



Personal Data Protection in the Schengen Information System



What is the Schengen Area?

It is a territory of the States without internal borders named after the town of Schengen in Luxembourg where the Schengen Agreement was signed. Lithuania became a member of the Schengen Area in 2007.



What is the Schengen Agreement?

On 14 June 1985 five Member States – Belgium, the Netherlands, Luxembourg, Germany and France signed the Schengen Agreement on the gradual abolishment of their common border control (the Schengen Agreement) the purpose whereof was to abolish the control over persons, citizens of the Member States crossing the borders and facilitate the cross-border movement of vehicles and goods. Several years later other Member States, except the United Kingdom and Ireland, joined the Schengen Agreement. Norway, Iceland, Switzerland and Liechtenstein, which are not the Member States, also joined the Schengen Agreement.



What is the Schengen Convention?

On 19 June 1990 a Convention implementing the Schengen Agreement of 14 June 1985 among the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolishment of their common border control (Convention implementing the Schengen Agreement) was signed. It constitutes the basis for the establishment of the Schengen Information System and facilitates the enforcement of the principle of free movement by establishing the Schengen Area.



What is the Schengen Information System?

The Schengen Information System is the largest information system in Europe where personal data are processed for the purposes of ensuring a high level security, including the maintenance of safety of the society and public order and security in the territories of the Member States.

Information on individuals who pose threat to public order, safety of the society and national safety when a third country national has been convicted in the Member State for an offence carrying a penalty involving deprivation of liberty of at least one year or there are reasonable grounds to believe that a third country national has committed serious offences, or there are clear evidences that he/she intends to commit such offences in the territory of the Member State, also when a third country national has entered (attempted to enter) the States of the Schengen Area unlawfully or he/she has no right of residence in the EU is processed in the Schengen Information System. This system also contains alerts on missing persons, especially children, as well as information on certain objects, for instance, banknotes, vehicles, firearms and personal identity documents, which could have been stolen, misappropriated or gone missing. Information entered into the SIS by the national authorities is provided via the central system to all Schengen States.

On 09.04.2013 the Schengen Information System of the second generation (hereinafter – SIS II) started its operation. It was replenished with new functions, such as the possibility to enter biometric data (fingerprints and photographs), new type alerts (on stolen aircrafts, ships, containers, payment instruments) or the possibility to relate different alerts (for instance, alert on a person and a vehicle).



How is personal data protection ensured?

Institutions in every country using SIS II are required to check the quality of information entered by them into the system. There are strict requirements for the data protection in the Schengen Area. When personal data are stored persons shall have the right to request access to data related to them and make sure they are entered correctly and lawfully. If that is not the case, persons shall have the right to request that data related to them are corrected or deleted. Denying access is possible only when it is necessary for the performance of a lawful task related to the request and the implementation of other rights and freedoms of individuals.



How to address concerning access, correction, modification or unlawful use of personal data?

If you believe that your personal data were used unlawfully, they need to be corrected or deleted, you may address concerning the access to these data in any Schengen State contacting directly to the competent authority or institution. Requests for access, correction or deletion in Lithuania should be addressed to the Ministry of Interior of the Republic of Lithuania (www.vrm.lt) which is the data controller.



National supervisory authority

The purpose of the national supervisory authority is to monitor independently the legality of personal data processing performed by SIS II in its territory as well as transfer of personal data performed by SIS II from its territory and the legality of further exchange of additional information and

its processing. The State Data Protection Inspectorate is appointed as the competent authority in Lithuania.

For more information please check the "Guide for Exercising the Right of Access" that may be accessed on the website of the State Data Protection Inspectorate at www.ada.lt or contact the State Data Protection Inspectorate at

A. Juozapavičiaus St. 6, LT-09310 Vilnius, Lithuania
Tel. + 370 5 271 2804. Fax. + 370 5 261 9494
<http://www.ada.lt>
ada@ada.lt

