



## DATA PROTECTION NOTICE

### Database on International Protection in Europe

#### 1. Introduction

The European Union Agency for Asylum (hereinafter ‘the EUAA’ or ‘the Agency’) is committed to protecting your privacy. The EUAA collects and further processes personal data pursuant to [Regulation \(EU\) 2018/1725](#)<sup>1</sup> (hereinafter ‘the EUDPR’).

This Data Protection Notice explains *inter alia* the reasons for the processing of your personal data, the way we collect, handle and ensure protection of your personal data and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, as well as of the Data Protection Officer (DPO) and the European Data Protection Supervisor (EDPS) to which you may have recourse as well to exercise the said rights.

#### 2. Why and how do we process your personal data?

Your personal data are processed when you visit the EUAA’s Database on International Protection in Europe (‘DIP’), which includes a public interface and a restricted interface for EUAA personnel and EU+<sup>2</sup> officials.

We process your personal data as follows: during browsing, as long as you have accepted the cookies, we collect usage analytics (e.g. pages accessed, page views per session, country of access, downloads) For the restricted area we process account details and collect usage analytics.

#### 3. On what legal ground(s) do we process your personal data?

We process your personal data on the basis of Articles 5, 6(2) and Article 69 of [Regulation \(EU\) 2021/2303](#)<sup>3</sup> (hereinafter ‘the EUAA Regulation’), because processing is necessary for the EUAA to gather, analyse and disseminate information on the situation of asylum.

Consequently, the processing operation is lawful under Article 5(1) point (a) of the EUDPR given that it is “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested” in the EUAA. When accessing the restricted part of the website, to the extent that processing of personal data is based on consent obtained by users, such processing is lawful also under point (d) of Article 5(1) of the EUDPR.

#### 4. Which personal data do we collect and further process?

---

<sup>1</sup>. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39-98.

<sup>2</sup> EU countries plus Norway, Switzerland and Iceland

<sup>3</sup>. Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010, OJ L 468, 30.12.2021, p. 1-54.





The following (categories of) personal data may be processed:

- For users of the public interface: pages accessed; page views; country of access; downloads;
- For registered users: name, surname, institutional email, working position, institution, country of access;

#### **5. How long do we keep your personal data?**

In general, personal data are stored only for as long as necessary to achieve the purposes of the operation of the DIP. Data processed for analytics will be first anonymised and then retained for a period of time that allows to assess the usage and performance of the database over time.

Personal user data required to access the restricted parts of the database will be erased after the user requests termination of the user account. Personal user data will only be retained insofar as the data subject has an active account to access the restricted parts of the database.

#### **6. How do we protect and safeguard your personal data?**

In order to protect your personal data, we have put a number of technical and organisational measures in place as required under Article 33 of the EUDPR. Technical measures include:

- Encryption of data at rest on EUAA-managed on-premises infrastructure and cloud environments;
- Secure storage of backups in encrypted format, with network filtering and monitoring to detect threats;
- Role-based access controls for administrative actions on systems and services.

Organisational measures include:

- Access to backups and systems limited to authorised ICT staff and contractors only;
- Continuous review and update of access rights and logging of administrative actions.

#### **7. Who has access to your personal data and to whom are they disclosed?**

The following (categories of) recipients have access to your personal data:

- Personnel of the Information and Communications Technology Unit ('ICTU') maintaining the website on a strict need-to-know basis;
- Staff of the Situational Awareness Unit ('SAU') on a strict need-to-know basis.

#### **8. Do we transfer any of your personal data to third countries or international organisations (outside the EU/EEA)?**

No

#### **9. Does this processing involve automated decision-making, including profiling?**

No

**10. What are your rights and how can you exercise them?**

According to the EUDPR, you are entitled to access your personal data and to rectify them in case the data are inaccurate or incomplete. If your personal data are no longer needed by the EUAA or if the processing operation is unlawful, you have the right to erase your data. Under certain circumstances, such as if you contest the accuracy of the processed data or if you are not sure if your data are lawfully processed, you may ask the Data Controller to restrict the data processing. You may also object, on compelling legitimate grounds, to the processing of data relating to you. Additionally, you have the right to data portability which allows you to obtain the data that the Data Controller holds on you and to transfer it from one Data Controller to another. Where relevant and technically feasible, the EUAA will do this work for you.

Should you have any queries/questions concerning the processing of your personal data or should you wish to exercise your rights, please contact the Data Controller, i.e. the Head of the Situational Awareness Unit, by sending an e-mail to [ids@euaa.europa.eu](mailto:ids@euaa.europa.eu).

You may always submit queries, remarks or complaints relating to the processing of your personal data to the Data Protection Officer (DPO) of the EUAA using the following e-mail address: [dpo@euaa.europa.eu](mailto:dpo@euaa.europa.eu).

In case of conflict, complaints can be addressed to the European Data Protection Supervisor (EDPS) using the following e-mail address: [supervision@edps.europa.eu](mailto:supervision@edps.europa.eu).

*Endorsed: September 2025*