

Information for Third-Country Nationals on the Processing of Personal Data in the Entry/Exit System

The Entry/Exit System (EES)(1) contains personal data on third-country nationals who enter the territory of the Member States(2) for a short stay (a maximum of 90 days within a 180-day period). Information regarding your entries into and exits from the territory of the Member States, and if applicable, information on any refusal of entry, will be recorded in the Entry/Exit System.

Your data will be collected and processed on behalf of the General Commissariat of the Federal Police and the Immigration Office. See the contact details below. Your personal data is processed for border management, preventing irregular immigration, and facilitating the management of migration flows. This is required in accordance with Regulation (EU) 2017/2226(3), particularly Articles 14, 16 to 19, and 23 of Chapter II and Chapter III of the regulation.

Please note that the Entry/Exit System (EES) is being introduced gradually. During this period, starting on 12 October 2025, your personal data, including biometric information, may not be collected for the purposes of the EES at the external borders of all Member States. If the collection of such data is mandatory and you choose not to provide it, you will be denied entry. During the transitional phase, your data will not automatically be added to a list of overstayers. Additionally, you will not be able to check how long you are allowed to stay via the EES website or the equipment at border crossing points. You can verify the duration of your permitted stay using the short-stay calculator available on the European Commission's website at: <https://travel-europe.europa.eu>

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 to verify whether entry conditions are met. The following personal data is collected and recorded:

- 1/ Data from your travel document, and

- 2/ Biometric data including facial images and fingerprints(4)

Depending on your situation, data about you may be collected from other sources:

- 1/ The Visa Information System: data from your personal file, and

- 2/ The European Travel Information and Authorization System: particularly the status of your travel authorization and potentially your status as a family member.

(1)Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) for the registration of entry and exit data and data on refusals of entry of third-country nationals crossing the external borders 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)Belgium, Bulgaria, Denmark, Germany, Estonia, Finland, France, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Spain, the Czech Republic, Sweden, and Switzerland.

(3)Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) for the registration of entry and exit data and data on refusals of entry of third-country nationals crossing the external borders 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)The fingerprint data of third-country nationals who do not require a visa to enter the Schengen area and holders of a facilitation transit document are also stored in the Entry/Exit System. If you require a visa to enter the Schengen area, your fingerprints are already stored in the Visa Information System as part of your file and are not stored again in the Entry/Exit System.

What happens if you do not provide the required biometric data?

If you do not provide the required biometric data for registration, verification, or identification in the Entry/Exit System, you will be denied entry at the external borders.

Who has access to your data?

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

Your data will be stored in the Entry/Exit System for the following period and will then be automatically deleted(8):

1/ Records of each entry, exit, or refusal of entry will be retained for three years from the date of the entry, exit, or refusal of entry(9);

2/ The personal file containing your personal data will be retained for three years and one day after the date of the last exit record or refusal of entry record if no new entry record is made within that period;

3/ If no exit record is made, your data will be retained for five years after the last day of the authorized stay.

Remaining duration of authorized stay and overstay

You have the right to request information from the border guard on the maximum remaining duration of your authorized stay in the territory of the Member States. You may also consult the website <https://travel-europe.europa.eu> or, if available, use the equipment installed at the borders to verify the remaining duration of your authorized stay yourself. If you overstay your authorized duration, your data will automatically be added to a list of identified persons (an overstay list). The list is accessible to the competent national authorities so that they can take appropriate measures.(10) However, if you can provide credible evidence to the competent authorities that you exceeded the authorized stay due to unforeseen and serious events, your personal data in the Entry/Exit System may be rectified or supplemented, and you may be removed from the overstay list.

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

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

(7)Article 41, paragraph 6.

(8)If you require a visa, your fingerprint is not stored in the Entry/Exit System as it is already stored in the Visa Information System.

(9)In the case of third-country nationals who are family members of a mobile EU, EEA, or Swiss citizen (i.e., an EU, EEA, or Swiss citizen who travels to or resides in a state other than their nationality's state) and who accompany or join the EU, EEA, or Swiss citizen, all entry and exit records or refusal of entry records will be retained for one year from the date of the exit record or refusal of entry record.

(10)The calculation of the duration of the authorized stay and the generation of notifications to the Member States when the authorized stay has expired do not apply to third-country nationals who are family members of a mobile EU, EEA, or Swiss citizen (i.e., an EU, EEA, or Swiss citizen who travels to or resides in a state other than their nationality's state) and who accompany or join the EU, EEA, or Swiss citizen.

Your rights regarding the processing of personal data

You have the following rights:

- 1/ To request access to data concerning you from the data controller;

- 2/ To request the rectification or completion of inaccurate or incomplete data concerning you, and

- 3/ To request the deletion or restriction of the processing of unlawfully processed personal data concerning you.

If you wish to exercise one or more of the rights mentioned in points 1, 2, and 3, you can contact the data controller or data protection officer listed below.

Contact details:

<p>Data Controller(s):</p> <p>Minister of security and the interior Rue de Louvain 1 1000 Brussels, Belgium</p> <p>Immigration Office Pachecolaan 44 1000 Brussels, Belgium</p>	<p>Data Protection Officer(s):</p> <p>Federal Police (CG/ISPO) Koningsstraat 202A 1000 Brussels, Belgium https://www.politie.be/5998/nl/contact/contactformulier</p> <p>Immigration Office Pachecolaan 44 1000 Brussels, Belgium dpo.dvzoe@ibz.fgov.be</p>
--	--

In accordance with the division of responsibilities between the authorities of the Member States and the relevant European agencies, you can **file a complaint** with:

<p>The supervisory authority of Belgium responsible for processing your data (e.g., if you claim that your data has been incorrectly recorded):</p> <p>Supervisory Body for Police Information Leuvenseweg 48 1000 Brussels https://www.controleorgaan.be/nl/contact</p> <p>Data Protection Authority Drukpersstraat 35 1000 Brussels, Belgium contact@apd-gba.be</p>	<p>The European Data Protection Supervisor for issues related to data processing by European agencies:</p> <p>European Data Protection Supervisor (EDPS) Wiertzstraat 60, 1047 Brussels, Belgium https://edps.europa.eu</p>
---	---

For more information, consult the public website of the Entry/Exit System:

<https://travel-europe.europa.eu>