

## State Data Protection Inspectorate

# Requirements to personal data protection according to Schengen Convention

Information on persons' right to private life acceding to Schengen zone

Vilnius  
2006

### Schengen zone

It is a territory of states without the internal borders, named after Schengen – the city in Luxembourg, in which the Schengen Agreement was signed.

According to plan, Lithuania is going to accede to the Schengen zone in 2007, after the forthcoming evaluations in 2006 of Lithuania's readiness for the Schengen *acquis* and the implementation of the second generation Schengen information system SIS II.

### The Schengen Agreement

On the 14<sup>th</sup> of June, 1985 five Member States: Belgium, the Netherlands, Luxembourg, Germany and France signed the *Schengen Agreement on gradual abolition of checks at their common borders* (The Schengen Agreement), the aim of which is to remove checks at their common borders on the movement of persons, citizens of Member States and facilitate the transport and movement of goods.

After some years other Member States, except the United Kingdom and Ireland, acceded to the Schengen Agreement. The two states - Norway and Iceland, a non-Member States have also acceded to Schengen Agreement.

### Schengen Convention

On the 19<sup>th</sup> of June, 1990 there was signed the Convention Applying the Schengen Agreement of 14 June 1985 concluded between the Governments of the States of the Benelux economic union, the Federal Republic of Germany and the French Republic on gradual abolition of checks at their common borders (Convention on Schengen Implementation Agreement), was the basis for establishing Schengen Information System and facilitating the implementation of the principle of free movement in Schengen *acquis*.

### Data protection supervisory system according to Schengen Convention requirements

*Schengen Joint Supervisory Authority* (Shengen JSA) is an authority set up pursuant to Article 115 of the Convention on Schengen Implementation Agreement. The Schengen JSA shall be responsible for supervising the technical support function of the Schengen Information System, joint police information system.

The Schengen JSA shall consist of two representatives from each national supervisory authority of Schengen Agreement Contracting Party. According to its composition and authorization, Schengen JSA is an independent authority.

Currently Schengen JSA is comprised of all representatives of Contracting Parties to Schengen Agreement (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden) and also of the United Kingdom and Ireland with the observer status. The representatives of State Data Protection Inspectorate as well as representatives of other new Member States of the European Union since July 2003 participate at Schengen JSA with observer status.

Schengen JSA also examines any difficulties of application or interpretation that may arise during the operation of the Schengen Information System, studies any problems that may occur with the exercise of independent supervision by the national supervisory authorities of the Contracting Parties or in the exercise of the right of access to the system, and draws up harmonized proposals for joint solutions to existing problems.

The website of Schengen JSA is by the address: <http://www.schengen-jsa.dataprotection.org/>.

### Schengen Information System (SIS)

*Schengen Information System* (SIS) was set up as an instrument of making out a balance in removing the common border controls within the States of Schengen zone. The purpose of SIS – following the Convention on Schengen Implementation Agreement is to maintain public policy and public security, including national security, in the territories of Member States and, to apply the provisions of this Convention relating to the movement of persons in those territories, using information communicated via this system.

Member States provide information through its national section (NSIS), which is connected to the central data

section (CSIS). This joint system establishes communication among all Member States and provides for the end users (police departments, embassies and consulates, migration institutions, etc.) access to information online, necessary for fulfillment of their direct functions.

### **What type of personal data and for what purposes may be stored in Schengen Information System?**

According to Article 94 of the Convention on Implementation Schengen Agreement, SIS shall store only those categories of data, supplied by Contracting Countries. The mentioned categories shall be related to data regarding persons, objects and vehicles.

Data stored in the SIS regarding persons are as follows:

- a) surname and forename, any aliases possibly entered separately;
- b) any specific objective physical characteristics not subject to change;
- c) first letter of second name;
- d) date and place of birth;
- e) sex;
- f) nationality;
- g) whether the persons concerned are armed;
- h) whether the persons concerned are violent;
- i) reason for the alert;
- j) action to be taken.

Other data, in particular the data, specified in Article 6 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (sensitive personal data: data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life) shall not be authorised.

Pursuant to Articles 95-99 of Convention for Schengen Implementation Agreement, alerts about persons may be included to SIS for the following reasons:

- arrest for extradition purposes (Article 95);

- alert on aliens for whom an alert has been issued for the purposes of refusing entry (Article 96);
- alert on missing persons, missing minors and persons who must be detained following a decision by a competent authority (Article 97);
- alert on witnesses, persons summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted, or on persons who are to be served with a criminal judgment or a summons to report in order to serve a penalty involving deprivation of liberty (Article 98);
- alert on persons or vehicles for the purposes of discreet surveillance or of specific checks, for the purposes of prosecuting criminal offences and for the prevention of threats to public security (Article 99).

### **The rights of persons whose personal data are stored in SIS**

The Convention on Implementation of Schengen Agreement establishes that person's rights are:

- to have access to data relating to him which are entered in the SIS (Article 109);
- to have factually inaccurate data relating to him corrected or unlawfully stored data relating to him deleted (Article 110);
- in the territory of each Contracting Party, bring before the courts or the authority competent under national laws an action to correct, delete or obtain information or to obtain compensation in connection with an alert involving him (Article 111);
- to ask the supervisory authorities to check the data concerning him which are entered in the SIS and the use made of such data (Article 114);

Communication of information to the person shall be refused if this is indispensable for the performance of a

lawful task in connection with the alert or for the protection of the rights and freedoms of third parties. In any event, it shall be refused throughout the period of validity of an alert for the purpose of discreet surveillance.

### **Where to apply for the right to data protection?**

For the exercising of his rights, a person may apply either directly to institution in charge of the processing of his data (e.g. police institutions), or to national supervisory authority – State Data Protection Inspectorate.

### **National supervisory authority**

The purpose of the *National Supervisory Authority* is in accordance with national law for carrying out independent supervision of the data file of the national section of the SIS and for checking that the processing and use of data entered in the SIS does not violate the rights of the data subject.

State Data Protection Inspectorate was assigned responsible for performing independent checking of lawfulness of personal data processing in national SIS. One of the functions of State Data Protection Inspectorate – to execute supervision of lawfulness of personal data processing in national SIS.

For more information, please apply to us:

#### **State Data Protection Inspectorate**

Gedimino Ave. 27/2  
LT-01104 Vilnius  
Lithuania

Tel. +370 5 279 1445  
Fax. +370 5 261 9494

<http://www.ada.lt>