Personal Data in the Schengen Information System
The Schengen Agreement and Schengen Area

The Schengen Agreement Area is a territory without internal border control between the Schengen Agreement Member States. The border control is carried out once entering the Schengen Area. The Schengen cooperation purpose is to protect the individuals and their property by reducing opportunities for this right to be abused. In order to ensure information exchange, a special information system has been established, the Schengen Information System (SIS), and within this system there is intensive and effective cooperation between Schengen Area countries, ensured through the cooperation of police, customs, external border control and judicial authorities, which has all been necessary in order to eliminate the internal borders. The first action to move towards internal border within the common border management policy was carried out on 14 June 1985, when five out of ten member states of the European Economic Community signed the

The Schengen Area encompasses the following 26 European countries

Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Island, Italy, Latvia, Lichtenstein, Lithuania, Luxemburg, Malta, the Netherlands, Norway, Poland, Portugal, Slovakila, Slovenia, Spain, Sweden and Switzerland.

Table No.1 The Schengen Area Member States
Schengen Agreement. Furthermore after five years a Convention implementing the Schengen Agreement was signed (this agreement and convention known as Schengen acquis).

Latvia joined the Schengen area on 21 December 2007 and the citizens of Latvia are not going through the border control procedure once entering the countries of the Schengen Area. Once travelling outside the Schengen Area or entering in the Schengen area from the countries that are not within the territory of the Schengen Agreement, the border control procedure applies. Travelling between the Schengen Agreement countries, the border control is not being carried out, also when crossing the internal borders of the Schengen Area (for example, the border between Latvia and Lithuania). However, at the frontier area there might be some border check-ups carried out by the border guards.

**Schengen Information System**

The Schengen Information System was established in accordance with the legal acts of the European Union, in order to strengthen public order and security in the territory of the Schengen Area Member States, ensuring access to alerts for the competent institutions and authorities of the Member States.

Initially the Schengen Information System (SIS I) was elaborated within the intergovernmental project and it started to operate in 1995. The SIS I was in operation until May 2013 when it was replaced with the SIS II (already in December 1996, it was decided to establish the second generation information system (SIS II), considering the need to connect more member states to the system).

Both the SIS I and the SIS II comprise the national systems which are established in the member states of the Schengen Area and with the help of network they are connected to the central system. The SIS II ensures the information management infrastructure that is helping to ensure the border control and the security control, as well as it helps for the court cooperation.

The SIS II is a highly efficient large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The SIS is the largest shared database on maintaining public security, supporting police and judicial cooperation, and managing external border control in Europe. Participating states provide entries in the SIS (called “alerts”) on wanted and missing persons, lost and stolen property, and entry bans. It is immediately and directly accessible to all authorized police officers and other law enforcement officials and authorities who need the information to carry out their roles in protecting law and order and fighting crime. It covers most of the European Union countries (see the table No.1) as well as Norway, Iceland and Switzerland. The SIS II is managed by the European Agency for the Operational Management of large-scale IT Systems in
the Area of Freedom, Security and Justice (eu-LISA), a newly established EU agency to provide a long-term solution for the operational management of large-scale IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU (additional information - http://www.eulisa.europa.eu).

In Latvia, the Law on Operation of the Schengen Information System determines the procedure for maintenance and use of this system. The Information Centre of the Ministry of the Interior is the controller in relation to Latvia’s section of the SIS II. Additionally, the SIRENE information system has been established, which processes supplementary information and alerts. SIRENE stands for Supplementary Information Request at the National Entry, and outlines the main task of the “SIRENE Bureau” established in all the Schengen States, which is the exchange of additional or supplementary information on alerts between the states. SIRENE Bureaus provide supplementary information on alerts and coordinate measures in relation to alerts in the SIS II, ensuring that appropriate action is taken if a wanted person is arrested, a person who has been refused entry to the Schengen area tries to re-enter, a missing person is found, a stolen car or ID document is seized, etc.

In order to ensure the information exchange among the law enforcement institutions of the Schengen member states at the moment when it is concluded that an alert is entered into the SIS II regarding a person or an object, as well as to ensure the search for wanted persons internationally, there is a SIRENE national unit established under the International Police Co-operation Department of the State Police of Latvia. The SIRENE Latvia National Unit checks the quality of the alerts to be entered into the SIS II and their legal validity deriving from the requirements of the Schengen acquis.

