BSA Position on the European Commission’s Draft General Data Protection Regulation

February 2012

The BSA | The Software Alliance1 is the leading global organization dedicated to promoting a safe and legal digital world. Comprising the world’s leading innovators, BSA companies deliver a range of digital products and services to consumers across the EU. For each of our members – in all of their offerings – data protection is a cornerstone upon which everything else is built.

BSA welcomes any enhancements to the Regulatory framework which can protect individuals’ privacy while ensuring that personal data can be processed and move freely through the ever-expanding digital economy. BSA believes that the review of the existing framework represents a major opportunity to both improve privacy and advance the digital age in Europe by crafting forward-looking solutions that are precisely focused to achieve their goals: maximizing individuals’ privacy and leaving breathing room for innovative development of new Internet-based products and services.

A balanced, no-nonsense and utilitarian Regulation is needed that can help citizens better understand and control how their data is processed, give regulators a tool that can grow and evolve with the technology it aims to govern, and provide data controllers, with the legal certainty they need to develop new services. Those facts, in turn, will foster user trust and confidence in the online experience. Such trust is essential for the growth of the digital economy.

1 BSA | The Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.

Real Solutions for Real Technologies

Technology is an integral part of today's life and the backbone of every modern economy. People, business and Governments rely on, and expect, technological solutions to everyday problems. Consumers enjoy and expect – and often largely take for granted – a seamless, rich, diverse and rapidly expanding variety of online services spanning from content (online newspapers) and media (radio, online TV stations) to services (blogging portals, social networks, search) and communication (VoIP, e-mail). While the explosive growth of the Internet brought these tremendous social and economic benefits, Internet technologies also fundamentally expanded how, where and by whom data is collected, transmitted and used. A prime example is the rapid growth of cloud computing which offers a great promise for Europe, with estimates indicating that the cloud will create a million new jobs and several hundred thousand new small- and medium-sized enterprises and drive down the cost of ICT for the public and private sector.2 In order for these benefits to continue and the promise of cloud computing and other new technologies to be realized, users must have confidence that their personal data is safe.

The Framework must allow for achievable results and set the right level of expectations. For example, certain elements of the proposal – particularly those relating to online technologies, such as the Right to be Forgotten, Privacy by Design, Profiling, and the consent regime – need refining in order to make them achievable. Ultimately, the strength of the revised Framework will depend on whether it can be implemented in practice, accurately reflects citizens’ expectations, and remains consistent with the architecture and design of key technologies. Overly broad and unreachable goals will provide no solutions at all.

Ensuring an Internal Market for Data Protection

Legal Certainty

BSA supports the decision of the European Commission to replace Directive 95/46/EC with a directly applicable Regulation because of its ability to bring legal clarity on the rules that apply and to reduce confusion and inefficiencies associated with the current patchwork of EU data privacy laws. If correctly drafted, a Regulation could bring greater legal certainty for both businesses and consumers and ensure a higher level of privacy for EU citizens.

Main Establishment

We welcome the decision to create a “one-stop shop” with a lead Data Protection Authority (“DPA”) based on the concept of a “main establishment” regime. This approach will facilitate and encourage companies operating in multiple EU markets. The success of this approach will

---

depend, however, on the requirements that determine which DPA is responsible being absolutely clear.

**Administrative Burdens**

Drawing from the well-established international concept of “accountability,” the Regulation will require controllers and processors to be “responsible” for how they handle data. For example, the Regulation contains many new ex ante requirements, including, maintaining records, conducting Privacy Impact Assessments (PIAs) in certain circumstances, and appointing a Data Protection Officer. Controllers also would be required to verify the effectiveness of these measures, which may be carried out by “independent internal or external auditors”.

These reforms could help keep data safe and build consumer confidence. However we are concerned that introducing ex-ante controls, combined with wide-ranging prior authorization requirements, and backed-up by a significant sanction regime, is actually to misconstrue the accountability concept. Introducing layer upon layer of control moves the EU away from a principles-based framework to a control and compliance regime which is likely to actually reduce incentives for companies to make data protection a competitive advantage.

