



Schengen Area and data protection

Persons whose personal data are collected held or otherwise processed in the second generation Schengen Information System (hereinafter „SISII”) are entitled to rights of access, correction of inaccurate data and deletion of unlawfully stored data. The ways of exercising these rights are described in this brochure.

What is the Schengen Area?

The legal framework governing the Schengen Information area is governed by Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862.

The border-free Schengen Area guarantees free movement to EU citizens, along with non-EU nationals, legally residing in the EU. Free movement of persons enables every EU citizen to travel, work and live in an EU country without special formalities.

Countries, which are part of the Schengen Information Area must meet the requirements for effective border control at the external borders, as well as implement security measures in connection with the abolition of internal border controls.

At the present moment, almost all EU Member States, as well as Iceland, Norway, Switzerland and Liechtenstein, fully implement the Schengen acquis. Bulgaria is a full user of SIS II, fully applying the Schengen acquis. A political decision on its accession is expected *de jure*.



КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

Commission for personal data protection

2 Prof. Tsvetan Lazarov Blvd., Sofia 1592

E-mail: kzld@cpdp.bg

Web-site: www.cpdp.bg

For consultation on the implementation of Regulation (EU) 2016/679 and the national legislation on the protection of personal data – 02/91-53-555





The second generation Schengen Information System(SIS II)

The Schengen Information System was set up to help maintain internal security in the Schengen Information Area, and is accessible only to the competent authorities - the Ministry of the Interior (MoI); Ministry of Foreign Affairs (MFA); State Agency for National Security (SANS) and the institutions in charge of border and customs control; National Customs Agency; State Agency for Refugees and the Judiciary in the performance of their duties in SIS II. The system consists of:

- ✓ Central system (Central SIS II);
- ✓ National system (N.SIS II) in every member state, which is connected to the SIS II;

✓ A communication infrastructure between Central SIS and N.SIS that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between authorities, responsible for the exchange of any additional information (SIRENE Bureau). The data controller for the N.SIS II is the Minister of Interior, and the SIRENE Bureau is a part of the International Operational Cooperation (IOC) Directorate with the MoI.

Rights of individuals in the SIS II

Individuals are entitled to rights of information and access to their personal data, collected in SIS II, as well as the right to demand correction or deletion of their data.

- ✓ Right to information – whether personal data of the individual is stored in the system;
- ✓ Right to correction or deletion of data – personal data may be corrected when they are in fact inaccurate or incomplete, and their deletion may be requested if they have been illegally stored;

The right to access for individuals can be exercised directly to the SIRENE Bureau in the IOC Directorate or indirectly through the Commission for Personal Data Protection.

Suspicious of misused identity

False identity documents or identity documents belonging to someone else can be used when carrying out criminal offences or attempting to enter or stay in the Schengen Area.

Once duly established by the competent authorities with the relevant "identity theft" act, data on the person whose identity has been misused may be added to a SIS alert, given that the person has given their explicit consent and the data is used for avoiding misidentification only.

Legal Remedies

When the individual's request has not been granted or they considers that their rights have been violated, they have the right to file a complaint to the national data protection supervisory authority - the Commission for Personal Data Protection, or to appeal before the relevant competent court.

Contacts with the national competent authorities in N.SIS II:

