**Some General Trends and Phenomena Noted by the Czech DPA**

**in Relation to the Private Sector**

In the short time I have I would like to share some experience noted by the Czech DPA on general trends and phenomena in relation to the private sector.

They are mostly related to the question whether there is something of common in the data protection trends in the both sectors, private and public, and how far the approach of DP authority to both sectors can influence the confidence of business that the data protection principles don´t mean factual burden. We´ll also see that it is sometimes very difficult to leave on business entities to ensure the actual compliance with data protection principles being well aware that more and better data protection means – through trust of their clients and employees – better business. I´ll also touch at the end our experience with some business-friendly tools for enhancing and empowering DP principles.

**1. Certain trends posing new risks for data protection are identical in the public and private sectors, particularly**

- **attempts to concentrate major quantities of data in central databases or through interconnection of decentralized sources; and**
- **monitoring of persons by videosurveillance systems and other means of identification and localization**
- **increased merging of the public and private sectors either imposed or permitted by the law.**

In general, it can be stated that all these trends (subject to certain exceptions, which I will mention later) are favorable for business. Where businesses feel that data protection supervisory bodies are opposed to these trends, they are also convinced that data protection is a burden for business. However, it must be clearly stated that efforts to overcome this conviction cannot be aimed at gradual weakening or even suppressing of the basic principles of protection of privacy and personal data, or any of these principles. On the other hand, these trends cannot be entirely denied (it would be unrealistic to do so). This results in an effort to influence, as far as we are able to with our powers, the individual measures in the sense of their modification that would correspond as much as possible to the principles of protection.

I would like to devote some attention to the issue of central databases in the public sector having something to do with business.

Public sector databases apparently do not fall within the scope of our panel; nevertheless some of them have a lot in common with business. Probably all central databases used in other European countries can be found in the Czech Republic, together with all their drawbacks. This includes, for example, the Commercial Register with publicly accessible names and addresses of natural persons, owners and members of the management and the possibility of search based on the natural persons' index.

It must be noted that the business lobby at the level of the EU Commission, as well as at the national level, strongly supports the trends aimed at centralization and interconnection of databases and provision of access to them. This is a result not only of the mentioned comfort, but also of increasing income from re-use of information from the public sector.

Also for publicly accessible databases, the DPAs should enforce compliance with the objective, for which the databases were created and made accessible, in case of re-use.

Our Office recently encountered a rather amusing case of "re-use", where a company attempted to offer paid access to the records from our register, which we provide free-of-charge, on a website located at an address that showed striking similarity to the address of our Office.

Unlike the mentioned trend of "re-use", in the area of ever increasing information growing through between G – B, we can define an area where business could be our close ally. These are cases where the law imposes or intends to impose on market undertakings, i.e. business, the obligation to process and maintain vast quantities of personal data for use in the public sector, particularly by law enforcement bodies. However, the effectiveness of this alliance is weakened by the fact that the main measures of this kind origin at an international level, i.e. in the binding *acquis communautaire*. Of course, I am referring particularly to measures based on

- Directive 2004/82/EC on obligations of air carriers (regarding API data), which is already applied in the Czech Republic, and we are still awaiting evaluation of its security effect;
- Directive 2006/24/EC on the retention of traffic data of electronic communication service providers, whose transposition to the national legislation is yet to be completed in this country; and
- a measure to use PNR data in the EU for law enforcement, which is currently under preparation at a supranational level.

These major pending and contemplated interventions are accompanied by numerous smaller and less visible measures, which may appear innocent when assessed individually, but together they continue to erode privacy. A recent example consists in the currently discussed proposal that private companies would, not only measure the velocity of vehicles on roads, but also collect personal data on the drivers for use by traffic police. Or another example: a measure is being prepared according to which traffic police would not only inform insurance companies of accidents, as has been the case to date, but also provide them with information on penalty points for road traffic offenses, etc.

