POSITION PAPER

BUSINESSEUROPE

12 December 2011

REVIEW OF THE EU DATA PROTECTION FRAMEWORK

KEY MESSAGES

1 The 1995 EU data protection directive and its basic principles have established an adequate technology-neutral and flexible legal framework that has stood the test of time. They should therefore not be fundamentally changed. A revised legal framework should be principles-based and flexible in order to guarantee technological neutrality.

2 Any future review should address the need for a more consistent implementation of the directive across the EU, as substantive divergences in its implementation by Member States run counter to its objective to ensure free flow of personal data within the single market.

3 Limiting administrative burden for companies, supporting industry self-regulation and using checks and balances instead of prescriptive rules should be key objectives of a future review.

WHAT DOES BUSINESSEUROPE AIM FOR?

- The legislative framework governing general data processing in companies does not warrant any radical or significant changes insofar as strengthening individuals' rights. It should stay flexible, applicable to different situations, refraining from any undue restrictions on the free flow of data across borders and avoiding administrative burden, complex and contradictory legal provisions in Member States. The current framework captures for e.g. the so-called "right to be forgotten" sufficiently and there is no need to "re-invent" existing safeguards.

- BUSINESSEUROPE is reluctant to support the introduction of new obligations regarding a general personal data breach notification.

- BUSINESSEUROPE calls for a promotion of a harmonised but flexible set of measures that can be chosen by the data controllers to comply with the data protection framework. Companies should have discretion on how to organise compliance.

- A flexible concept for consent should be maintained in order to enable innovation, development of new services and consumer choice.

- BUSINESSEUROPE believes that the revision of the directive is an opportunity to come up with more appropriate and flexible ways to address international transfers, without diminishing the possibilities for innovation, employment and growth in the digital market.

- The review should also aim at achieving a truly level playing field for all data controllers in an on-line environment. Irrespective of the geographical location of the service provider, EU citizens' personal data should be granted the same level of protection.

BUSINESSEUROPE

POSITION PAPER

12 December 2011

REVIEW OF THE EU DATA PROTECTION FRAMEWORK

I. INTRODUCTION

Europe's knowledge-based economy is increasingly based and dependent on creating, collecting, distributing and utilising information. Processing of data is an everyday reality in the context of a global trading environment. Society is becoming increasingly connected and the virtual world more prevalent in the lives of European citizens. European businesses are developing leading-edge products and services addressed to consumers, supporting jobs, growth and innovation. The ability to process customer data in a way that ensures consumers' confidence that their data are processed safely is key in order for Europe to remain a leading digital economy, as outlined in the Growth 2020 Strategy.

This is why BUSINESSEUROPE has been following with interest the Commission's plans to review the EU data protection directive 95/46/EC and would like to provide its views on the future of the data protection framework in the EU.

In BUSINESSEUROPE's view, the 1995 data protection directive and its basic principles have established an adequate technology-neutral and flexible legal framework that has stood the test of time. They should therefore not be fundamentally changed. A revised legal framework should be principles-based and flexible in order to guarantee technological neutrality.

Furthermore, existing definitions of personal data and sensitive personal data are satisfactory. It is clearly the context of processing which determines whether data are to be considered personal, i.e. related to an 'identified or identifiable person, either directly or indirectly', or not. Flexibility, therefore, as well as technology neutrality are important virtues recognised in directive 95/46/EC, as they enable data controllers to provide protection to data subjects' data in a manner proportionate to the risks they actually face in a given context of processing. We therefore suggest considering a "use and obligations" model that places greater emphasis on the uses to which data are put – rather than the circumstances under which the data are collected – to determine obligations in relation to processing the data.

However, a crucial aspect that needs to be addressed in any future review is the need for a more consistent implementation of the directive across the EU as substantive divergences in its implementation by Member States run counter to its objective of ensuring a free flow of personal data within the single market and need to be addressed in any future review. In addition, clarification of the definitions and principles of the directive will be more beneficial than introducing new measures and requirements.

In particular, the following key objectives should be taken into account:

BUSINESSEUROPE a.i.s.b.l
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL MAIN@BUSINESSEUROPE.EU
WWW.BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

- foster trust on data being processed securely and boost confidence in the use of new products and services
- ensure companies' ability to innovate and provide existing and new services, thereby promoting Europe's competitiveness
- limit the administrative burden for companies
- maintain a technology-neutral legal framework
- create a level playing field by applying European data protection rules to all operators offering their services to EU citizens.
- ensure coherent implementation of the directive across European countries.

