



*The 7<sup>th</sup> International Scientific Conference*  
**“DEFENSE RESOURCES MANAGEMENT  
IN THE 21<sup>st</sup> CENTURY”**  
**Braşov, November 15<sup>th</sup> 2012**



## **THE REFORM OF THE EU'S DATA PROTECTION RULES**

**Cpt. cdor Lucian MOLDOVAN**

The 71<sup>st</sup> Air Flotila / Campia Turzii / Romania

### **Abstract:**

The rapid rhythm of technological change and globalisation have profoundly transformed the life of every people and the way in which an ever-increasing volume of personal data is collected, accessed, used and transferred. As of 1 January 2012, the European Union has 503.5 million people and more than 250 million internet users. A big part of these people use online services for commercial or social activities. In exchange for these services people provide personal data that can be used later by companies for different goals. Obtaining personal data has become a purpose and an asset for many companies. Collecting, accessing, analysing, transferring and using the data of potential customers is often an important part of their activities. Companies are using new technologies to develop smart ways for obtaining information and ordinary users are increasingly less protected. Many times, in this fast growing race for information, the rules, the laws and the people's rights are violated. In order to protect the public against these abuses the European Commission was obliged to take action. This paper sets out the main elements of the reform of the EU framework for data protection.

*Key words: personal data, collecting information, data protection, people's rights*

### **1. Introduction**

According to Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) personal data protection is a fundamental right in Europe and needs to be protected accordingly. The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, receiving medical treatment, at a police station or on the Internet.

Personal data is any information **relating to an individual**, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information or computer's IP address. The EU data protection rules apply when a person can be identified, directly or indirectly, by such data.

Although individuals have the right to enjoy effective control over their personal information 72% of internet users in Europe still worry that, in this new digital medium, their personal data are poorly protected, they don't have enough control over them and they are not properly informed of what happens to their personal information, to whom it is transmitted and for what purposes. Often, they don't know how to exercise their rights online.

Lack of confidence makes consumers hesitant to buy online and accept new services. Therefore, a high level of data protection is very important to enhance trust in

# ***THE REFORM OF THE EU'S DATA PROTECTION RULES***

online services and to use the potential of the digital economy. This level can be achieved by modern and clear rules across the EU. That is why the European Commission was proposing a fundamental reform of the EU's data protection framework.

## **2. Evolution of data protection reform**

The EU's 1995 Directive, the central legislative instrument for the protection of personal data in Europe, was a milestone in the history of data protection. Its objectives remain valid.

In 2007 the Lisbon Treaty has created, with Article 16 TFEU, a new legal basis for a modernised and comprehensive approach to data protection and the free movement of personal data, also covering police and judicial cooperation in criminal matters.

Since 2009 the European Commission has launched public consultations on data protection and engaged in intensive dialogue with stakeholders.

On 4 November 2010, the Commission published a Communication on a comprehensive approach on personal data protection in the European Union which set out the main themes of the reform.

Between September and December 2011, the Commission was involved in a dialogue with Europe's national data protection authorities and with the European Data Protection Supervisor to explore options for more consistent application of EU data protection rules across all EU Member States. These discussions made clear that both citizens and businesses wanted the European Commission to reform EU data protection rules in a comprehensive manner.

In 2012 the European Commission proposed a strong and consistent legislative framework across Union policies, enhancing individuals' rights, the Single Market dimension of data protection and cutting red tape for businesses.

This new framework consist of a Regulation (replacing Directive 95/46/EC) setting out a general EU framework for data protection and a Directive (replacing Framework Decision 2008/977/JHA) setting out rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

## **3. The main problems affect the right to data protect**

The main problems that cause difficulties for individuals and business in exercising the right to data protected are:

- the rules are not updated and modernised;
- the ways are not sufficiently harmonised across Member States;
- inconsistent enforcement of data protection rules across UE;
- the powers of the national authorities responsible for data protection are not harmonised enough to ensure consistent and effective application of the rules;
- exercise of the rights is more difficult in some Member States than in others, particularly online;
- too large volume of data collected everyday;
- users are often not fully aware that their data is being collected;
- there is not a mutual trust between police and judicial authorities of different Member States;
- the mechanisms for transferring data to third countries have to be improved;

## ***THE REFORM OF THE EU'S DATA PROTECTION RULES***

- the development of the digital economy across the EU's Single Market and beyond is not stimulated enough.