**Administrative Sanctions**

The Regulation introduces high administrative sanctions (up to 2% of the annual global turnover). We believe that a “one-size-fits-all” approach, which applies the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely negligent, is inappropriate. The fact that administrative sanctions for non-compliance with ex-ante obligations are based on loosely defined criteria (e.g., “negligence”), creates significant legal and financial exposure for many companies – particularly smaller enterprises. High fines, combined with rules that would diminish DPAs’ discretion by requiring them to impose fines, could be extremely detrimental to the survival of start-up companies and innovative SMEs and disproportionate to the harm caused to data subjects. Moreover, any automatic assessment of penalties will deter self-reporting, reducing overall transparency, security and privacy. Such a regime significantly raises the costs and associated risks of introducing new products and services into the market while neither reducing the risks to data being processed nor providing added protection for consumers.

**BSA Recommendations**

- The definition of “main establishment” must be based on objective criteria that recognizes the nature of today’s global business operations and corporate structures and allows a controller and processor to determine the competent authority, based the enterprises the place of main establishment.

- BSA believes that it is important to encourage companies to be responsible by providing...
clear benefits for doing so. We therefore recommend a qualified and constructive approach to administrative requirements, one that is focused on reducing risk to data being processed and which rewards companies that demonstrate responsibility and adopt and validate particularly rigorous data protection programs. One way to do this would be to allow such companies to be eligible for reduced sanctions in cases of breach.

- We recommend the removal of the prior authorization requirements in Article 34, which – given their potentially huge scope of application – are likely to create an enormous and unworkable administrative burden for supervisory authorities, with no appreciable benefits for data subjects.

- The Regulation should ensure that punitive sanctions are reserved for truly bad actors. We believe that an effective data protection regime requires meaningful sanctions in cases of serious violations. Sanctions need to be carefully calibrated so as not to deter companies from operating and investing in Europe.

- We would caution against introducing statutory sanctions. Sanctions should be tied to the potential harm caused by the infringement and a distinction needs to be made between the penalties appropriate for each level of culpability. A precise criterion is needed for what constitutes “intentional” and, most importantly, “negligent” activities by an individual in an enterprise.

- It should be clearer that the administrative sanctions can only be levied by the lead DPA in the jurisdiction of main establishment.

**Ensuring Technology Neutrality and Focusing on Substantives Outcomes**

**A Future-Proof Framework**

The current legal framework has remained relevant and appropriate as the Internet has evolved and matured because it is technology neutral. Europe’s new data protection regime needs to be flexible, adaptable, relevant and technology-neutral and avoid creating moving targets for businesses. The rules need to recognise and take into account the fast-paced and changing digital environment. Consumer/social behaviour and norms as well as the use of the Internet (Social networks, eCommerce sites, user-generated content, blogging, etc.) constantly evolve. Today’s small businesses, start-ups and emerging technologies could be the leading forces in the digital economy tomorrow, but like all businesses they need a secure regulatory environment in order to attract the investment that is needed to develop innovative products, services and technologies.
Ensuring Substantive Outcomes

BSA members fully support the substantive goals of the Regulation: increased predictability, transparency, and accountability and clear rules for both providers of data services and users. We are strongly of the view that these goals are best achieved by providing flexibility to entities subject to the Regulation on how best to fully comply with the Regulation’s goals while providing breathing room for those entities to update their implementation as technology improves and evolves and as new threats to privacy emerge.

We believe prescriptive rules mandating specific procedures or technologies to achieve privacy outcomes should be avoided. Severe mandates will not stand the test of time and will dampen R&D and the further development of the Internet. Rigid rules will not lead to an increase in privacy protection standards and practices as snapshot-in-time; such rigid rules will most likely not promote compliance, but rather may encourage creative circumvention of underlying policy goals. Rigid rules are also likely to chill the investment and innovation of privacy protection technologies and will turn privacy protection into an administrative box-ticking exercise. With this in mind we note with concern:

**Secondary legislation:** Throughout the current draft text, for areas such as data portability, security of processing and certification schemes, the Commission is granted substantial authority to adopt delegated and implemented acts. These acts could include introducing technical standards, design requirements and criteria for technical measures and procedures. The Commission’s ability to propose secondary legislation in a wide number of areas threatens to complicate, rather than simplify, data protection. If new rules are regularly adopted, it effectively means that the benchmarks for data protection are always changing and it becomes virtually impossible for enterprises ever to achieve compliance. Further, if the Commission chooses to adopt highly prescriptive measures or dictate specific technology outcomes it could hinder innovation in privacy protection and lead to sector-specific legislation – negating the harmonization goal of the Regulation.

