Security *versus* Data Protection – the balanced approach?
Czech Republic case

A/ GENERAL PART
B/ SPECIAL PART

A/1. Public safety and State security are the highest-risk domains of the public sector from the personal data protection point of view

Practically refering to what we were told by my more experienced colleague Peter Schaar and what we have heard at many other meetings of data protectioners that were aimed at the 3rd pillar matters. That is to lower or higher extent applicable also for the situation in the Czech Republic.

In our country as well there are well justified reasons to warn against an imbalanced approach to increasing public safety and State security, on the one hand, and to the fundamental rights of individuals, including the right to privacy, on the other hand. This includes especially certain ongoing, planned or discussed security measures, which are usually justified by the fight against terrorism and which tend to be gradually extended to other forms of crime, with an extensive impact on privacy to a great many persons. Mostly innocent people. The duty of business entities to retain, over and above the framework of their usual activities and needs, personal data of their clients, such as operational data of providers of telecommunication and internet services, or identification data of air passengers, and submit them to the authorities. - That is an example of this phenomenon. As far as the adopted and contemplated measures are concerned, the Czech Republic does not differ from other European countries. And we also noted a lot of sympathy and understanding in this respect from many representatives of Czech law enforcement bodies. I will touch on this aspect again later on.

A/2. Principle of "export of wrong practices" works as a motive power for enhancement of risk measures at both national and international levels

The Czech Republic as well as most of the EU countries could hardly boast about inventing on their domestic ground the idea of some of the latest security measures with hard privacy impacts. It is very usual to look for the roots of such trends in the United States. It is clear that the majority of the tendencies, to introduce extensive security measures can be seen in the United States and this is also to some extent comprehensible after the events of September 2001. And - it is gratifying that even in the United States there are increasing calls for the need of a balanced approach. Of the awareness of certain limits which should not be exceeded without sacrificing those values of the democratic world_that must be defended against terrorism. The

assessing the efficacy of adopted measures from the viewpoint of the security effects, on the one hand, and the expended material and moral costs, on the other hand.

But what is important and the most alarming now is that the initiative of taking doubtful security measures is being successively taken over by the EU itself. It is under the pressure of certain EU countries to achieve adoption of common security measures. For example – the data retention and the Prüm Convention - being the main latest cases. Rich documentation of this case was presented by our British colleagues last year at the London Conference of DP Commissioners. And we should also not forget that while the security measures in the United States regard mostly foreigners coming to or passing through or over the USA, the measures introduced by EU are touching directly its own citizens.

A/3. Even without the threat of new risk security measures the DPAs would have plenty of problems to solve in practical activities of law enforcement bodies

I am convinced that the real powers and independence of a DP authority can be proved by the way of how the individual authorities are exercising their competence towards the public sector in general and the law enforcement bodies such as the ministries of interior or police especially. I am glad to be able to say that the Czech Office for Personal Data Protection has all necessary prerequisites to apply its powers in this domain and it is also applying them. To illustrate the situation in the Czech Republic from the viewpoint of practical experience of the Office, I should note that a number of findings on breach of law have been made during the Office's control activities concerned with law enforcement authorities.

A/3a. Examples of breach of law enforcement bodies:

- taking of biometric samples of fingerprints for non-legitimate purposes
- non–compliance with the duty to verify whether the data are still needed
- using data of police alerting service for intelligence

The taking of biometric samples of fingerprints is an example of this breach, where relatively high fines have been imposed. In particular, contrary to the special laws, regulating this procedure, data on fingerprints stored in information systems were also utilized for purposes other than those stipulated

by applicable laws. It is highly likely, that this is a very common, if not general, practice. We have also found other shortcomings related to the police practice when processing fingerprints.

The duty to tri annually verify, for example, whether the processed data are further needed / was neglected.

Our inspectors found that data of the police alerting service had been used not only for informing the service but subsequently for intelligence needs.

A/4. Is there any hope to achieve consensus of advocates of security and of privacy and data protection at national level about what the balanced approach is?

Based on previous experience the answer is: No, if the balanced approach is not reached at the level of the whole EU (and even there an overblown optimism is not justified) and/or without carrying the discussion to much wider platforms at national level with broader public and parliaments involvement.
But it doesn't mean at all that our experience in relation to the law enforcement bodies would be exclusively negative. A lot of very good results in mutual cooperation could be presented.

