Prof. Dr. Gerrit Hornung, LL.M., University of Passau

**Abstract of the presentation for the Interparliamentary Committee Meeting**

**"The reform of the EU Data Protection framework – Building trust in a digital and global world". Session II – Harmonised and strengthened data protection rights and principles for an interconnected world, 9/10 October 2012, Brussels**

The proposal of the Commission on the reform of the data protection framework **has to be welcomed** as a valuable opportunity to modernise the hitherto existing data protection rules and principles in the face of new technological developments, new business models and new governmental possibilities to process personal data. In this reform process, the rights of the data subjects and the fundamental principles underlying these rights are of utmost importance.

The Commission's proposal rightly includes the **rights of the data subject** known in the current Directive and specifies them in more detail, although some of those rights could be further developed. By way of example, Article 20 regarding **measures based on profiling** could learn from the Council of Europe's Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling. The **restrictions for consent** in cases of a significant imbalance between the position of the data subject and the controller in Article 7 (4) **should specify** beyond recital 34 in which circumstances such an imbalance shall be assumed (i.e. in cases of monopolies, where an essential service is not otherwise available).

The rights of the data subject could significantly benefit from **privacy enhancing technologies**. In this respect, the proposal **lacks any binding statement** concerning the design of the technology and does not regulate general principles of data protection through technology at all (most notably, there is no mentioning whatsoever of anonymisation and pseudonymisation). **Data protection seals and marks** are valuable tools in this respect. As such, the Regulation should **not only include the very vague duty** of the Member States and the Commission to "encourage" these tools. Instead, there should be provisions as to the competent authorities, the procedure, applicable criteria, and legal consequences of certification.

One major issue of both the existing and the proposed rights is the **problem of enforcement**. In that respect, the restrictions provided in **Article 21** could further endanger the efficiency of date subject's rights and should thus **be tightened**. As independent supervisory bodies are an essential part of the enforcement mechanism, the **consistency mechanism appears to be problematic**. The proposal rightly forces Member States to grant national supervisory authorities complete independence. On a European level however, an institution would have the final say whose composition, organisation and working methods by no means reflect the principles of independent data protection supervision.

Both the two "new" rights, namely the right to be forgotten and the right to data portability, appear to address relevant problems. At the same time however, both face serious problems. **Data portability** may prevent data subjects from lock-in effects, but there will be hardly any transition from one controller to another in social networks if that transition **cuts of the communication** with existing contacts. Thus, portability is likely to be hampered without interoperability and cross-service communication (which are not only data protection issues).

As for the "**right to be forgotten**", this is **way too strong a term** for what is proposed in the Commission's draft (which at the same time finances research such as the "BlogForever" project aiming at indefinitely preserving internet content). In its current form, the right will hard-

ly have any effect: first, a controller who has made personal data public will in most cases not know which third parties process the data afterwards (this follows from the very notion of "public") and thus not know who it has to inform. Second, this duty to inform is in not a right of the data subject, and it is **in no way a right to be forgotten**. The **real problems** are located on the substantial level, i.e. within the relationship of the data subject and the third parties, which may have legitimate grounds to further process the data. This may include publishers, content providers, search engines or private parties who do not even fall within the ambit of data protection law (the legal consequences of the last case are unclear). Thus a right to be forgotten would **need to mitigate the conflict** between, on the one hand, freedom of speech and freedom of the press and on the other hand personality rights (including, but not limited to data protection). It appears that the Commission's approach aims at solving this substantial problem with a procedural duty. Instead, a substantial right to be forgotten cannot be developed without a coherent strategy as regards the competence of the Member States to provide for exemptions and derogations pursuant Article 80 (1).

The **principles underlying these rights** are mainly derived from the current Directive. While the **need for a legal basis** for data processing should in any case be upheld, the provisions share some of the problems of the current data protection framework. Two of these problems may be highlighted.

Frist, the lawfulness of processing "necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller" (Article 6 (1) lit. e) appears to be **very broad**, particularly as regards the notion of public interest. Apart from the vague principles in Article 6 (3), there are no requirements for the laws of the Union and the Member States in that respect, and indeed no further explanation of what may be regarded as "public interest". The same applies to the term "task", which in turn leads to the **unclear margins for the Member States** in that respect: Are they only allowed to define certain tasks or objectives (i.e. "issuing passports and operating a passport register"), or are there possibilities to specify detailed rules, e.g. on data collection, transfer to other public authorities, access for private parties etc.? This point should be clarified in the further legislative process.

Second, data processing on the grounds of "**legitimate interests** pursued by a controller" (Article 6 (1) lit. f) could potentially render the rest of Article 6 meaningless for private controllers, depending on which grounds are considered legitimate in this respect. Importantly, it **should be clarified** that where the legal relationship between a data subject and a controller is governed by a contract (lit. b), this contract may not be overruled on the grounds of vague legitimate interests. This and other clarifications should be included in the Regulation itself. The competence to adopt **delegated acts** in this respect (Article 6 (5)) is one example for the fact that, under the current proposal, the Commission would gain a range of competences that is inadequately wide and raises **concerns with regard to primary law**.

*G. Hornung*: A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012. (2012) 9:1 SCRIPTed 64, available at http://scripted.org/?p=406.

*M. Bäcker and G. Hornung*: Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on the national Police Laws and Laws of Criminal Procedure. Computer Law & Security Review 28 (2012), forthcoming.

*G. Hornung*: Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the future European Data Protection Framework. INNOVATION: The European Journal of Social Science Research 25 (2012), forthcoming.