- **Prescriptive Requirements:** The proposed framework focuses on very specific requirements and mandates how fundamental principles should be applied. In order to deliver effective privacy protection, rules should focus on substantive outcomes rather than on specific procedures. The rules should establish a high level of baseline practices, require companies to be held accountable to them, and be enforceable. Overburdening companies with specific procedures and requirements that do not add protection to citizens will harm innovation and new ideas.

- **Profiling:** existing language on “automated decisions” has been extended in the draft Regulation to a loosely-defined category of data processing called “profiling”. In doing so the new Article 20 makes two significant and incorrect assumptions: that any automated decision amounts to profiling; and that profiling necessarily identifies an individual. As
such these provisions threaten to subject a vast range of legitimate data processing activities - including any processing of anonymous data - to additional controls, without consideration for the actual privacy implications of the processing in question, and without consideration for the many positive impacts of profiling. BSA recognizes that safeguards are needed against data processing that produces negative legal effects or adversely affects a data subject. However profiling techniques and technologies have many positive impacts - such as improving or customizing services for similar customers, or for anti-fraud or accounting purposes - which are fundamental to the success of the internet should not be prohibited under the Regulation.

BSA Recommendations

- **Controllers and processors should not be subjected to prescriptive requirements in the form of technology mandates;** they should have the flexibility to achieve their legal obligations and the substantive outcomes sought after by the Regulation. Legislation that mandates technologies and prescribes specific procedures brings no added value in privacy protection. Such rules could lead to rigid sector-specific legislation – negating the harmonization goal of the Regulation.

- **We strongly support the principle of Privacy by Design.** All of our member companies already ascribe to such an approach to developing new products and services. However, Privacy by Design should be considered a process for ensuring that data protection is carefully considered in the design and implementation of products and services. It should not be based on prescriptive and specific technologies. Imposing design mandates on particular technologies would hinder, rather than promote, user privacy and security.

- **BSA recommends that, as part of Privacy by Design, the Regulation encourage innovators to assess the full universe of potential privacy risks and make appropriate decisions about privacy designs and settings.** Although the intention behind the new Privacy by Default obligation may be well founded, it is unclear what this obligation entails, which could have unintended consequences, such as impairing innovation, limiting functionality and creating user frustration.

- **Right to be forgotten:** BSA recommends the Regulation should limit the right to be forgotten to data retained by and under the control of the controller and reasonably accessible in the ordinary course of business. The right should extend only to a user’s own data (i.e., data that a user inputs directly). For user convenience, service providers should also be permitted to retain data for a limited period in order to re-enable users where users expressly request this. Users should have a significant degree of choice and control over their data wherever technically feasible, but to be workable the right...
cannot obligate companies to do that which is technically impossible. The existing Directive already includes important rights and principles relating to the legitimate and proportional use of data as well as the erasure of data. These considerations are exceptionally important in the context of providing effective security tools. While the timely deletion of obsolete data can help protect the privacy of data subjects, this requirement should not subject data controllers to obligations that they are ultimately incapable of satisfying.

- **Data portability**: BSA strongly supports giving individuals more control over their data – increased data mobility is not only good for users, it’s also good for business and overall ecosystem. But the Regulation goes beyond this and requires that data be returned to users in a way that allows for a transfer to other services. The Regulation also gives the Commission the power to impose technical standards governing the format in which data is to be returned. The Regulation should recognize the technical reality that the right to export data does not necessarily mean that such data can be used “as is” in other services. Companies use a wide range of mechanisms to enable the export of data depending on the technology, service and functionalities involved. Mandating a single format for data transfer will require technology providers to change other aspects of their products and services which may result in less functionality, less diversity and a worse overall user experience. BSA proposes a solution that provides users a right to port the data they had originally created but allows industry to decide on formats and technical modalities of returning user data back to users based on a variety of technical and commercial factors – including an emphasis on ease of use and the prevalence of a particular format and method **Profiling**: BSA agrees that safeguards are justified where processing can adversely affect a data subject. However, we urge recognition of the positive impact of profiling (e.g. for improving or customizing services for customers, or for anti-fraud or accounting purposes) and that some processing activities can be in the legitimate interests of the data controller. This should be recognized in article 6.1.f.

