

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:55
To: Verweij, Ellen
Subject: FW: BUSINESSEUROPE letter on data protection in view of the Justice Council on 4 December 2014
Attachments: 2014-12-02 Council Justice and Home Affairs Council 4 Decembre 2014.pdf
Follow Up Flag: Follow up
Flag Status: Completed

From: [redacted] [mailto:[redacted]]
Sent: dinsdag 2 december 2014 16:08
To: Kaai, Geran
Subject: BUSINESSEUROPE letter on data protection in view of the Justice Council on 4 December 2014

Dear Kaai,

As promised, please find enclosed our letter on the one-stop shop in view of your discussions at the Justice Council. I hope this is going to be helpful.

Do not hesitate to get back to me if needed.

Best regards,

[redacted]
ADVISER
INTERNAL MARKET DEPARTMENT
DIRECTORATE GENERAL

BUSINESSEUROPE

[redacted]
168 AVENUE DE CORTENBERGH
1000 BRUSSELS - BELGIUM

Tel : [redacted]

Fax : [redacted]

Mobile: [redacted]

[redacted]
www.businessseurope.eu
EU Transparency register 3978240953-79

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Mr. Andrea Orlando
Minister for Justice
Ministero della Giustizia
Via Arenula 70
00186 Roma
Italy

1 December 2014

Dear Minister,

Dear Mr. Orlando,

BUSINESSEUROPE message on the General Data Protection Regulation in view of the discussions at the Justice and Home Affairs Council on 4 December 2014

The upcoming discussions on the General Data Protection Regulation at your meeting on 4 December will be decisive for the future of EU competitiveness and growth. Big data technology and services will grow worldwide to more than €13 billion in 2015 at a compound annual growth rate of 40% – about seven times the growth rate of the information and communications technology market overall. Europe is lagging behind in seizing the huge opportunities offered by big data. Only 45% of EU companies have implemented big data, versus 68% in the US. Global big data technology and services will create hundreds of thousands of new jobs in the EU in the coming years – but only if the EU regulatory framework will enable this opportunity.

In this context, BUSINESSEUROPE believes that the reform of data protection rules could achieve greater harmonisation in the digital single market and help Europe to grasp the opportunities of the digital economy, ensuring balanced rules on data protection. We welcome the efforts of the Italian Presidency in this direction. However, it is fundamental that the rules agreed truly fulfill this objective.

BUSINESSEUROPE calls for a meaningful one-stop shop

The discussions you will have on the one-stop shop mechanism will be important in this perspective. The creation of the one-stop shop is a major improvement to the current EU rules on data protection, as it will make their application more consistent throughout the single market, thereby ensuring a level playing field for companies, increasing legal certainty and reducing administrative burdens for controllers and processors in the EU.

It is therefore essential that the regulation provides a **meaningful, clear and workable legal framework for the one-stop shop**, with simple and easy procedures. We urge you to consider the following elements:

- **An effective one-stop shop means one decision, one outcome.** A meaningful one-stop shop is one of the key improvements that the proposed Regulation was intended to offer all stakeholders by providing legal certainty.

and greater efficiency for industry, citizens, and data protection authorities alike. The current Council texts propose to involve several data protection authorities in issuing decisions and enforcing data protection rules. This would lead to lengthy procedures and lack of legal certainty for controllers, processors and even data subject seeking redress. Moreover, allowing for local judicial review might result in simultaneous procedures and divergent rulings issued by national courts in appeal from the same decision. This option would be detrimental for both companies and citizens.

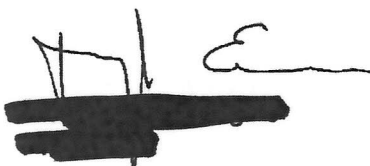

- **Clarity on role and responsibilities of the competent data protection authorities.** Businesses operating in several Member States require legal certainty as to one "lead authority" being their single point of contact and the one they may be addressed by, in particular in the preliminary authorisation and notification processes, which directly affect the lawfulness of the activities of the data controller. The Council must refrain from creating a system which can lead to confusion as to competency questions and to conflicting approaches by different authorities. It is fundamental that the identification of the competent lead authority can take into account different organisational structures of the businesses concerned by the Regulation. Where interaction between data protection authorities becomes necessary, the procedures that govern those interactions must be effective and swift.

It is essential that the current Regulation preserves the one-stop shop in its original structure, because this is one of the elements that could truly help businesses in taking advantage of the potential of data-driven innovation. BUSINESSEUROPE underlines that data processing will be key not only for businesses, but also for the whole society, delivering improvements in healthcare through more accurate diagnosis and systems and more efficient public services through e-government.

Data protection legislation is complex and impacts all segments of the economy. It will have major consequences on the development of the digital single market and on European competitiveness. We urge the Council to take the necessary time to adopt a balanced compromise which will not undermine the EU economy and citizens in the years to come.

A more exhaustive list of BUSINESSEUROPE priorities and recommendations for the data protection Regulation is enclosed.

Yours sincerely,




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.

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 addressed 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.
