DATA PROTECTION NOTICE
EUAA Early warning and Preparedness System (EPS) Networks

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[1] (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 for the purpose of managing the EUAA EPS-Statistics Network and the EPS-Analysis and Research Network in EU Member States.

More specifically, information, including contact details, about officials in the Member States that will serve as National Contact Points (NCPs) for the EUAA EPS Networks is collected through a table in an excel file that is maintained by the Data Analytics and Reporting Sector (DARS) and the Strategic Analysis and Research Sector (SARS) under the Situational Awareness Unit (SAU) within the Asylum Knowledge Centre (C3) of the Agency on the restricted Member Area of the EUAA website entitled 'EPS Networks Area'. This restricted Member Area is only accessible to persons who have been nominated to have access by their Member State authority (i.e., designated contact point(s)).

The NCPs are the interface between the Member States and the EUAA EPS-Statistics and EPS-Analysis and Research Networks. Each Member State decides itself if it wishes to appoint one or several NCPs for each of the EUAA EPS Networks.

The Member States are also invited to indicate who shall be granted access to:

- the Asylum Data Exchange and Processing Tool (ADEPT)
- the dedicated EPS BI workspaces
- the EPS Query Portal
- the 'EPS Networks Area' restricted Member Area of the EUAA website
- the 'Analytical Area' restricted Member Area of the EUAA website

The table in the excel file mentioned above is divided into tabs where each Member State stores the information about their contact points. The said table also includes a number of tabs under which automated functions generate 'sectoral send lists' with recipients in all Member States in the respective categories based on the data entered in the Member State specific tabs. The 'sectoral send lists' are

[1] 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.

created by adding the contact details of all the nominated contact points from the different Member States. For instance, one of the lists contains all the nominated NCPs for the EPS-Statistics Network from the different Member States whilst another one contains a list of all persons nominated for the EPS-Analysis and Research Network. This will allow the EUAA to better direct its communication to the correct NCPs for a specific task.

The data contained in the table in the excel file are updated regularly by NCPs in each Member State. This table is stored on the Agency's internal document management system (ERDMS) and made available on the EUAA EPS Network Area with restricted access. Through the EPS Network Area, designated contact point(s) of the Member States can themselves, at any point, update the relevant contact information for their Member State's nominated contact points. Member States will be reminded twice per year to validate/update the information provided in the table in the excel file. Member States are also encouraged to provide information, upon their own initiative, on any changes in the contact points for the EUAA EPS Networks when such changes occur.

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

We process your personal data on the basis of Article 1(2) of Regulation (EU) 2021/2303[2] (hereinafter 'the EUAA Regulation') which reads as follows: "*The Agency shall contribute to ensuring the efficient and uniform application of Union law on asylum in the Member States in a manner that fully respects fundamental rights. The Agency shall facilitate and support the activities of the Member States in the implementation of the Common European Asylum System (CEAS), including by enabling convergence in the assessment of applications for international protection across the Union and by coordinating and strengthening practical cooperation and information exchange*".

Whereas the Agency's duty to cooperate in good faith and exchange all information in a timely and accurate manner with the national authorities responsible for asylum and immigration and other relevant services is set out in Article 4(4) of the EUAA Regulation which reads as follows: "*The Agency shall organise, promote and coordinate activities enabling the exchange of information among Member States, including through the establishment of networks, as appropriate* ".

Consequently, the processing operation is lawful under Article 5(1) point (a) of the EUDPR given that it is necessary for the performance of the tasks that the Agency has been vested with by virtue of its mandate.

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

The following (categories of) your personal data may be processed under the excel file tab dedicated to the relevant Member State:

- Name
- Surname
- Title
- Work e-mail address
- Work phone number

5. How long do we keep your personal data?

[2] 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.

Your personal data are accessible through the EUAA EPS Network Area as described above and are stored in the internal document management system of the Agency (ERDMS). Once data are deleted from the excel file table, in the event that the data subject concerned is no longer a designated or nominated contact point in respect of any of the categories identified in point 4 above, while the relevant data will no longer be visible in the said table, they still may remain stored on ERDMS, for a maximum duration of 10 years or until such time as the excel file is deleted and/or replaced, for security and backup purposes.

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

All personal data in electronic format (e-mails, documents, etc.) are stored on the servers of the EUAA. In order to protect your personal data, the EUAA has put in place a number of technical and organisational measures as required under Article 33 of the EUDPR. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

For website security purposes and to ensure that the EUAA EPS Network Area remains available to all users, network traffic is monitored to identify unauthorized attempts to exploit or change information on this website or otherwise cause damage or conduct criminal activity. Anyone using this website is advised that if such monitoring reveals evidence of possible abuse or criminal activity, results of such activity might be provided to the appropriate authorities in line with the applicable rules.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, the following security measures are applied:

1. The pseudonymisation and encryption of the data;
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
5. Personal data will solely be processed by authorised personnel who are:
    a. granted access to the personal data on a need-to-know basis;
    b. familiar with the obligations stemming from the applicable data protection rules;
    c. regularly trained in the care, protection and handling of personal data;
    d. authorised to process the personal data; and
    e. subject to a duty of confidentiality (either as a statutory or contractual obligation);
6. Additional particular security controls: The Information and Communications Technology Unit (ICTU) of the EUAA has implemented and maintains the following security controls for user data, consistent with industry best practices, including:
    a. Controls, Policies & Procedures: Appropriate technical and administrative controls, and organisational policies and procedures;
    b. Named person in the role as a dedicated Information Security Officer (ISO) with focus on security in all areas of the EUAA business;
    c. Logging: System and application logging where technically possible, whereas the EUAA ICTU retains logs and verifies such logs periodically for completeness;
    d. Malicious code and/or software: Malware prevention software (e.g. antivirus) is implemented on the technical infrastructure where applicable;
    e. Traffic inspection: Vulnerability exploit inspection is implemented on the technical infrastructure where applicable.

7. System Security: System and IT security controls applied by the EUAA ICTU follows industry best practices, including:
    a. A high-level infrastructure diagram, which can be provided upon request:
    b. A mix of industry standard software firewalls to dynamically limit external and internal traffic between our services;
    c. A program for evaluating security patches and implementing patches using a formal change process within defined time limits;
    d. Ad-hoc penetration testing by an independent third party, with a detailed written report issued by such third party and provided upon request;
    e. Documentation of identified vulnerabilities ranked based on risk severity and corrective action according to such rank;
    f. Password policy controls are implemented to protect data, including complexity requirements and multi factor authentication where available.

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:

- EUAA personnel within DARS and SARS;
- Other EUAA personnel, only on a need-to-know basis, including ICTU personnel for security-related purposes;
- Designated contact point(s) authorised by the respective Member State authorities to access the EUAA EPS Network Area.

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

This processing activity does not entail any transfers of personal data to third countries or international organisations (outside the EU/EEA).

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

This processing activity does not involve automated decision-making, including profiling. The only automation that takes place is the collating in the excel file table of the information provided which is used to generate 'sectoral send lists' to facilitate communication with the nominated contact points on specific issues.

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 them from one Data Controller to another. Where relevant and technically feasible, the EUAA will do this work for you.

If you wish to exercise your rights, please contact the Data Controller, i.e. the Head of Data Analytics and Reporting Sector (DARS), by sending an e-mail to data-hub@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 by using the following e-mail address: 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: edps@edps.europa.eu.