14/EN
WP 227

JOINT STATEMENT OF THE EUROPEAN DATA PROTECTION AUTHORITIES ASSEMBLED IN THE ARTICLE 29 WORKING PARTY

Adopted on 26 November 2014

Introduction

Our daily life is increasingly digital. In less than a decade, professional, economic and private activities have gradually shifted towards a digital environment. This evolution has opened a world of new opportunities and has enabled the development of extraordinarily innovative goods and services, which meet individual and collective demands. Personal data is the basic building block of this digital world.

The functioning of the digital environment largely relies on complex information infrastructures built by private entities for their own purposes. These entities gather huge amounts of personal data which some of them may store, further process and share often without an appropriate level of user control and outside any form of effective supervision. Moreover, as the Snowden revelations recently unveiled, public authorities and intelligence services have requested massive access to this data infrastructure for other purposes, namely national security.

The routine and massive nature of such access has shocked the public around the globe. The question is now raised of how to address both the lack of confidence in (foreign or national) governments, intelligence and surveillance services, as well as the underlying problem of how to control access to massive amounts of personal data. How can a framework be built that enables private companies and other relevant bodies to innovate and offer goods and services that meet consumer demand or public needs, whilst allowing national intelligence services to perform their missions within the applicable law but avoiding a surveillance society?

Because of its common history and culture, Europe must make its voice heard in terms of ensuring that fundamental rights, including the rights to privacy and data protection, are respected without obstructing innovation or the need to ensure security in our society. In this context, the independent Data Protection Authorities assembled in the EU Article 29 Working Party (WP29) want to deliver several key messages on how to address this global challenge.

Therefore, the Article 29 Working Party, on its plenary meeting of 25 November 2014, has adopted the following declaration:

European values

1. **The protection of personal data is a fundamental right**. Personal data (which includes metadata) may not be treated solely as an object of trade, an economic asset or a common good.

2. **Data protection rights must be balanced with other fundamental rights**, including non-discrimination and freedom of expression, which are of equal value in a democratic society. They must also be balanced with the need for security.

3. **Technology is a medium that must remain at the service of man.** The fact that something is technically feasible, and that data processing may sometimes yield useful intelligence or enable the development of new services, does not necessarily mean that it is also socially acceptable, ethical, reasonable or lawful.

4. **Public trust in the products and services of the digital economy** depends largely on the technology industries' compliance with data protection rules. Such compliance is a key competitive factor for the digital economy; it will also ensure its sustainable development, to the benefit of consumers and industry alike.

5. **Public awareness and individual empowerment** must be strengthened to help individuals limit their exposure to excessive surveillance by public or private actors. In that respect, key measures are improving digital literacy, including privacy education, and opening collective judicial actions to individuals to facilitate reporting of widespread data protection violations.

Surveillance for security purposes

6. **Secret, massive and indiscriminate surveillance** of individuals in Europe, whether by public or private players acting in an EU Member State or from elsewhere, is neither lawful with regard to the EU Treaties and legislations nor ethically acceptable.

7. **Unrestricted bulk retention of personal data for security purposes is not acceptable in a democratic society**. Retention, access and use of data by national competent authorities should be limited to what is strictly necessary and proportionate in a democratic society, and be subject to effective substantive and procedural safeguards.

8. **Processing of personal data in the context of surveillance activities** may take place only under adequate safeguards defined by law, in accordance with Article 8 of the European Charter of Fundamental Rights. Such safeguards include **independent and effective supervision**, in which DPAs should be genuinely involved, within the limits of their competences.

9. As a rule, a public authority in a non-EU country should not have unrestricted **direct access to the data of individuals processed under EU jurisdiction**, whatever the conditions of this access and the location of the data. Conflicts of jurisdiction shall be resolved only under certain conditions – e.g. through prior authorisation by a public authority in the EU or through a mutual legal assistance treaty, respectively covering access by foreign law enforcement authorities to data transferred from the EU or to data stored in the EU. Foreign requests must not be served directly to companies under EU jurisdiction.

10. None of the provisions of the **European instruments designed to frame international data transfers** between private parties provide a legal basis for the transfer of data to a third country authority for the purpose of massive and indiscriminate surveillance (whether Safe Harbor, binding corporate rules or standard contractual clauses).

11. When public or private parties collect massive amounts of data which provide very precise information on the private lives of the individuals whose data are retained, they should organize the storage of this data in such a way that an independent authority can effectively control their compliance with the data protection requirements. The **storage of the relevant data on EU territory** is an effective way to facilitate the exercise of such control**.**

European influence

12. **The EU draft data protection package should be adopted in 2015**. Whilst contributing to the unification of the European digital market, it must ensure a high level of data protection to individuals, in accordance with European values and fundamental rights.

13. The European level of protection of personal data should not be eroded, wholly or in part, by bilateral or **international agreements, including agreements on trade** in goods or services with third countries.

14. EU data protection rules are necessary to safeguard the political, social and economic situation of the EU and those subject to EU legislation. Their principles must be considered to be of an **internationally mandatory nature under public and private international law**. Foreign laws or international agreements cannot override them nor can organizations derogate from them by contract.

15. Striking the right balance between data protection, innovation, and surveillance entails **neither rebuilding internal EU borders nor closing the gates of Europe** to foreign partnerships. It requires respect for the high level of protection derived from the European data protection heritage, including Convention 108 of the Council of Europe and EU data protection rules.

Next steps

16. The Working Party welcomes **comments** on this Statement by all interested stakeholders, whether public or private. Such comments may be addressed through the dedicated website available at www.europeandatagovernance-forum.com. The Working Party will take these comments into account in its activities over the year 2015.