**Ensuring Security in the Online World**

Privacy in the digital age can only be achieved if the Internet environment is secure. The Regulation should ensure that security technologies can continue to be developed and deployed based on identified threats and that privacy rules fully support and promote the development and deployment of effective security technologies. Computer systems/networks – and, as a result, EU citizens online – are continuously faced with a barrage of increasingly sophisticated and complicated attacks. Companies not only need to ensure that the user data
they collect, process and store is properly protected against cyber threats but they also must guarantee the ongoing security confidentially, integrity, resilience and availability of the network and systems providing services. The importance of security considerations applies beyond the realm of privacy and includes the availability of broadband and wireless networks, vital communication systems and the critical infrastructure that runs hospitals, energy grids and financial systems among many others.

Given the current online threat environment, ICT security companies that combat botnets and other serious security threats online must be able to process certain data to perform their duties and ensure network and information security. In addition, security systems and technologies deployed by a wide range of entities – including banks, hospitals, retailers, e-commerce web sites and governments – all process certain data to prevent malicious attacks and information security breaches. It is therefore vital that the ability of these critical infrastructure providers to legitimately process such data to protect systems that are relied upon by EU citizens is not put at risk.

Breach Notification

A breach notification obligation, properly implemented, can serve as an important instrument to enhance network and online security and thus foster trust and confidence in the digital world. It would motivate entities to ensure robust protection for personal data while enabling data subjects to take action to protect them in the event their data is compromised.

BSA Recommendations

- We recommend including an explicit clarification in a legal binding article that processing data for security purposes constitutes a legitimate interest. Recital 39 of the current Draft Regulation recognizes this need. BSA calls for this language to be included in a binding article to ensure legal consistency across the EU and provide legal certainty for those companies that need to process certain data to provide network and information security.

- BSA recommends the adoption of a harm-/risk-based system with regard to breach notification. This would avoid over-notification and desensitizing consumers. Not all breaches are of equal importance or pose the same level of risk. To ensure the regime is effective, controllers should be required to notify data subjects and/or regulators of a breach only when there is significant risk of serious harm to the data subject. Criteria to be considered in making this assessment could include the type of data involved and its sensitivity; the nature of the breach; and the type of harm threatened by the breach. There should be a “safe harbor” from notification to both supervisory authorities and data subjects for data that has been rendered unusable, unreadable, or indecipherable through technological protection measures. The current proposal only provides a notification exemption to data subjects.
The timeframe for notification should be modeled on the regime in the ePrivacy Directive, which calls for notification “without undue delay” once a company has been made aware of the breach. The currently envisaged 24-hour notification timeline does not give companies sufficient time to properly assess the implications and nature of the breach or put in place effective solutions. In practice, depending on the nature and scope of a personal data breach, the data controller will require more time to understand the nature of the breach, who is affected, and whether the breach poses a substantial likelihood of harm to the data subjects involved. In addition, severe penalties for non-compliance should be reserved for those controllers who willfully and repeatedly fail to notify.

Context is Everything

The complex nature of today’s digital environment has led to an explosion of the use of information technology for everyday communication and information processing.

The response of the current proposal to these new developments is to significantly broaden the type of data considered to be “personal data” without consideration for the context in which data is being collected or used. This is ill-suited to today’s complex environment, which requires a more flexible and context-based approach to determine when robust protections for data should apply, considering the different levels of potential harm to individuals and uses of data.

The current proposal parts from the existing approach by expanding the definition of personal data beyond data that the controller can use to identify the data subject. It defines “data subject” to cover anyone “who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person”. This blanket approach does not address the issue of how closely related, or the proximity, to an individual data needs to be for identification to actually occur. There are legitimate reasons and circumstances – such as in the security context – where organizations need to process information relating to an individual in a manner that does not impact their privacy and that should not trigger the same core obligations and protections that rightly apply in different contexts. The regime must also recognize circumstances where organizations may have a legitimate reason to process data that does not relate to an identifiable individual in some manner and as such that cannot simply therefore be classified as personal data.

An overly broad definition of personal data that ignores the nature and context of the data being processed will have an adverse effect on the future development of the European information society, and may actually undermine individual privacy. By diverting resources from value
creation to unnecessary administrative compliance, it is also likely to discourage entrepreneurship and innovation.

**BSA Recommendations**

- **Adopt a context-based approach to personal data defining data as “personal data” if the controller could actually identify the specific person to whom the data relates.** Such an approach would be proportionate, as it would recognize that safeguards must apply where data subjects are identifiable by the data controller.

