



DATA PROTECTION NOTICE

EUAA MedCOI Portal

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 notice explains the reasons for the processing of your personal data in the context of the EUAA Medical Country of Origin Information (MedCOI) Portal, the way EUAA collects, handles and ensures the protection of your personal data, how that information is used 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).

2. How and why do we process your personal data?

The MedCOI portal consists of two different sections: one public and the other restricted as defined by the [MedCOI Database Access Policy](#)². Your personal data is processed for the purpose of giving you access to the restricted section of the MedCOI Portal.

You have access to the restricted section of the Portal if you belong to one of the following categories:

- MedCOI users, i.e. persons who are in need of medical COI and who have access to the MedCOI website and database; these are duly designated and trained employees of the national administrations responsible for asylum and immigration in the EU+ countries or any other body mandated by an EU+ country to carry out research on information contained in the database (internal users);
- MedCOI service providers, i.e. information providers which have been contracted for the purpose of providing information on general or case-specific availability/accessibility of medical treatments/medicines in countries of origin, consisting in local MedCOI experts (e.g. local doctors and other experts such as pharmacists) and International SOS, which is an international medical assistance company, but also medical officers who perform the quality

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.

² Art 1. Decision No 91 of the Management Board of the European Asylum Support Office of 7 October 2021 on the MedCOI Database Access Policy. Ref. number: EASO/MB/2021/184.





check of outgoing MedCOI requests and of incoming MedCOI responses as outsourced task carried out by an independent organisation for medical advice;

- MedCOI administrators, i.e. EUAA personnel (statutory staff, temporary agency workers and Seconded National Experts) processing information contained in the database.

Contact details of users having been assigned certain specific roles, such as MedCOI National Contact Points³ (MedCOI NCPs), members of the MedCOI Strategic Network and of the MedCOI Advisory Committee⁴, are provided in the restricted section of the MedCOI Portal to promote transparency amongst MedCOI users from EU+ Countries.

In addition, we process your personal data for the purposes set out below:

- Creation and handling of MedCOI Portal accounts (set-up of different access profiles), including authentication and/or updating of user credentials, assignment of user permissions and enabling or disabling different levels of access rights, troubleshooting issues with user access rights and ICT-security related issues and monitoring analytics related to usage of the MedCOI portal;
- Participation in MedCOI training activities, including activities related to internal and external quality assurance of the MedCOI Portal (for example satisfaction surveys, overall audit or policy and case law research related to MedCOI);
- Exchange of relevant information and communication with MedCOI users/service providers (via the Portal or by e-mail);
- Participation in MedCOI meetings and publication of meeting summaries through the MedCOI Portal (for example MedCOI Strategic Network meetings, etc.).

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

We process your personal data on the basis of points (e), (f), (g) of Article 2(1) of [Regulation \(EU\) 2021/2303](#)⁵ (hereinafter “the EUAA Regulation”) pursuant to which the EUAA’s mandate covers, among others, the following tasks:

³. MedCOI NCPs are employees of government agencies in EU+ countries directly involved in the use of MedCOI information. They are either using directly the EASO MedCOI Portal or managing a department whose employees are direct users of the said portal. MedCOI NCPs essentially act as the liaison between the EUAA MedCOI Sector and the respective national authorities using the MedCOI service. Only one NCP is nominated by an EU+ country, together with a back-up NCP in case of absence of the nominated person.

⁴. The MedCOI Strategic Network and the MedCOI Advisory Committee are both MedCOI advisory bodies, forming part of the two-tier advisory system introduced by the Agency with the aim of supporting and reaching out to all EU+ countries. The MedCOI Strategic Network (Strat-Net) is an annual general meeting of representatives of EU+ countries interested in EUAA MedCOI, whereas the MedCOI Advisory Committee is a more restricted advisory body composed of EU+ countries representatives with a close connection to the MedCOI service and its day-to-day working.

⁵. 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.



- draw up and regularly update reports and other documents (e.g. MedCOI individual requests) providing information on the situation in relevant third countries, including countries of origin, at EU level;
- set up and coordinate European networks on third-country information;
- organise activities and coordinate efforts among Member States to develop common analysis on the situation in countries of origin.

More specifically, by virtue of point (h) of Article 8(4) of the EUAA Regulation, the Agency shall provide training covering *inter alia* the use of expert medical and legal reports in the procedure for international protection, whereas Article 9(1) and 9(2) point (b) of the said Regulation read, in this respect, as follows:

“1. The Agency shall be a centre for gathering relevant, reliable, objective, accurate and up-to date information on relevant third countries in a transparent and impartial manner, making use of relevant information, including child-specific and gender-specific information, and targeted information on persons belonging to vulnerable and minority groups.

2. The Agency shall, in particular:

[...]

(b) manage and further develop a web portal for gathering and sharing information on relevant third countries, which shall include a public section for general users and a restricted section for users who are employees of the national authorities responsible for asylum and immigration or any other body mandated by a Member State to carry out research on third-country information”.

In this respect, reference is also made to the Decision No 91 of the Management Board of the Agency of 7 October 2021 on the MedCOI Database Access Policy, which defines the overall modalities for regulating access to the restricted and public sections of the MedCOI Database, and the documents therein, in line with the applicable legal framework.

It follows from the above that processing of your personal data is necessary for providing you with access to the MedCOI Portal and for developing associated internal and external quality assurance activities such as validations, audits and peer reviews.

Consequently, the processing of your personal data 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. To the extent that processing of personal data is based on consent obtained by users of the MedCOI Portal, where this is deemed appropriate, 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?