In addition, any future review should: focus on outcomes rather than processes, support industry self-regulation and use checks and balances rather than prescriptive rules to achieve business compliance.

In this context, BUSINESSEUROPE would like to address a number of specific issues raised in the context of the review of the data protection framework.

II. SPECIFIC COMMENTS

1. INDIVIDUALS' RIGHTS

Every day personal data of virtually every EU-citizen are processed in some way. It is done in order to manage society's complicated networks and individuals' rights and duties in the society – from taxation to healthcare and from education to customer services and employment issues, among others. When properly planned and executed, the everyday collection and processing of personal data is in the individual's interest – not in contradiction to it.

Individuals' rights are a fundamental pillar of the data protection legal framework. Generally, when protecting individuals' data it is important not only to focus on simply seeking compliance with legislation, but also on providing security to individuals. It should be ensured that data are not accessed by unauthorised persons or used without the individual's knowledge or directly against individual interests. Risk minimisation from the perspective of the individual is the foundation for privacy and for creating trust between individuals on the one side and business and public administration on the other side.

At the same time, a balance is needed vis-à-vis the capacity of companies to provide innovative services and products that consumers want and respect legal requirements. We believe that the legislative framework governing general data processing in companies does not warrant any radical or significant changes insofar as strengthening individuals' rights. It should stay flexible, applicable to different situations, refraining from any undue restrictions on the free flow of data across borders and avoiding administrative burden, complex and contradictory legal provisions in Member States.

Moreover, professionals have to collect certain data information in order to carry out their activities. This is particularly true in financial services, for the purposes of consumer protection or the fight against money laundering, where the law imposes on the financial producers to verify a series of personal data to respect its legal obligations.

- **"RIGHT TO BE FORGOTTEN"**

The right to be forgotten is not a new concept. It is inherent in some basic principles that can be found in the current data protection directive. The basic principles of data quality (Article 6), right of access and right of rectification (Article. 12) as well as consent (Article. 7) reflect what is now named as the new "right to be forgotten". We consider that the current framework captures this right sufficiently and that there is no need to "re-invent" the existing safeguards.

Instead, it would be more efficient to focus on a more consistent implementation at national level of the rights of access, correction, cancellation and opposition by all online service providers processing personal data than introducing "new rights". Technical means and infrastructures to exercise those rights should be developed.

Similarly, the principle of data minimisation is sufficiently reflected in Article 12 of the directive which clarifies that data collection should be limited to a minimum: the data controller is allowed to collect only the data needed.

Therefore, it may not be necessary to strengthen it from a policy perspective but from the point of view of its effective practical enforcement. We also believe that an assessment of what data is needed for a certain service and what not, is part of the concept of "privacy by design".

- **DATA BREACHES NOTIFICATIONS**

The Commission has announced that it will examine whether a general duty to notify personal data breaches could be included in the legislative framework.

BUSINESSEUROPE is reluctant to support the introduction of new obligations, as it is only on those systems that are well protected that a possible breach of data security is discovered. For all the systems where the protection is not sufficient, data breaches will not be discovered. Thus, this notification does not necessarily give the consumer an accurate picture of the risks he faces. Moreover, in cases of minor and non-harmful breaches the administrative burden could be disproportionate when compared with possible benefits.

However, as part of the processing of personal data is often outsourced to data processors, BUSINESSEUROPE believes that an obligation for data processors to notify the data controller(s) of a confirmed security breach would be an effective way to enhance the protection of personal data in outsourcing situations.

A general personal data breach notification without proportional assessment could also raise competitions concerns. Questions could be raised as to how to ensure that the control authority cannot put this information in the public domain and whether it is reasonable to first provide for reporting to the authority and to decide subsequently whether and how the data subject has to be informed.

If a mandatory personal data breach notification is imposed, the harm that a personal data breach poses or could reasonably pose in the future to the data subject should be one of the main criteria that trigger the obligation to notify. If the risk of harm is limited, the benefit that the data subject will gain from the notification will also be restricted and cause unnecessary stress. It might also lead to consumer apathy, which is the case in the USA where so many notifications were received that significant ones were overlooked.

