Explanatory Notes

for the Resolution of the 85th Conference of the Data Protection Commissioners of the Federal Government and the *Länder* in Bremerhaven on 13 – 14 March 2013
"Europe must strengthen data protection"

- **All data able to identify specific persons must be protected**

According to Article 8 (1) of the EU Charter of Fundamental Rights, "Everyone has the right to the protection of personal data concerning him or her." European data protection law must therefore equally cover all data that can be traced to a natural person. Personal data should be defined as individual information about personal or property relations of a specific or identifiable person. This also includes pseudonymised data and identifiers such as IP addresses, identification numbers and location data.

- **There should be no gaps in the protection of fundamental rights**

Attempts to exempt entire categories of data, such as employee-related data, and entire occupational groups, such as freelancers, from the scope of fundamental data protection law conflicts with the principle of the universal scope of fundamental rights. Releasing all small and medium-sized enterprises from key data protection obligations fails to recognize that the number of employees is irrelevant for the degree of infringement on fundamental rights.

- **Consent must be explicitly given**

Consent to the processing of personal data can be legally effective only when based on the data subject's clear and explicit statement of intent, given with knowledge of the situation. We cannot make any concessions concerning the demand that effective consent must be based on a truly voluntary decision. Consent which is in fact forced must remain invalid. The proposals of the Commission and the rapporteur in the competent Committee for Civil Liberties as well as the demands of the European Parliament in its Resolution of 6 July 2011 (items 11 and 12) – also in view of Article 8 (2) of the EU Charter of Fundamental Rights – must not be watered down. The capacity of data subjects to protect their own data must be promoted.

- **Data controllers should not be allowed to change their purposes on their own authority**

The existing principle of restrictions on use is a key element in ensuring transparency and predictability of data processing and it must remain, as the European Parliament also demanded in its Resolution of 6 July 2011 (item 11), drawing on Article 8 (2) of the EU Charter of Fundamental Rights. Also in the future, data should be allowed to be processed only for the purpose for which they were collected. In addition, the purposes for which personal data are collected should be specifically defined.

- **Profiling must be restricted**

Profiling, or compiling a large quantity of data related to a single person, must be effectively restricted. The proposals presented must not be watered down. On the contrary, the requirements for the lawfulness of profiling must be made stricter, and it should be specified that special categories of personal data may not be used in profiling due to their highly sensitive nature. Profiling rules must apply to all systematic processing for the purpose of creating profiles. It should also be made clear that these rules also apply to online activity, such as analysing user behaviour, creating profiles in social networks for targeted advertising and assessing creditworthiness.

- **In-house data protection officers are needed to make data controllers more accountable**

The Conference points out the positive experience with in-house data protection officers in Germany. The Commission’s plan to require such officers only in companies having more than 250 employees therefore threatens a successful and established mechanism of corporate data protection in Germany. In the case of high-risk data processing, the requirement to appoint an in-house data protection officer should not depend on the number of employees. Nor should the responsibility of data controllers be watered down by requiring supervisory authorities to provide advance approval or advice on large-scale processing operations. Instead, effective self-regulation should be the first step in ensuring accountability.

- **Data controllers should not be able to choose their own supervisory authority**

Consistent data protection in the EU requires not only uniform regulation, but also uniform interpretation and enforcement by the data protection supervisory authorities. If only one supervisory authority has exclusive jurisdiction, there is a danger that companies will designate as their main establishment the one located in a Member State whose supervisory authority is considered less able or willing to enforce the law, which would undermine the standard of data protection. If a supervisory authority fails to act, legal structures are needed to ensure that data protection law is effectively enforced.

- **Supervisory authorities must have complete independence, also from the Commission**

Giving the Commission the right of final decision in enforcing the law, as provided in the Commission's proposal, violates the independence of the data protection supervisory authorities and must therefore be rejected. Assigning these competences to the Commission is not compatible with Article 8 (3) of the EU Charter of Fundamental Rights or Article 16 (2) second sentence of the Treaty on the Functioning of the European Union (TFEU), which assigns the responsibility for compliance with EU data protection to independent supervisory authorities. Drawing on the demands of the European Parliament in its Resolution of 6 July 2011 (items 42 – 44), as a consequence of the independence of the supervisory authorities, only the European Data Protection Board, and not the Commission, should decide on matters and measures that come under the Consistency Mechanism.

- **The protection of fundamental rights requires effective supervision**

As the European Parliament already made clear in its Resolution of 6 July 2011 (item 33), sanctions must have a deterrent effect and thus be appropriate to ensure that controllers and data processors permanently comply with the data protection regulations. In the framework of their independence, the supervisory authorities must be able to decide whether to use sanctions and to what extent. Without the threat of substantial fines, data protection supervision of companies would remain toothless. The possible sanctions provided for by the Commission should therefore be retained in any case.

- **A high standard of data protection for all of Europe**

For areas not specifically related to the internal market, some Member States already have numerous regulations that exceed the data protection standard set by the

general data protection directive (95/46/EC). Among other things, they consider special needs for protection and have significantly helped improve the European legal framework. A General Data Protection Regulation should therefore leave open the possibility for higher standards of data protection.