Personal data collected and further processed may relate to the following categories of individuals:

- Employees of the national administrations responsible for asylum and immigration in the EU+ countries or any other body mandated by an EU+ country to carry out research on information contained in the database or nominated as MedCOI NCPs, MedCOI Advisory Committee members or MedCOI Strategic Network members;
- MedCOI service providers;
- EUAA personnel acting as MedCOI administrators (EUAA contract and temporary staff, temporary agency workers and Seconded National Experts).

The following (categories of) personal data are collected and processed:

- Name and surname;
- User credentials (username);
- E-mail addresses;
- When applicable, function, organisation and country of residence or country(-ies) for which the services are provided.

5. How long do we keep your personal data?

Personal data related to MedCOI Portal accounts is retained for as long as the user has access to the Portal or until the Platform ceases to operate. Moreover, personal data of requesting persons is retained for as long as such data is needed in the system to maintain relevant individual requests active in the database, and in any case not longer than ten (10) years.

Personal data is kept for a period of five (5) years when linked to reimbursement of participants in MedCOI meetings and MedCOI events.

In particular, the personal data (names, surnames, email addresses and countries of residence) of members of MedCOI Advisory Bodies and MedCOI NCPs are published in the restricted section of the MedCOI Portal. Periodic review of this data takes place (at least annually) and data of persons who are no longer active under the above-mentioned roles is deleted from the MedCOI Portal. The composition of the MedCOI Advisory Committee is reviewed every three years and therefore personal data of the members of this body is consequently updated and, when necessary, deleted.

6. Who has access to your personal data and to whom is it disclosed?

The data collected by the EUAA in the MedCOI Portal is shared with the EUAA personnel responsible for the day-to-day operation and maintenance of the MedCOI Portal and management of the system, including the EUAA's Centre of Asylum Knowledge (C3), the MedCOI Sector, the ICT Unit and the relevant MedCOI national focal point/s (MedCOI NCPs).



Your personal data is also shared with the International Centre for Migration Policy Development (ICMPD) in the context of external quality assurance activities and its sub-processor SoSci Survey GmbH which provides services in relation to online surveys. You may find relevant information about [ICMPD's privacy policy](#) on its website. You may also consult the [General Terms and Conditions](#) of Sosci Survey and find more information about its Privacy Policy [here](#) and [here](#).

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

This processing activity may entail transfer of personal data to an international organisation, i.e. the International Centre for Migration Policy Development (ICMPD), in the context of external quality assurance activities (including MedCOI satisfaction surveys).

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

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

For Portal security purposes network traffic is monitored to identify unauthorised attempts to exploit or change information on this website or otherwise cause damage or conduct criminal activity. Anyone using this Portal 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:

- The pseudonymisation and encryption of the data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- Personal data will solely be processed by authorised personnel who are:
 - granted access to the personal data on a need-to-know basis;
 - familiar with the obligations stemming from the applicable data protection rules;
 - regularly trained in the care, protection and handling of personal data;
 - authorised to process the personal data; and
 - subject to a duty of confidentiality (either as a statutory or contractual obligation);



- Additional particular security controls: The EUAA ICT has implemented and maintains the following security controls for user data, consistent with global cloud service provider industry best practices, including:
 - Controls, Policies & Procedures: Appropriate technical and administrative controls, and organisational policies and procedures;
 - Named person in the role as a dedicated Information Security Officer (ISO) with focus on security in all areas of the EUAA business;
 - Logging: System and application logging where technically possible, whereas EUAA ICT retains logs for a maximum six (6) months and verifies such logs periodically for completeness;
 - Malicious code and/or software: Malware prevention software (e.g. antivirus) is implemented on the technical infrastructure where applicable;
 - Traffic inspection: Vulnerability exploit inspection is implemented on the technical infrastructure where applicable.
- System Security: System and IT security controls at EUAA ICT follows industry best practices, including:
 - A high-level infrastructure diagram, which can be provided upon request;
 - A mix of industry standard cloud and software firewalls to dynamically limit external and internal traffic between our services;
 - Ad-hoc penetration testing by an independent third party, with a detailed written report issued by such third party and provided upon request;
 - Documentation of identified vulnerabilities ranked based on risk severity and corrective action according to such rank;
 - Password policy controls are implemented to protect data, including complexity requirements and multi-factor authentication where available.

Moreover, given that certain processing of personal data in the context of the EUAA MedCOI Portal may entail transfers of such data to ICMPD, which is an international organisation as mentioned above, appropriate safeguards have been provided as required under Article 48(1) and (2) point (a) of the EUDPR by means of a legally binding and enforceable instrument.

More specifically, a Framework Contract (FWC) for services with reference number EASO/2021/858⁶ has been concluded between the Agency and ICMPD (contractor) which includes, among others, detailed clauses on the processing of personal data by ICMPD⁷. On top of this FWC, ICMPD receives documented instructions from the Data Controller concerning the processing of personal data, in particular with regard to the purposes of the processing, the categories of personal data that may be

⁶. Consisting in 3 Lots which concern MedCOI external quality audits/verifications (Lot 1), MedCOI satisfaction surveys and overall MedCOI services' quality review (Lot 2) and MedCOI policy research/state practices and case-law analysis (Lot 3).

⁷. Clauses I.9.2 and II.9.2.



processed, the applicable retention periods and the recipients of the data, which it then has to pass on to any sub-contractors used in the processing of personal data by ICMPD (e.g. SoSci Survey GmbH).

In addition to the above, a Data Processing Agreement (DPA) has been signed between ICMPD and its sub-processor, i.e. SoSci Survey GmbH, in relation to services provided by the latter concerning online surveys.

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

This processing activity does not involve automated decision-making, including profiling.

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 it in case the data is inaccurate or incomplete. If your personal data is 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 is 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, under certain circumstances, 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.

If you wish to exercise your rights, please contact the Data Controller, i.e. the Head of the MedCOI Sector of the EUAA using the following e-mail address: MedCOI@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.