- **New categories of data – “anonymous data” and “pseudonymous data” – also could be recognized.** The former would refer to data that could never be used to identify an individual and therefore would not be subject to the regime. The latter would cover data relating to an individual to which a pseudonym is attached (such as a code, or alias) and would be subject to a less stringent set of rules than personal data.

- **The scope of personal data should not be expanded to apply in a blanket manner to other forms of data, such as location data.** The existing definition is flexible enough to cover any data – including location data – where that data relates to an identified or identifiable person.

- **We caution against introducing a “one-size-fits-all” approach to consent requirements regardless of risk or context.** When linked to the current proposed definitions of “personal data” and “data subject”, the proposal that consent must be “explicit” by either a “statement” or “clear affirmative action” would in effect require a single, standard form of consent regardless of whether a specific data subject can reasonably be identified or of the context in which consent is obtained or the data is used. There would not be any scope to adapt the form of consent to the specific context in cases where anonymous or pseudonymous data is concerned; a single requirement for “explicit” consent would be disproportionate. The Regulation should permit innovators to use different mechanisms to obtain consent that reflect how and in what contexts consent is obtained and data will be used.

**International Data Transfers**

European citizens and organizations now routinely move data between countries, both within and beyond the EU, to deliver the services consumers request in the most effective, cost efficient and therefore competitive manner. Flexible and efficient legal mechanisms must be in place to ensure that this can be done, while at the same time guaranteeing the security of data of EU origin regardless of its geographic location. Although we welcome many of the proposed reforms related to data transfers to third countries, we are concerned that under the proposed
Regulation, many companies would need to combine different compliance mechanisms with no single solution enabling the data transfers necessary for the activities with a global reach.

**BSA Recommendations**

- We welcome the approach in the current proposal regarding Binding Corporate Rules (BCRs), which has now been extended to cover data processors. However, the Regulation should take into consideration that enterprises that operate in many jurisdictions should be free to include only certain of their subsidiaries in their BCR, depending on their needs and in line with the flexibility characterizing this instrument.

- The Regulation introduces important new mechanisms to facilitate the secure flow of personal data, including in the cloud. These mechanisms include new rules on "standard" contractual clauses. We welcome these measures. But we also believe that cloud processors and others should be encouraged to go beyond the "baseline" safeguards set out in the Regulation in certain contexts. Where controllers and processors have practical experience that suggests that additional safeguards are appropriate to protect data, they should be incentivized to adopt these safeguards. Our amendments create a mechanism to do this. Specifically, our amendments:
  - propose a change to Article 42 to make it clear that organizations can offer supplemental, legally binding protections (e.g., data processing agreements) in addition to the protections included in the standard clauses,
  - propose a further change to Article 42 to offer organizations an incentive -- in the form of an EU data protection seal or trust mark -- to adopt such supplemental protections, and propose a change to Article 39 (on certifications) that requires that any mechanisms for seals or trust marks are voluntary, affordable, technology neutral and capable of global recognition. This will ensure that certifications are open to the widest possible participation by all controllers and processors.

**The European Data Protection Board**

The Draft Regulation envisages a new and enhanced Data Protection Board. BSA supports this proposal provided the Board is directed to adopt a transparent decision-making process that reflects the views of a broad range of stakeholders. Given the extensive influence the new Board would have on future legislation in this area we urge the following to be considered:

**BSA Recommendations**

- The Data Protection Board should respect and follow the principles laid down in the European Commission’s Better Regulation initiative. Decisions should be based on extensive input from the public and experts to ensure the Commission and the
bodies that assist it, in this case the European Data Protection Board, have access to the broad range of information needed to formulate policy that strikes an appropriate balance among all affected entities.

- The Data Protection board should include a Permanent Stakeholders Group (“PSG”), which could be modeled on the highly successful Permanent Stakeholders Group for ENISA. The PSG would be composed of representatives of a broad cross-section of stakeholders (consumers, academia, industry, etc.) selected by the European Commission and would assist the Data Protection Board in preparing an annual work plan and in ensuring communication with stakeholders on policy matters.

For further information, please contact:
Thomas Boué, Director, Government Relations EMEA,

at thomasb@bsa.org

or Tel: +32 2 274 13 10