BUSINESSEUROPE

25 September 2014

PERSONAL DATA ARE THE BACKBONE OF THE DIGITAL ECONOMY

- Data have a huge potential. The use of data will be beneficial for society at large, improving healthcare through better diagnosis and treatments, facilitating democratic participation and making the public sector more efficient and close to citizens. The smart use of ICT by public bodies can reduce cost of public administrations by 15-20%.

- Personal data are an extremely valuable asset, both in economic and non-economic terms. The estimated value of EU citizens' data was €315 billion in 2011 and has the potential to grow to nearly €1 trillion annually by 2020. The market for the analysis of large sets of data is growing by 40% per year worldwide.

- Europe will be able to take advantage of this huge potential only if the regulatory framework for data protection is appropriate to take up this challenge. Europe is facing a crucial opportunity and must make the right choice.

- BUSINESSEUROPE calls on the EU Institutions to truly deliver on a set of rules that will strike the right balance between protecting personal data and enabling their collection, analysis and transfer in the single market and beyond.

KEY PRIORITIES FOR AN EU DATA PROTECTION FRAMEWORK

1 ***Enable lawful data processing:*** Companies need to be able to collect and process data to perform data-based innovation, which can leverage €330 billion a year in the EU by 2020.

2 ***Establish an effective one-stop shop:*** This will make the application of data protection rules more consistent throughout the single market. It will also create a level playing field for companies, increase legal certainty and reduce red tape.

3 ***Define simple, future-proof and harmonised rules:*** The legal framework must be simple, easy to understand, technologically neutral and flexible to apply in different branches and different data processing operations. It is necessary to guarantee uniform interpretation and application of data protection rules to ensure a level playing field between companies. The rules should define the principles and objectives, not the means to reach those objectives.

4 ***Allow cross-border data flows:*** Data flowing across borders, according to data protection rules, is a necessary condition for international trade and for the internal functioning of European companies of all sizes.

5 ***Implement a risk-based approach:*** The requirements must be defined taking into account context and purpose of the data processing, as well as the level or risk for the citizens involved in the data processing. They should incentivise businesses to protect privacy and avoid creating unnecessary burdens for companies.

BUSINESSEUROPE

RECOMMENDATIONS

1. **Recognise the role of data in the economy.** Data protection regulation must respond to the need to protect citizens' rights, but also to create the appropriate conditions for companies to unlock the economic value of data. The two objectives should be pursued at the same time.

2. **Allow lawful data processing, also in the employment context.** Lawful data processing is essential for companies' internal functioning and for their activities. Too restrictive criteria to enable data processing must be avoided, not to undermine the functioning of organisations and their potential for innovation in the data economy. Adequate legal basis for data processing in the employment context must also be ensured. In some Member States, collective agreements are a generally accepted basis for legal data processing as much as national legal provisions. This must be recognised in the regulation at EU level. Additionally, employees' consent must be recognised as a valid basis for data processing.

3. **Avoid disproportionate burdens.** Requiring detailed documentation for every processing operation, even the ordinary ones which do not present specific risks, is not proportionate. The proposed provisions on privacy impact assessments and prior consultations should not result in disproportionate burdens for companies. Also, the obligation to appoint a data protection officer, without allowing a degree of flexibility to each organisation, is excessively prescriptive.

4. **Avoid negative perception of profiling.** Profiling enables companies to provide customers with tailored services on the basis of customers' interests, hopes and needs, enhancing the quality and attractiveness of such services. It is the harmful use of profiling, not profiling in itself, that should be adressed in the regulation.

5. **Put in place an effective and workable *one-stop shop* system.** The functioning of this system must be clear for companies in ensuring a single authority is responsible for deciding cross-border cases. It is fundamental to define clear and harmonised competences, duties and powers of data protection authorities in all Member States.

6. **Avoid making international data transfers excessively burdensome.** The digital economy is global by nature. Its business models increasingly rely on international transfers of data. Increased and disproportionate requirements for international data transfers will disrupt emerging European digital business with a negative impact on EU innovation and growth.

7. **Ensure a balanced approach to sanctions.** As currently discussed, potential sanctions may vary from 1 million to 100 million euro, or 2 to 5% of a company's worldwide turnover. Such fines are based on a competition law model and are not appropriate for data protection, where the type of conduct and the impact of violations on the market are not comparable to anticompetitive behaviours. Sanctions should also be proportionate to damage incurred.

8. **Right to be forgotten must be workable.** The right to obtain from the controller rectification or deletion of personal data which are inaccurate or collected not in compliance with the legislation, as required by the current data protection directive, is welcome. It will increase citizens' trust in the digital world. However, it must address the issue of the balance of rights so as not to result in excessive burdens imposed on controllers who lawfully process personal data. Furthermore, it should not jeopardise the balance with other fundamental rights such as the freedom of expression.

9. **Ensure clarity of the provisions**. Provisions, roles and responsibilities must be clear. For instance, a clear distinction should be made between the liabilities of the controller and those of the processor.

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