



ENTRY EXIT SYSTEM - EES

The Entry/Exit System (1) contains personal data records on third-country nationals coming to the territory of the Member States (2) for a short stay (maximum of 90 days in any 180-day period). The system became operational on 12th of October 2025. As of this date, information about your entries into and exits out of the territory of the Member States, and, if applicable, information on whether you have been refused entry, is registered in the Entry/Exit System.

To this end, your data is collected and processed on behalf of Police Authority of the Member State responsible for the processing] (controller(s)). Please see below the contact details. Your personal data is processed for the purposes of border management, preventing irregular immigration and facilitating the management of migration flows. This is required in accordance with Regulation (EU) 2017/2226 (3), specifically Articles 14, 16 to 19 and 23 of Chapter II and Chapter III of the Regulation.

Please note that the Entry/Exit System is being progressively rolled out. During this period (from 12th of October until 9th of October 2025), your personal data, including your biometric data, might not be collected for the purposes of the Entry/Exit System at all Member States' external borders. If the collection of that information is mandatory and you choose not to provide it, you will be refused entry. During the progressive roll-out, your data will not automatically be added to a list of overstayers. In addition, you will not be able to check how much longer you are authorized to stay using the EES website or equipment available at border crossing points. You can verify the duration of your authorized stay by using the short stay calculator tool available on the European Commission website at: https://home-affairs.ec.europa.eu/policies/schengen/border-crossing/short-stay-calculator_en.

After the progressive roll-out of the Entry/Exit System, your personal data will be processed as otherwise set out in this form.

What data is collected, recorded and processed?

During checks at the external borders of the Member States, the collection of your personal data is mandatory for the examination of entry conditions. The following personal data is collected and recorded:

- (1) data listed in your travel document; and
- (2) biometric data: from your facial image and fingerprints (4)

Data about you is also collected from other sources, depending on your situation:

- (1) the Visa Information System: data contained in your personal file; and
- (2) the European Travel Information and Authorization System, in particular the status of your travel authorization and your family member status, if applicable.

What happens if you do not provide the requested biometric data? If you do not provide the requested biometric data for registration, verification or identification in the Entry/Exit System, you will be refused entry at the external borders.

(1) Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011

(2) Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and Switzerland.

(3) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 on establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327 9.12.2017, p. 20).

(4) Please note that the fingerprints data of third-country nationals who do not need a visa to enter the Schengen area and holders of Facilitated Transit Documents will also be stored in the Entry/Exit System. If you need a visa to enter the Schengen area, your fingerprints will already be stored in the Visa Information System as part of your file there and will not be stored again in the Entry/Exit System.

Who can access your data?

Member States can access your data for the purposes of border management, facilitation of border crossings, immigration, and law enforcement. Europol may also access your data for law enforcement purposes. Under strict conditions, your data may also be transferred to a Member State, a third country or an international organization listed in Annex I of Regulation (EU) 2017/2226 (5) for the purposes of return (6) or law enforcement (7).

Your data will be stored in the Entry/Exit System for the following duration, after which it will be automatically erased: (8)

- (1) records of each entry, exit or refusal of entry record are stored for 3 years starting on the date of the entry, exit, refusal of entry record; (9)
- (2) the individual file containing your personal data is stored for 3 years and one day starting from the date of the last exit record or of the refusal of entry record where is no entry recorded during that period;
- (3) where there is no exit record, your data are stored for 5 years starting on the date of the expiration of your authorized stay.

Remaining authorized stay and overstay

You have the right to receive from the border guard information on the maximum remaining duration of your authorized stay on the territory of the Member States. You can also consult the following website [link to EES public website] or, where available, the equipment installed at borders to self-verify your remaining authorized stay.

If you overstay the period of your authorized stay, your data will be automatically added to a list of identified persons (a list of overstayers). The list can be accessed by competent national authorities. If you are on this list of overstayers [consequences of being an overstayer to be added by the Member States]. (10) However, if you can provide credible evidence to the competent authorities that you exceeded the authorized duration of your stay due to unforeseeable and serious events, your personal data can be rectified or completed in the Entry/Exit System and you can be removed from the list of overstayers.

Your rights with regard to the processing of personal data

You have the following rights:

- (1) to request from the controller access to data relating to you;
- (2) to request that inaccurate or incomplete data relating to you is rectified or completed; and
- (3) to request that unlawfully processed personal data that concerns you is erased or that the processing thereof is restricted. If you want to exercise any of these rights listed in points (1) to (3), you must contact the data controller or data protection officer indicated below.

(5) UN organization, the International Organization for Migration (IOM) or the International Committee of the Red Cross.

(6) Article 41(1) and (2) and Article 42.

(7) Article 41(6).

(8) If you are subject to visa requirement, your fingerprint will not be stored in the Entry/Exit system as they are already stored in the Visa Information System.

(9) In the case of third-country nationals who are family members of mobile EU, EEA or Swiss citizens (i.e. of EU EEA or Swiss citizens who travel to a State other than the State of their nationality or already reside there), and are accompanying or joining the EU, EEA or Swiss citizen, each entry, exit or refusal of entry record will be stored for one year following the date of the exit record or of the refusal of entry record.

(10) The calculation of the duration of the authorised stay and the generation of alerts to Member States when the authorised stay has expired do not apply to third-country nationals who are family members of mobile EU, EEA or Swiss citizens (i.e. of EU EEA or Swiss citizens who travel to a State other than the State of their nationality or already reside there) and are accompanying or joining the EU, EEA or Swiss citizen.

Contact details

Data controller: Police Authority, Department of National Operations, National border police unit, SE-106 75 Stockholm, Sverige, e-mail: granspolisenheten.noa.kansli@polisen.se

<https://polisen.se/en/laws-and-regulations/travel-to-and-stay-in-sweden/border-control/>

Data protection officer: Police Authority, Data protection officer, SE-106 75 Stockholm, Sweden. E-mail: dataskyddsbud@polisen.se

In line with the division of tasks between Member States' authorities and the European agencies involved, you can lodge a complaint with:

Supervisory authority of Sweden which is in charge of processing your data (e.g. if you allege that they have recorded your data incorrectly): Swedish Authority for Privacy Protection, Box 8114, SE-104 20 Stockholm, Sweden. Phone number: +46 (0)8 657 61 00, E-mail: imy@imy.se

European Data Protection Supervisor for matters of data processing by European Agencies:

<https://travel-europe.europa.eu/ees/contact-details-for-data-protection-matters>

[Further information by Member States on rights of the data subjects or the possibility of assistance by the supervisory authorities]. For additional information please consult the Entry/Exit System public website <https://travel-europe.europa.eu/en/ees>