SIRENE Latvia National Unit is the only institution in Latvia that has rights to consider the access right requests from natural persons and to provide the answer on those requests regarding the personal data processes within the SIS II and SIRENE information system. Additional information regarding the SIS II is available at the website of the State Police - http://www.vp.gov.lv.

Rights of access to personal data, and their rectification or deletion

Any individual has the right to receive information regarding his or her personal data in the SIS or
SIRENE information system, as well as information regarding recipients of his or her personal data, if its disclosure is not prohibited by a law within the field of national safety, protection and criminal law, as well as if restrictions for issuing data have not been determined by another Member State. Moreover, any individual has the right to request the correction of one’s personal data in the SIS II or its deletion, and erasure in case when personal data is inaccurate, is outdated or incomplete, or illegally obtained or not necessary for the purpose that they have been collected for.

In order to receive the information processed in the SIS II, individuals must submit a written application to the State Police or the corresponding diplomatic or consular representation of the Republic of Latvia.

The contact information of the State Police of Latvia:
SIRENE Latvia National Unit
Ciekurkalna 1. linija 1, k-4
Riga LV-1026
ph. + 371 67219053

Information regarding the diplomatic and consular representation for the Republic of Latvia is available at the website of the Ministry of Foreign Affairs of the Republic of Latvia: http://www.mfa.gov.lv.

The application should contain the following information:

1. information regarding the applicant: given name (names), surname, date of birth, personal identity number (if any), place of birth, nationality, and the type, number, issuing authority, date of issue, and term of validity of a personal identification document (if any);
2. the amount of requested information (information regarding the data subject, information regarding recipients of the personal data of the data subject);
3. the type of receipt of information (appearing in person at the State Police institution or mission or sending information to the indicated address);
4. the given name, surname, personal identity number (if any) and the date of birth of the authorized person, if information is requested by the authorized person.

The application can be submitted in Latvian, English and Russian. A sample application form is available at the website of Data State Inspectorate of Latvia: http://www.dvi.gov.lv.

The data subject, by submitting an application, shall confirm his or her identity by providing a personal identification document. An authorized person shall present a notary-certified power of attorney that gives the right to receive information regarding the data subject or shall present a document that confirms the rights of parents, adopters, guardians or trustees. If the application is submitted electronically, the identity of the data subject shall be confirmed by secure electronic signature.

The SIRENE Latvia National Unit shall examine the application and, within a time period of one
month after the receipt thereof, shall provide the requested information or shall refuse to provide the information by sending a letter to the indicated address or issuing it upon signature. If the data subject has indicated a wish to receive the answer in person by appearing at the State Police institution or mission, the SIRENE Latvia National Unit shall send the requested information to the relevant State Police institution or mission.

The requested information can be withheld if some of the necessary information has not been submitted, if it is inaccurate and therefore hinders identification of the data subject, as well as in cases when the requested information cannot be provided in accordance with national legislation in the fields of national security, protection and criminal law, or in cases when another Member State has determined such restrictions. Additionally, the individual has the right to request rectification and deletion of his/her data if his/her personal data are inaccurate. In case the requested information is withheld from the data subject or an authorized person, or there is a refusal to delete or to rectify personal data, the data subject or authorized person has the right to submit a request/complaint to the Data State Inspectorate regarding the necessity to examine whether the rights of the data subject have been ensured. Requests/complaints can be sent to the Data State Inspectorate in Latvian, English and Russian, sample form available at the website of the Data State Inspectorate - http://www.dvi.gov.lv.

The contact information of the Data State Inspectorate:
Blaumana iela 11/13–11
Riga, LV-1011
Latvia
Phone: + 371 67223131
Fax: +371 67223556
E-mail: info@dvi.gov.lv

A Guide for Exercising the Right of Access to the Schengen Information System

In order to assist the data subjects in exercising their right of access to the SIS II, the SIS II Supervision Coordination Group that consists of the personal data protection supervision authorities of the Schengen Area member states and the European Data Protection Supervisor Bureau has elaborated a guide in English. This guide explains how the data subject can exercise his/her rights, such as information on all the Member State data protection authorities, police and other institutions related to the SIS II issues. The text of this guide is available in English at the website of the Data State Inspectorate of Latvia – www.dvi.gov.lv.