Moreover, it would create undue administrative costs for firms and possible damage to reputation even when there is no consumer detriment.

Finally, BUSINESSEUROPE would like to underline the multiplicity of control authorities and the possible interaction between data protection authorities and other control authorities.

The focus in the directive should be on ensuring that individuals do not have to deal with data breaches at all.

- **AWARENESS-RAISING**

Awareness-raising is essential. Awareness of existing rights should be improved. In addition, it is important to raise individuals' awareness of their own choices related to the use of new ways of communication and new business models on the internet, such as social media.

Modern-day online services are often considered ‘free’ of charge by the user. Such services are typically funded by advertising. BUSINESSEUROPE believes that it is important that consumers are educated about the fact that such services are usually not really ‘free’, and that their use of such services may require that some data related to their use of the service are collected by the service provider. Data protection law should not prohibit the introductions of such business models where consumers freely choose to sign up for such services and willingly participate in the collection of their data.

- **INFORMED AND FREE CONSENT**

The Commission wants to examine ways of clarifying and strengthening the rules on consent.

BUSINESEUROPE recalls that it is of utmost importance to maintain a flexible concept for consent in order to enable innovation, development of new services and consumer choice. The e-Privacy directive, places requirements on internet service providers

(ISPs) and other companies deploying cookies for achieving customer consent, but by allowing consumers to express consent through their browser settings, the directive manages to address privacy concerns effectively while supporting the accountability principle.

2. ENHANCING THE BUSINESS ENVIRONMENT AND COMPLETING THE DIGITAL SINGLE MARKET

One of the key goals of the data protection directive is to facilitate the free flow of personal data within the single market and at the same time protect citizens' privacy. However, fragmented implementation of the current framework across the EU and introduction of new administrative burdens (e.g. for obligatory notification and data protection officers that do not necessarily improve citizens' privacy) are costly for companies.

BUSINESSEUROPE calls for a promotion of a harmonised but flexible set of measures that can be chosen by the data controllers to comply with the data protection framework. The European Commission should define a non-exhaustive list of measures that could be implemented to help comply with the data protection framework. Companies should have discretion on how to organise compliance.

Compliance must be easier and less costly as that will benefit all businesses allowing them to focus on actual data protection measures instead of navigating between different national rules and dealing with administrative procedures that do not contribute much to data protection. Among the set of measures are: appointing data protection officers (DPOs), carrying out privacy impact assessments, make obligatory notification and use technical measures such as privacy by design and privacy enhancing technologies. It is important that these measures are used only where they could actually make a difference for the protection of citizens' privacy. Using them in this way will further contribute towards completion of the digital single market.

- **ENHANCING DATA CONTROLLERS' RESPONSIBILITIES**

The future data protection framework should mainly focus on enhancing the data controller responsibility by a general requirement for data controllers to implement appropriate measures to ensure that the obligations are complied with. How this compliance is achieved, should be left open so that flexibility is assured.

Appointing a DPO should consequently be decided by each company, taking into account their specific circumstances and the risks that may result from the intended data processing.

- **PRIVACY IMPACT ASSESSMENT**

A Privacy Impact Assessment (PIA) can provide a promising tool ensuring a holistic and harmonised approach towards compliance. However, in many situations a PIA could also be unnecessarily burdensome to perform.
The decision on whether to use a PIA or not should be decided by the data controller himself.

- **SIMPLIFYING AND HARMONISING THE CURRENT NOTIFICATION SYSTEM**

Current divergences between the national laws concerning the ex-ante compliance procedures such as registration and notification requirements are unreasonably onerous for businesses with operations in several Member States. BUSINESSEUROPE welcomes the Commission's intention to simplify and harmonise the current notification system.

- **NEW TECHNOLOGIES**

Unnecessary collection and processing of personal data should be avoided. Privacy-enhancing technologies (PET) and privacy by design (PbD) principles are measures that should be promoted to achieve this goal. In general there has been too much focus on creating new legislation instead of focusing on how new technologies could help promote the protection of citizens' privacy.

BUSINESSEUROPE welcomes the European Commission's intention to promote the use of those technologies without being too prescriptive. As already stated, the legal framework should remain technology neutral. Also, these new technologies are no silver-bullet to solve all privacy challenges. They could be taken into consideration by data protection officers and as such they should be promoted.