A/4a Positive examples of cooperation with law enforcement bodies:

- preparation if bilateral international agreements on police cooperation, readmission etc.
- preparation of access to Schengen area
- information duty when tapping e-communication

When preparing instructions for negotiating bilateral international agreements the police invites our Office to participate and often tries to uphold our remarks.

The longterm procedure of preparing the Czech Rep. to join the Schengen family has been full of fruitful cooperation

Upon the evaluation of findings in an inspection into the processing of personal data on ongoing criminal investigations, several weak points in law were revealed related mainly to the telephone tapping and call monitoring. We sent letters to two of the Ministers and succeeded to enforce some improvements amendment of the law of criminal procedure. Namely a new provision on granting the data subject the right to be informed subsequently

about the fact that his electronic communication was tapped is worth mentioning.

B/ SPECIAL PART - PNR data in the EU as a project illustrating the gap in viewpoints between data protection and security fans

Komentář: Examples of positive and negative experiences at a national level were presented. However there is evidence that cab be clearly documented on how sharply different the views of the law enforcement authorities and the personal data protectioners are, where something almost completely new is being set up or intended for the field of security measures. One of the most striking examples has been lenghtly and unfinished procedure of the birth of the Council Framework Decision on the protection of personal data in the framework of police and judicial cooperation within criminal matters. This is still full of conflicts and misunderstandings even at a national level.
Another example, and there I feel necessary to highlight before closing my presentation, is the Commission's survey on a common EU approach to the use of PNR data for law enforcement purposes.

B/1. When completing the questionnaire on the use of PNR data for EU law enforcement purposes the differences in views were sharply demonstrated

Let's look at several of Ministry of Interior answers from the questionnaire distributed by the Commission, when compared with the opinion of Czech data protectioners. Our Office completed the questionnaire first and sent it both, to WP 29 and the Ministry of Interior. We were also invited to take part in the discussion of several involved bodies before the Ministry of Interior sent the official final version to the Commission.
The questions, as well as the written replies, have been simplified and shortened for the purposes of this presentation.

B/2. Questionnaire on the possible use of PNR data in EU -

OPTION 1: DO NOTHING

Ministry of Interior ("MI"): Do nothing means to give up finding new, effective ways of fighting the wide spectrum of criminal acts."...

So they refused this option.

Despite the suggestive wording of Option 1, that the preference of doing nothing raises suspicion of passivity, our Office's standpoint was clearly in favor of this option for its prevailing benefits. We admitted to a possible reassessment of this situation after the drafting of the Council Framework Decision on the protection of personal data in the 3rd pillar is satisfactoryly finalized.

B/3. Questionnaire - OPTION 2: LEGAL INSTRUMENT

A question on scope of the instrument as regards to the forms of transport: (a) only airline PNR data, (b) air and sea data, (c) air, sea and rail data

MI: ..."We find it useful to start with an instrument that is limited to airline PNR data"...this "would be a suitable first step"...

The Ministry of Interior evidently has a taste to start with istruments limited to airline PNR data, in the same time their desire to continue with broader and broader scope of data. It is apparent.

B/4. Questionnaire - OPTION 2: LEGAL INSTRUMENT

Question addressing the data retention period: (a) immediate deletion, (b) 3,5 years, (c) longer period

MI: ..."To harmonize the procedure with the US and Canada we find it most appropriate to delete data after three and a half years" ...(with the possibility of prolongation if a person is convicted)

No long commentary is necessary to illustrate the opposite views of security and data protection advocates. Even if our Data Protection Office admitted to the possibility of considering longer period before deletion if the narrowest purpose of terrorism and related crimes is chosen.

B/5. Questionnaire - OPTION 3: ENCOURAGE COOPERATION between Member States

MI: "Policy option 3 has no practical importance. It is similar to policy option 1."

Contrary to that / our Office admitted to the possibility of encouraging the security cooperation on the basis that the existing legislation (national law, international bilateral agreements, conventions, etc., mainly if the drafting on the Council Framework Decision on the personal data protection in the 3rd pillar is satisfactorily finalized.

B/6. **TO CONCLUDE:** The idea that the discussion between advocates of security without frontiers and the human rights defenders could lead to balanced approach is unfeaseble. The only hope is to open up these bilateral discussions

along with the warnings and challenges presented at data protections conferences, such as on “Big brother”, “Little Sister”, “Globalized World”, “Terra Incognita”, etc. to much wider both national and international platforms.