Statement of the Working Party on current discussions regarding the data protection reform package.

Since the adoption of the data protection reform package on 25 January 2012, the Working Party has issued two opinions providing input into the legislative process (WP191 and WP199). Having regard to the current discussions and the stage of the legislative procedures both in the European Parliament and in the Council, the Working Party would like to again express its views on 6 identified areas of concern that are in need further attention, these are flexibility public sector, personal data and pseudonymisation, consent, governance, international transfers and risk-based approach.

In addition to these areas of concerns, the issues of lead DPA and competence and of the exemption for household and personal activities have been more thoroughly discussed, the outcomes of which are attached to this statement.

Flexibility public sector

The Working Party is aware that there is an ongoing discussion on providing more flexibility for the public sector in the proposed Regulation on the protection of personal data. The Working Party understands that processing activities by the public sector for public interest purposes will have to remain possible also under the proposed Regulation, there are however no compelling reasons to create even more flexibility than already provided. The Working Party would like to stress that data protection is a fundamental right, guaranteed both by the Treaty of Lisbon and the Charter on Fundamental Rights. As a fundamental right, the right to data protection is not dependent on whether the data controller is from the private or the public sector. Moreover, given the powerful position of governments in relation to individuals, effective protection is all the more needed. A distinction between the public and private sectors would only lead to legal uncertainty and would also be unworkable in practice, since there are large differences between the Member States regarding what functions are done by public bodies and what by private bodies.

Personal data and pseudonymisation

Since 2007 the Working Party has held that a natural person can be considered identifiable when, within a group of persons, (s)he can be distinguished from others and consequently be treated differently. This means that the notion of identifiability includes singling out.[1] Where identification of the data subject is not one of the purposes of the processing, technical measures to prevent identification can play an important role. Using pseudonymising techniques, to disguise identities to enable collecting data relating to the same individual without having to know his/her identity, can help mitigate the risks to individuals. Encryption is a measure to technically protect personal data, it however does not change the nature of the data, which remains personal. Pseudonymising data is disguising identities in a retraceable way. When identities are disguised in a way that no re-identification is possible this is anonymisation. Therefore using a pseudonym or encryption, means that where it is possible to backtrack an individual or (indirectly) identify an individual by other means, data protection rules continue to apply.

[1] Identification numbers, location data, IP-addresses, online identifiers or other specific factors relating to an individual should be considered personal data.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Consent

Consent of the data subject is one of the legal grounds for processing. The Working Party insists that it is absolutely necessary to ensure consent cannot be misused. Therefore, where consent is used as the legal ground, it must be sufficiently clear. Consent can be expressed in many different ways, for instance through a statement or an affirmative action, but it should be an essential requirement that it is *explicit*. To truly enable data subjects to exercise their rights, especially on the internet where there is now too much improper use of consent, requiring it to be *explicit* is an important clarification of the notion and should therefore not be deleted from the text. Furthermore placing the burden of proof on the controller and introducing safeguards in the context of a written declaration, greatly strengthen the rights of individuals. In addition, the Working Party would like to stress that consent cannot be a valid legal basis if there is a significant imbalance between the position of the parties concerned.

Governance

The Working Party has played an important role until now in terms of policy making and the provided interpretative guidance has proven its added value. The Working Party's successor, the European Data Protection Board (EDPB), will possibly play an even more important role in the future. The enhanced duties for both DPAs and the EDPB will help ensure EU-wide compliance and will greatly enhance the protection of personal data. These extended duties however also imply great changes for the DPAs regarding the (re-)allocation of their scarce resources. To ensure all DPAs are sufficiently equipped to perform their tasks, the budget of a DPA should be based on a fixed amount to cover the basic functions that all DPAs have to undertake equally, supplemented by an amount based on a formula related to the population of a Member State and its GDP and the amount of main establishments in that Member State. In addition, the Working Party feels DPAs should be enabled to be selective in order to be effective. They should be able to define their own priorities and to start actions, such as investigations, on their own initiative, notwithstanding the obligations regarding cooperation, mutual assistance and consistency according to Chapter VII. Therefore, to ensure DPAs and the EDPB can effectively carry out their duties it is necessary to provide clear rules on issues such as budget, equality of powers, the margin of discretion for DPAs and how the mutual assistance and the consistency mechanism are to be put to practice.

International transfers

Considering the interconnected world and the trend of globalization, the Working Party recognizes the need for data to cross borders. It is however important that individuals receive the same protection of their personal data when it is transferred to 3rd countries as within the European Union. Considering the discussions that currently take place on the Regulation on data protection to also enable data transfers by using non binding instruments, the Working Party would once more like to stress that bindingness is one of the most important requirements for tools enabling international transfers for ensuring appropriate safeguards for data subjects. Furthermore, self-assessment for transfers to third countries should remain a derogation to adequate safeguards with a very limited scope. As already stated in Opinion 1/2012, such a derogation must be based on an exceptional basis, only for non-massive and non-repetitive transfers. The Working Party furthermore stresses the need to include in the Regulation the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law. Without a provision on the obligatory use of MLATs when they are in place will, amongst others, allow for wide transfers of personal data for a large and unlimited category of "*important grounds of public interests*". When a judgement of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to transfer data from the EU to that third country and there is no MLAT or another international agreement in force between the requesting third country and the Union or Member State(s), the transfer of such data should be prohibited.

Risk-based approach

The Working Party recognizes that some of the provisions in the proposed Regulation may pose a burden on some controllers which may be perceived as unbalanced and has therefore in earlier opinions already expressed the view that all obligations must be scalable to the controller and the processing operations concerned. Compliance should never be a box-ticking exercise, but should

really be about ensuring that personal data is sufficiently protected. How this is done, may differ per controller. This difference however, is not only dependent on the size of the controller, or on the amount of processing operations it carries out, but is also dependent for example on the nature of the processing and the categories of the data it processes. Basing exceptions on quantitative qualifiers risks excluding companies from certain obligations that are actually of vital importance. Data subjects should have the same level of protection, regardless of the size of the organisation or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner.

Done at Brussels, on 27/02/2013

For the Working Party
The Chairman
Jacob KOHNSTAMM