



PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data

1. Introduction

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereafter, 'eu-LISA') is committed to protect your personal data and to respect your privacy. eu-LISA collects and further processes personal data pursuant to [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 (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data

The information in relation to processing operation "COVID 19 - Manual contact tracing" undertaken by the Security Unit is presented below.

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

As part of the response measures adopted by the Agency in an attempt to prevent and control the spread of the coronavirus (COVID-19) within the working environment, a specific process has been adopted to determine contact with low-risk exposure and contact with high-risk exposure (close contacts).

The Security Unit collects and uses your personal information to allow eu-LISA personnel to report contacts with COVID-19 infected persons, to report on positivity, as well as contacts colleagues with whom infected staff member was in contact with during incubation period, in order to break the chain of contamination and reduce the risk of infection in the Agency's premises. This processing enables eu-LISA to provide a safe working environment for its staff according to the applicable legal and statutory obligations, implement policies to promote staff health and wellbeing and provide adequate follow-up towards suspect or confirmed cases.

Your personal data will not be used for an automated decision-making including profiling.

Your personal data processed may be reused for the purpose of procedures before the EU Courts, national courts, or the European Court of Auditors.

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

We process your personal data, because:

(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body:

- Article 1 (e) of the Staff Regulations of officials according to which "Officials in active employment shall be accorded working conditions complying with appropriate

PUBLIC

health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties".

- Regulation (EU) 2018/1726, in particular art.2 "*the agency shall ensure [...] continuous and uninterrupted service*", that requires the agency to implement the relevant measures to ensure availability of staff during the COVID-19 outbreak.
- Decision of the Management Board on Security in eu-LISA 133-REV3 adopted on 27.07.2017, in particular art.17 that enables the implementation of *urgent measures* under exceptional situations (including threat to the interest of eu-LISA vital for the Agency's management and functioning).
- Enabling access to the agency sites in Tallinn, Brussels, Strasbourg and Austria in line with art.2 of Regulation (EU) 2018/1726 eu-LISA Health and Safety Policy 192-2017 of 18.12.2017, in particular point 3.2.5. that requires the agency to "develop and implement separate, more detailed information, policies or procedures on specific risks and HS [Health and Safety] issues" where deemed based on the risk assessment.

(b) processing is necessary for compliance with a legal obligation to which the controller is subject:

- Article 19 (1), letter z of Regulation 2018/1726 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA): "*z) adopt the necessary security measures, including a security plan and a business continuity and disaster recovery plan taking into account the possible recommendations of the security experts present in the Advisory Groups;*".
- Decision of the Management Board on Security in eu-LISA 133-REV3 adopted on 27.07.2017, in particular art.17 that enables the implementation of urgent measures under exceptional situations (including threat to the interest of eu-LISA vital for the Agency's management and functioning).

We process special categories of personal data indicated in Section 4 below, because:

(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

The specific regulations on which the processing is based include:

- Article 1 (e) of the Staff Regulations of officials according to which "Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties"; and art. 59 (5).
- Setting up the necessary processes to allow the agency personnel to receive the required medical certificate for entering AT and the agency back-up site as per 80. Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz über Maßnahmen bei der Einreise aus SARS-CoV-2 Risikogebieten (80th Ordinance of the Federal Minister for Social Affairs, Health, Care

and Consumer Protection on measures for entry from SARS-CoV-2 risk areas).

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

In order to carry out this processing operation the Security Unit collects the following categories of personal data:

- Name, contact details and affiliation (e.g. address, first name, surname, e-mail, phone number, citizenship) – including non-staff persons.
- Travel details related to risk areas.
- Special categories of personal data, such as health data can be also processed. We're referring to: health status related to COVID-19; time of onset on COVID-19 symptoms or, if asymptomatic, the date of the positive test (used to calculate the contact tracing period); list of close contacts with the staff or non-staff members concerned over a period to be determined on a case-by-case basis after appearance of the first symptoms; result of the test (when the need for testing has been confirmed and limited only to "confirmed COVID-19 positive test" and whether symptomatic or asymptomatic) – data used to the purpose of manual contact tracing as above-mentioned in Section 2.

The provision of personal data is mandatory in order to meet the legal requirements. If you do not provide your personal data, the possible consequences are eu-LISA not being able to protect your health or the health of other member of its staff.

5. How long do we keep your personal data?

The Security Unit only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing. Personal data is stored for maximum 28 days – 14 days to ensure the complete tracing of the contacts of the affected data subject and an additional period of 14 days after the complete tracing of the contacts of the affected data subject.

When determining the maximum retention periods, the Agency takes also into account possible legal recourses, legal, auditing, archiving and reporting obligations.

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

Access to your personal data is provided to eu-LISA staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Designated eu-LISA staff members will receive your personal data to the purpose above-mentioned on Section 2 of manual contact tracing – mainly line managers, COVID-19 Task Force members and relevant Delegated Officer).

Regarding "external recipients", personal data might be processed by "contact points" of the contracting companies whose employees might be affected and "competent authorities", here limited information to what is necessary to pursue a local contact tracing strategy (e.g. people who have been in the same meeting, who share offices etc.).

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

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

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to

PUBLIC

restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a).

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor.

8. Contact information:

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, the Security Unit, to: eulisa-security@eulisa.europa.eu.

- The Data Protection Officer of eu-LISA

You may contact the Data Protection Officer (dpo@eulisa.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.