3. INTERNATIONAL DATA TRANSFERS

Many companies' activities regularly cross borders within the EU and around the world, involving large transfers of data within the EU and globally. The current rules are ill-suited to respond to this reality, especially in the era of cloud computing.

BUSINESSEUROPE believes that the revision of the directive is an opportunity to come up with more appropriate and flexible ways to address international transfers, without diminishing the possibilities for innovation, employment and growth in the digital market. As a result, BUSINESSEUROPE welcomes the Commission's intention to work on core elements of personal data protection in agreements between the Union and third countries for law enforcement purposes and the improvement and streamlining of current procedures for international data transfer including binding corporate rules.

Binding corporate rules (BCRs) should facilitate faster and more efficient transfers. However, they should be made fit-for-purpose and reflect modern business practices.

Member States who have yet to give legislative recognition to BCRs should also be encouraged to do so without delay.

BCRs are an accepted and appreciated measure to ensure an adequate level of data protection within a corporate group. They ease trans-border data flow and also maintain the appropriate level of data protection. They have proven to be a driver for privacy awareness and enhanced compliance in organisations which have adopted them. However, the current BCR approval process is burdensome and complex. The current approval process is still driven by distrust rather than trust, which does not reflect the value of BCRs for personal data protection. The approval process is lengthy and expensive, which discourages companies from adopting BCRs.

Therefore, BUSINESSEUROPE calls for simplified procedures, which encourage companies to adopt BCRs. Examples of such simplified procedures can be found in the Swiss Data Protection Act and in the proposals of former Information Commissioner Richard Thomas on the concept of 'Binding Global Codes'. Furthermore, in order to reach the full potential of BCRs, it is essential that the recognition of BCRs is fully integrated in the Directive by eliminating other obstacles totheir adoption, such as the rules for notification.

To further support and simplify international data transfers the directive should support the development of a framework for BCRs for data processors (or 'Safe Processor Rules') in order to close an important gap in the protection of personal data and to eliminate some of the burdens created by the new model contract for transfers to data processors (2010/87). We believe that two frameworks for BCRs, one for data controllers and one for data processors, is an efficient way to seamlessly protect personal data regardless of their location (e.g., cloud computing).

The current set of available solutions for international data transfer does not allow for a reasonable handling of data within a corporate group which leads to numerous problems. To monitor data flow within corporate groups various framework-agreements and contracts regarding commissioned data processing are necessary. These contracts need to be administered and controlled and tie up -an enormous amount of resources. Data transfer within a corporate group has to be possible without the construct of commissioned data processing and in a way that key-functions like customer service and human resources can be transferred to a company of the group that in turn can have access to the respective data and is able to control it independently. Where companies fall under consistent corporate governance a comprehensive data processing must be feasible according to the group's organisation. Units like customer service, legal or audit are often centralised in the group's headquarters.

The legal situation has to be adjusted to this reality allowing centrally organised units to have access to data of customers and employees.

Currently companies handling personal data in several Member States are subject to different rules in different Member States. In this respect, the review should also aim at achieving a truly level playing field for all data controllers in an on-line environment. Irrespective of the geographical location of the service provider, EU citizens' personal data should be granted the same level of protection. Otherwise, inconsistent

application of the EU rules has a clear negative impact on the competitiveness of EU companies and on individuals' trust and confidence.

4. GOVERNANCE

- **ENHANCING JUDICIAL REMEDIES AND SANCTIONS**

The Commission announces that it will consider the possibility of extending the power to bring an action before the national courts to data protection authorities (DPAs) and to civil society associations.

We do not believe such initiative is needed. Decisions on issues like power to bring an action before the national courts need to be left with the Member States to decide as they are essentially linked to Member States' legal systems and procedural law.

- **STRONGER INSTITUTIONAL ARRANGEMENTS FOR BETTER ENFORCEMENT OF DATA PROTECTION RULES**

The Commission announces that it will examine how the position of DPAs could be strengthened and how co-operation between DPAs could be facilitated.

BUSINESSEUROPE welcomes closer cooperation among all authorities and stakeholders involved in data protection. We support the idea of enhancing cooperation between DPAs. As regards the role of the DPAs, focus should be in particular on enforcing the directive coherently across European countries.

The Article 29 Working Party should be more transparent and required to consult all stakeholders before issuing opinions and guidance.

***