

CITIZENS' RIGHTS IN THE FIELD OF THE SCHENGEN INFORMATION SYSTEM

1. General presentation of the Schengen Information System

The Schengen Information System (SIS) was implemented as a search system for persons and objects by the Convention implementing the Schengen Agreement of 19 June 1990. The SIS was designed as a compensatory measure to the lifting of internal border controls with the aim of ensuring a high level of security in the European Union's area of freedom, security and justice.

The system includes alerts

- i. On persons, namely :
 - Third-country nationals subject to a return decision,
 - Third-country nationals subject to a refusal of entry and stay,
 - Persons wanted for arrest for surrender or extradition purposes,
 - Missing persons, including :
 - Children at risk of abduction by a parent, a family member or a guardian,
 - Vulnerable persons who need to be prevented from travelling,
 - Persons sought to assist with a judicial procedure,
 - Persons for discreet, inquiry or specific checks,
 - Unknown wanted persons for the purpose of identification under national law.
- ii. On objects:
 - For discreet, inquiry or specific checks,
 - For seizure or use as evidence in criminal proceedings.

2. Legal framework applicable to SIS as well as to data protection

The SIS is established by the following legal instruments:

- Regulation (EU) 2018/1860 of the European Parliament and of the Council, of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals,
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006,
- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

The following legal instruments are applicable in terms of data protection:

- *Loi du 1^{er} août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale* (Law of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters, transposing into national law the Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA) (hereafter « LPD »),
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereafter « GDPR »)

- *Loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données* » (Law of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework).

3. Information to be made available to the individual on data processing in the SIS

i. The data controller

In Luxembourg, the data controller for the data processing in the context of the SIS is the Grand Ducal Police, represented by its General Director.

ii. The purposes of the processing

The purposes of the processing for which the personal data are intended are the following:

- Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security,
- External border control,
- Immigration control.

iii. The categories of personal data that may be processed

The personal data that may be included in a SIS alert are listed in article 20 of Regulation 2018/1861 and of Regulation 2018/1862 as well as in article 4 of Regulation 2018/1860.

iv. The recipients or categories of recipients

National competent authorities of the Schengen Member States that can access the SIS and are thus to be considered as recipients are listed in article 34 of Regulation 2018/1861 and articles 44 to 47 of Regulation 2018/1862.

In addition to these national competent authorities, SIS can also be accessed by Europol, Frontex and Eurojust in accordance with articles 35 and 36 of Regulation 2018/1861 and articles 48 to 50 of Regulation 2018/1862.

v. The storage period

Alerts on persons and on objects shall be kept only for the time required to achieve the purposes for which they were entered.

The above-mentioned regulations foresee several time limits for a periodic review of the need for the storage of personal data with the possibility to renew the alerts.

Alerts on persons subject to a discrete, inquiry or specific check as well as certain categories of missing persons have in principle to be re-examined at the latest after one year.

Alerts on persons subject to a return decision, subject to a refusal of entry and stay, sought to assist with a judicial procedure as well as unknown wanted persons for the purpose of identification have in principle to be re-examined at the latest after three years.

Alerts on persons wanted for arrest for surrender or extradition purposes as well as certain categories of missing persons are in principle to be re-examined at the latest after five years.

Alerts on objects are in principle to be re-examined at the latest after ten years.

vi. The rights of individuals

Concerning the right for information provided under articles 13 and 14 of the GDPR, respectively article 12 of the LPD, the Grand-Ducal Police refers to the information on its website under the heading « Data

protection » (Link <https://police.public.lu/fr/support/protection-des-donnees-a-caractere-personnel.html>).

As foreseen in article 53 of Regulation 2018/1861 and article 67 of Regulation 2018/1862, individuals have the right to introduce

- A request for access to their data,
- A request for correction of inaccurate data,
- A request for deletion of unlawfully stored data,

In accordance with articles 15, 16 and 17 of the GDPR and 13 and 15 of the LPD.

These requests may be submitted to any Member State of the European Union operating the system and any of the four Schengen Associated States (Switzerland, Norway, Liechtenstein and Island). The receiving Member State will process the request according to their own national procedures in place as well as according to the European rules in force.

With regard to deadlines for processing such requests, it should be noted that both the requests for access and the requests for rectification and deletion must be answered within 1 month (article 53(4) of the Regulation 2018/1861 and article 67(4) of the Regulation 2018/1862, both referring to article 12(3) of the GDPR).

Regarding the form, Member States will have to strive to respect both the form (letter or email) of the requestor as well as the language used by them, this of course as far as possible. In general, the Grand Ducal Police processes access requests as well as correction or deletion requests if they are introduced in any of the administrative languages of the country (Luxembourgish, French, German) or in English.

In accordance with article 12(6) of the GDPR and article 11, paragraph 5 of the LPD, the Grand-Ducal Police must have sufficient guarantees to establish with certainty the identity of the person requesting information, so as not to prejudice the rights of others. The following documents have therefore to be enclosed to the requests:

For a request from an individual:

- A signed letter,
- A copy of an identity document (identity card or passport).

For a request from an individual on behalf of another individual:

- A power of attorney duly signed by both parties,
- A letter signed by the represented party,
- A copy of an identity document of represented party (identity card or passport),
- A copy of an identity document of the representing party (identity card or passport).

For a request from an attorney:

- A power of attorney duly signed by the client and the attorney,
- A copy of an identity document of the client (identity card or passport),
- A copy of an identity document of the attorney (identity card or passport),
- A copy of an attorney card or equivalent.

It goes without saying that the transmission of a copy of an identity card or passport via the Internet may present a certain risk in the event of possible abuse by a third party (for example, interception). Thus, the Grand Ducal Police recommends using the secured procedure using the data encryption key.

Finally, in exceptional circumstances and in accordance with article 53(3) of the Regulation 2018/1861, article 67(3) of the Regulation 2018/1862, and articles 14 and 15, paragraph 4 of the LPD, a Member State may take a decision not to provide information to the data subject, in whole or in part, in order to safeguard national security, defence and public security, or for the prevention, investigation, detection and prosecution of criminal offences, for as long as such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned.

vii. Right to lodge a complaint or to seek judicial remedy

In case the reply which is provided by the Grand Ducal Police does not satisfy the requestor, the latter has the right to file a complaint with the national supervisory authority, namely the « *Commission nationale pour la protection des données* », in accordance with article 77 of the GDPR, respectively in accordance with article 44 of the LPD. The national supervisory authority may be contacted under the following contact details:

Commission nationale pour la protection des données (CNPD)
Service des réclamations
15, Boulevard du Jazz
L-4370 Belvaux
Luxembourg.

Furthermore, the requestor also has the right to seek judicial remedy within three months after the receipt of the final reply at the Administrative Court of Luxembourg (Tribunal administratif) with the assistance of an attorney.