I would also like to mention two major trends in the application of modern technology with an important impact on privacy and data protection, where data protection will probably never be considered by businesses to be a business asset, but rather a business nuisance. These include videosurveillance systems and DNA databases. For beeing pressed by time, I'll mention only one of them.

Databases and commercial processing of DNA is a rapidly expanding fashion that will not cease in the foreseeable future, but rather to the contrary. In this relation, commercial companies usually publicly declare a high level of protection of personal data. However, their attention is very frequently concentrated only on the aspects of technological and organizational measures against data leaks and unauthorized access to databases.

An inspection, which is still underway in a very dominant and renowned company, has revealed a number of shortcomings. The objects of business include, amongst other things, genetic testing for the purposes of determining fatherhood, family relationships and DNA analysis for research and testing of genetically determined types of diseases and for predicting the effectiveness of their treatment. The company also monitors specific DNA mutants –

markers for the purposes of timely diagnosis of some groups of diseases. In certain cases, when participating in clinical projects, the company is in the position of the processor.

The main established shortcomings include the following: The company, as the controller, failed to store personal data processed on its clients only for the period necessary for the purpose of their processing. When using personal data for scientific purposes, it also failed to render the data anonymous as soon as this became possible. It processed sensitive data on the basis of inadequately informed consent and, in the position of processor, when it found that the controller breached his obligations, it failed to terminate the processing of personal data.

Undoubtedly, this panel intends to come to the conclusion that data protection should be considered to be a business asset, rather than a business nuisance. In general, this is certainly true as, in a balanced and specific situation, adequate application of our principles should lead to greater confidence amongst the clients and employees, with an unambiguously positive effect on functioning of the market. However, I must admit that, with respect to certain phenomena, such as the mentioned boom in cameras and commercial use of DNA, I also appreciate the role played by data protection regulations, as an administrative obstacle for unlimited expansion of this facet of commercial activities.

## 2. Globalized data flows and business-friendly tools

While almost every aspect of our lives is undergoing rapid globalization, this is even more true of exchange of information and transborder data flows, including flows of personal data. It must be noted with regret that the progress in globalization of the principles of personal data protection is not entirely in accordance with this trend. Standard contractual clauses, as developed by WP 29 in several modifications, are, in my opinion, a very effective instrument, which is relatively frequently applied in the Czech Republic for overcoming this discrepancy. This is confirmed by a number of inquiries put forth and consultations required by the controllers. We do not have any statistics available as, in the procedure approved by the EU Commission, it is not necessary to request our Office for a permit to provide personal data abroad. This also eliminates an important administrative obstacle for international activities of the private sector. Indeed, otherwise, the Czech Data Protection Act requires that the controller apply to the Office for a permit for the provision of data to third countries with inadequate legislative protection of personal data.

Our Office understands the constantly growing pressure exerted by the business sector and, specifically, supranational companies, for use of Binding Corporate Rules (BCR) to overcome obstacles following from differing legislation in various countries, and it intends to promote efforts exerted in this respect. However, this self-regulation tool entails a great many problems and drawbacks that we encounter when assessing the various proposals.

While supervisory activities are expected to be as flexible and liberal as possible, we have not yet encountered a similar approach on the part of corporations. The relevant companies have never been willing to modify the draft BCR in any way. Even in cases where the representative of the corporation explained some shortcomings or irregularities of the BCR, he did so by informal means (e-mail, telephone, personal interview) and we did not succeed with our requirement that the explanation supplementing and specifying the BCR be provided in a legally binding manner, i.e. a letter signed by the statutory body of the parent company.

It is clear that this promising “measure for future” is far from universal application. Undoubtedly, an important step could be taken by WP 29 if it managed to find a solution for BCR similar to standard contractual clauses, i.e. some kind of standard BCR, even if they were stipulated in various variants and modules. However, this is a very difficult and complex task, with an unclear result. Thus, it is merely a challenge for the future.

Anyway, even this step could not be very successful unless representatives of the business realized that a more flexible approach will be welcome also on their part.