Privacy is a fundamental right for European citizens, and a necessity in the digital environment. A balanced and workable privacy framework will ensure the protection of European citizens online and preserve the ability of companies to innovate and create new products and solutions that meet user demands.

To achieve that balance, BSA | The Software Alliance believes Europe’s data protection framework must recognize the importance of three key principles:

» User trust
» Shared responsibility
» Breathing room for innovation

BSA represents some of the world’s most innovative companies. They provide the essential backbone for the digital economy by constantly pioneering new ways to communicate and exchange data, enhance efficiency, increase security, and enrich user enjoyment. BSA’s member companies are fully committed to protecting user privacy, and welcome efforts to modernize the data protection framework in the European Union.
IN PRACTICE: USER TRUST

In the digital environment, the customer relationship is largely built on user trust. Users must have confidence that companies value and respect their privacy, and that their data is held and managed responsibly, securely, and transparently. Indeed, in this environment, user trust must be earned—not assumed. BSA member companies invest significant resources in earning, and keeping, the trust of their customers by meeting expectations regarding the use and processing of user data. Through innovative data management practices, technologies and security measures, software companies ensure that customer data of all types is treated with the respect and earnestness that it deserves. Good data management is not simply a matter of compliance, it is a market differentiator.

IN PRACTICE: SHARED RESPONSIBILITY

Privacy protections can only be met if all stakeholders are accountable. The online environment provides a variety of platforms, applications, and communication tools with which users can interact and share information. At the same time, users must use these services in a responsible way. While industry can deliver tools that enable users to make smart choices about how they share their information, no amount of technological protection can compensate for careless or reckless online behavior. Users must be educated about their online activities, the data they expose, and to whom.

IN PRACTICE: BREATHING ROOM FOR INNOVATION

Technology is a demand-driven business. Users know what they want and use their choices to drive information service providers and software developers to adapt. In this regard, data protection and innovation go hand in hand. New solutions are required to address the complex and ever-changing privacy challenges presented by the fast-paced digital environment. Likewise, data protection rules must be forward-thinking to accommodate for valuable emerging technologies such as cloud computing. A focus on substantive outcomes will promote respect for the basic rights of individuals and enterprises while leaving “breathing room” for technological progress so that products, services, and privacy protections can evolve. Rules that are too prescriptive will merely act as an administrative compliance exercise, and retard technological progress by preventing new products and technologies that lie outside the specific parameters of the regulation coming to market.

The end goal of Europe’s data privacy review should be a framework that allows for achievable results, and that works in practice to deliver high standards for user privacy while encouraging innovation and advancing Europe’s digital economy.
In order to deliver on these key principles, BSA believes the European data protection framework must accomplish the following:

**CREATE LEGAL CERTAINTY FOR DATA MANAGEMENT**

Businesses are subject to different, at times diverging, data protection regimes within and beyond the single market. In addition, they face moving targets regarding their obligations and ability to process data in new and innovative ways. The result is uneven protection for users, higher compliance costs, and market access barriers.

The complexity of this fragmentation is magnified as the digital economy expands on a cross-border and global scale. As interaction occurs in an increasingly virtualized world, the geographic location of users and services should become less consequential. The privacy framework should allow for a free flow of data while preserving necessary levels of protection.

**Solution:**

» Harmonize clear rules across the European single market and work towards global interoperability of data protection laws and privacy standards.

» Establish clear procedures for the assignment of a single lead data protection authority to act as a “one-stop-shop” for companies operating across multiple EU markets.

» Safeguard technology neutrality and avoid prescriptive mandates regarding technologies or privacy procedures.

» Clearly define practical and workable responsibilities for data controllers and data processors and avoid overlap in their obligations.

**RECOGNIZE A DIFFERENTIATED APPROACH TO DATA PROCESSING**

Data is not a one-size-fits-all concept. In today’s complex digital environment, a flexible and context-based approach is required to determine when robust protections for data should apply. Some data is clearly personal and sensitive: medical and financial records, for example. Other forms of data, such as IP addresses, might be considered personal in one context, but in another cannot be used to identify an individual. Processing data should trigger appropriate obligations and protections that reflect the context and sensitivity of the data. How data is gathered, how it is used, and by whom, matters a great deal.

**Solution:**

» Recognize differentiation in the definition of “personal data” to take into account its nature, context, and proximity to the controller, as well as risk factors to the data subject.

» Limit explicit consent to sensitive data only. A standard form of consent for all types of data will not encourage users to differentiate between risky processing, which warrants greater user attention, and processing of pseudonymous data, which has lesser privacy implications.

» Instill safeguards against data processing that adversely affects a data subject, without obstructing legitimate data processing activities and helpful “profiling” procedures, such as those used for anti-fraud mechanisms, customized services, and optimizing user experience.

» Reserve punitive sanctions for truly bad actors and cases which pose risk of significant harm to individuals. Give data protection authorities discretion as to whether sanctions are warranted.
PRESERVE COMPANIES’ ABILITY TO DELIVER EFFECTIVE SECURITY MEASURES

Privacy in the digital age can only be achieved if the Internet environment is secure. As information becomes more valuable, systems are faced with increasingly sophisticated and complicated attacks. Companies must take steps to ensure that the user data entrusted to them is properly protected against cyber threats. They must also be able to process certain types of data in order to guarantee the security and integrity of their networks and systems. Security systems and technologies deployed by a wide range of entities, including critical infrastructure providers such as banks, hospitals, and governments, all process certain types of data in order to prevent malicious attacks and information security breaches.

Europe’s data protection rules should support and promote the development of effective security technologies, and ensure that security technologies can continue to be deployed to address new threats.

**Solution:**

- Recognize processing of data for security purposes as a lawful basis for data processing.
- Define a breach notification obligation that is harm- and risk-based, on a timeline aligned with existing breach notifications rules in Europe.

ABOUT BSA

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.