### **4. How the new rules solved the problems**

Though the objectives of the EU's 1995 Directive remain valid should be kept in mind that it was adopted when the internet was initially and, in today's new digital medium, existing rules don't provide the harmonisation required and the necessary efficiency to ensure the right to personal data protection. New rules will update and modernise the principles enshrined in the 1995 Data Protection Directive.

One important problem is there are still considerable divergences in the rules across Member States. As a consequence, data controllers may have to deal with 27 different national laws and requirements. The results are a fragmented legal environment which has created legal uncertainty, unequal protection for individuals, unnecessary costs and administrative burdens. New rules will remove barriers to the internal market which exist because of the divergent legal approaches and will achieve substantial harmonisation of data protection rules at EU level, creating one single law applicable across the EU. The savings from having one single law in terms of removed administrative burden will be € 2.3 billion per year.

An „one-stop-shop” for enforcement will be established. Thus businesses or organisations will only have to deal with one single data protection authority - the authority in the country where they have their main base.

There are a lot of cases when online social networking services collect much more data than individuals were aware of and some personal data that they thought had been deleted are still stored. So “the right to be forgotten” is broken. In order to reduce these practices the online social networking services (and all other data controllers) will be obligated to minimise the volume of users' personal data that they collect and process and to delete an individual's personal data if that person explicitly requests deletion and where there is no other legitimate reason to retain it. In this specific case, this would oblige the social network provider to delete the person's data immediately and completely.

Another aim of the new legislative acts is to strengthen rights, to give people efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively. With new rules will be improved individuals' ability to control their data, improved the means for individuals to exercise their rights, reinforced data security and enhanced the accountability of processing data.

The new Directive will apply general data protection principles and rules to police and judicial cooperation in criminal matters. These rules will apply to both domestic processing and cross-border transfers of data. Having the same law in all EU Member States will make it easier for our police forces to work together in exchanging information. This will help fight crime more effectively. If people's personal data is shared in this way, they can be confident that it will be protected by the same law everywhere and that your fundamental right to data protection will be respected.

A stronger, simpler and clearer data protection framework will encourage companies to get the most out of the Digital Single Market, fostering economic growth, innovation and job creation. This will especially help small and medium-sized enterprises. For companies offering cloud services – remote storing and processing of data on computer servers – the trust in the EU's coherent regulatory regime will be a key asset and

## ***THE REFORM OF THE EU'S DATA PROTECTION RULES***

attractive point for investors. Having the same rights across the EU will also boost individuals' confidence in the fact that the protection they get for their data will be equally strong, wherever their data is processed. This will improve trust in online shopping and services, helping to boost demand in the economy. Both for citizens and business, these reforms will help break down barriers that are hindering Europe's response to the crisis.

Individuals' rights must continue to be ensured when personal data is transferred from the EU to third countries, and whenever individuals in Member States are targeted and their data is used or analysed by third country service providers. This means that EU data protection standards have to apply regardless of the geographical location of a company or its processing facility. In today's globalised world, personal data is being transferred across an increasing number of virtual and geographical borders and stored on servers in multiple countries. More companies are offering cloud computing services, which allow customers to access and store data on remote servers. These factors call for an improvement in current mechanisms for transferring data to third countries. This includes adequacy decisions and appropriate safeguards such as standard contractual clauses or Binding Corporate Rules, so as to secure a high level of data protection in international processing operations and facilitate data flows across borders.

In order to implement the new rules the Regulation provides for sanctions that are proportionate and dissuasive. For first offences, the national supervisory authorities may send a warning letter. For serious violations (such as processing sensitive data without an individual's consent or on any other legal grounds) supervisory authorities shall impose penalties up to €1 million or up to 2% of the global annual turnover of a company. The fines start out at €250,000 or up to 0.5% of turnover for less serious offences (a company charges a fee for requests from a user for his data) and move up to €500,000 or up to 1% for not supplying information to a user or for not having rectified data.

### **5. Conclusion**

The EU data protection reform aims to build a modern, strong, consistent and comprehensive data protection framework for the European Union. Individuals' fundamental right to data protection will be reinforced. The other fundamental rights will be respected too. The reform will first of all benefit individuals by strengthening their data protection rights and their trust in the digital environment. The reform will furthermore simplify the legal environment for businesses and the public sector substantially.

Finally, the reform will enhance trust among law enforcement authorities in order to facilitate exchanges of data between them and cooperation in the fight against serious crime, while ensuring a high level of protection for individuals.