of Brexit could also contribute to improving the efficiency and business-friendliness of this mechanism. To this day, codes of conduct and certification mechanisms remain largely theoretical, hindering those willing to invest in such programs and thereby impacting public trust. **BSA supports initiatives that make use of Article 46 to create additional tools to help address business needs in a legally and operationally sound manner, in line with the accountability principle**. BSA

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

[8] BSA has been admitted as an Amicus to the Court in both challenges. See press release: https://www.bsa.org/news-events/news/bsa-welcomes-irish-high-courts-decision-to-grant-bsa-amicus-status

members would welcome further certifications, including as they leverage existing international standards such as the Service Organization Control (SOC) 2[9] and ISO security standards, which are both recognized certifications on the B2B customer side as well.

Contractual and business relationships in a B2B environment

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, they are more often than not the processor acting on 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.

BSA members welcome the current efforts by the Commission to update the SCCs (per Article 46 (2)) to bring them fully in line with the GDPR. Ongoing litigation may also lead to additional, possibly significant, changes to the current SCC templates. BSA notes that the implementation of such updated clauses will be extremely time and resource-intensive, as for some organizations it will apply to thousands of contracts. This process should not compromise what has already been signed among the companies and shall not have retroactive effects. **Some existing SCC provisions governing the controller-processor relationship would gain to be clarified to make the application of these provisions as practical as possible, in particular in a cloud computing environment.** BSA offers concrete suggestions below to address specific implementation challenges:

- *Audit right requirements*: SCCs prescribe an audit right for the customer (i.e. data exporter) which could be interpreted as an on-site audit (Clauses 5(f) and 12(2)). For most 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 SCC audit right 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**.

- *Approval of sub-processors*: The GDPR and SCCs require the processor to inform and obtain customer's "prior written consent" to contract sub-processors (Article 28 (2); Clause 5(h)). Many software applications are now being operated as services from a cloud-based architecture (Software-as-a-Service or SaaS). Requiring prior written consent to enlist a sub-processor can become a significant pain point for both controllers and processors if they are required to obtain new consent for each respective sub-processor – given the thousands of customers' unanimous consent that would be required, the high volume of sub-processors used in many SaaS

[9] See ENISA's CCSL - Cloud Certification Schemes List https://resilience.enisa.europa.eu/cloud-computing-certification

environments and the unique (and sometimes non-fungible) role they play. Rather than requiring such prior written consent, the protection of the GDPR and contractual obligations may be properly passed on by the controllers to processors onto sub-processors, as contemplated in Article 28 paragraph 4. **Therefore, it would be helpful to clarify that the customer agrees to the use of sub-processors through a general written authorization**. In addition, Clause 11(4) requires that the data exporter keep a list of sub-processing agreements and update it on an annual basis. This concept of listing may have made sense in an environment of cloud services delivered on premise, which may have been the focus of regulators when the current SCCs were adopted. Now, however, the multi-layer environment in which B2B cloud companies tend to operate makes it operationally challenging to keep such a list updated, 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 5(a)). 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.

- *Notification of unauthorized access*: SCCs require processors to promptly notify the customer about any accidental or unauthorised access (Clause 5(d)(ii)). 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.

- In view of the above, processor-to-sub-processor SCCs should be provided by the European Commission to **simplify the contractual structure between controllers, processors and their sub-processors.** First, this will allow a processor to better select and control the sub-processors they work with, and ultimately achieve more security. This would be useful in the scenario in which an EU controller transfers personal data to an EU processor and the personal data is subsequently transferred to a non-EU sub-processor. Second, it will also help consistency and efficiency of contractual practices.

GDPR and emerging technologies including Artificial Intelligence [10]

The GDPR includes provisions that impact Artificial Intelligence (AI) development and use. As the EU and international policy and regulatory landscape applicable to AI evolves, it will be important to consider how the GDPR already 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

[10] For more information, see BSA filing to the High-Level Expert Group on Artificial Intelligence https://www.bsa.org/files/policy-filings/06062019bsasubmissionaihleg.pdf

innovation. For example, the GDPR defines "personal data" broadly, as any information that directly or indirectly identifies or could be used to identify natural persons (Article 4(1)). This broad definition can capture data used to engineer and train AI systems, as well as data used by AI systems to generate predictions and make recommendations. GDPR also applies heightened protections to certain uses of personal data, such as use of biometric data, profiling, and automated decision-making without human intervention. The GDPR comprehensively regulates the use of personal data, including in connection with the lifecycle of an AI tool that uses personal data, from inception to deployment.

Importantly, many of the principles endorsed by the High-Level Export Group on Artificial Intelligence Guidelines do mirror the GDPR's. The Guidelines set out seven requirements for "Trustworthy AI": accountability; privacy and data governance; human agency and oversight; diversity, non-discrimination and fairness; technical robustness and safety; transparency; and societal and environmental wellbeing. Virtually all these requirements are already contained in the GDPR. Importantly, and in the broader context of emerging technologies, the GDPR does not approach these 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.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315