Privacy Policy

EUROPEAN AGENCY
for Special Needs and Inclusive Education

PRIVACY POLICY

European Agency for Special Needs and Inclusive Education

CONTENTS

AGENCY PRIVACY POLICY

The European Agency for Special Needs and Inclusive Education (the Agency) is committed to protecting the privacy, confidentiality and security of your personal data.

As a data controller, the Agency is responsible for deciding how it holds and uses your personal data and for notifying you of the information contained in this Privacy Policy.

This Privacy Policy describes:

- what personal data about you the Agency collects and uses during and after your work relationship, and why and how it does so;
- with whom the Agency might share this data;
- how long the Agency keeps this data.

This is in accordance with the General Data Protection Regulation (GDPR). This Privacy Policy applies to all individuals working *with* and *for* the Agency. Individuals working *with* the Agency may include, but are not limited to, learners, families, experts and country representatives. Individuals working *for* the Agency may include, but are not limited to, those who are contracted by the Agency, such as Agency team members and consultants.

It is important that you read and understand this policy. If you have questions or do not fully understand this policy, please ask the Agency's Personal Data Protection Working Group (privacy@european-agency.org) for more information.

Personal data protection principles

The Agency complies with the GDPR. This means that personal data the Agency holds about you must be:

- used lawfully, fairly and transparently;
- collected only for valid purposes that the Agency has clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes the Agency has told you about and limited only to those purposes;
- accurate and kept up-to-date;
- kept only as long as necessary for the purposes the Agency has told you about;
- kept securely.

Your rights

The Agency will observe your legal rights regarding the personal data collected about you. These include your rights to:

- access your personal data;
- obtain information about how your personal data is stored;
- correct or have inaccurate personal data about you corrected;
- have your personal data securely removed or deleted when its retention is no longer necessary for the defined purposes;
- object to your personal data being processed;
- opt out of your personal data being shared with third parties;
- withdraw consent;
- request transfer of your personal data to another party.

You can exercise your rights by contacting privacy@european-agency.org if you wish to:

- review, verify, correct or request deletion of your personal data;
- object to the processing of your personal data;
- opt out of your personal data being shared with third parties;
- withdraw consent;
- make a complaint.

If you opt out of having your personal data shared with third-party providers or object to the Agency processing your personal data, it may affect the Agency's ability to perform its work relationship with you (such as paying you or providing a benefit) or prevent the Agency from complying with its legal obligations.

If you have questions or concerns about the processing of your data or wish to exercise your rights under applicable law, contact privacy@european-agency.org.

Your obligations

The Agency strives to maintain accurate, complete and up-to-date personal data (for example, private and/or work contact details). The Agency relies on you to inform it of changes to your personal data.

If, during your work relationship with or for the Agency, you come into possession of any personal data that is not strictly necessary for the performance of your tasks/services, you

must delete it immediately. In case of doubt, contact the Agency's Personal Data Protection Working Group (privacy@european-agency.org).

'Agency Data Protection Code of Practice'

The Agency strives to protect the data of everyone working for and with it. To do this, it commits itself to informing and educating those working for the Agency about data protection issues, and to assisting them where necessary. The 'Agency Data Protection Code of Practice' is an internal document stating the steps that everyone working for the Agency must take to ensure a high level of data protection. The Agency will handle unintended violation of the 'Agency Data Protection Code of Practice' on a case-by-case basis, with a focus on avoiding similar incidents in the future.

Types of personal data the Agency may hold

Depending on the circumstances of your work relationship/collaboration with the Agency, the latter may collect, store and use personal data about you from one or more of the following categories:

- Contact details (including full name, address, mobile numbers, email addresses – both private and work-related)
- Personal data (including date of birth, gender, marital status, nationality, ID numbers and accessibility/dietary needs)
- Salary information (including payroll records, tax information and benefits information)
- Bank account details (for example, for fee payments or travel reimbursement)
- Employment records (including start date, workplace, job titles, work history, working hours, training records, holidays/leave, absences, contract details)
- Recruitment information (including curriculum vitae, references)
- Performance information
- Disciplinary and grievance information
- Work-related photographs, videos and audio recordings
- Emergency contact details
- Criminal record.

In limited circumstances and only when required by law, the Agency may ask for your written consent to allow it to process 'special categories' of more sensitive personal data. This could be data about health issues. In this case, the Agency will give you full details of the information that it needs and why it needs it, so that you can carefully consider whether to give your consent.

Collecting your personal data

The Agency may collect your personal data in several different ways. This includes from you directly or from another source where your personal data is publicly available.

In case of recruitment, the Agency may also collect your personal data from an employment agency, employment business or from third parties, including your former employers (references).

Purposes of processing personal data

The Agency processes personal data for the following general purposes:

- to identify people working with and for the Agency;
- to communicate with people working with and for the Agency;
- to comply with human resources requirements (for example, recruitment, employment, performance management, learning and development, payroll administration, compensation and benefits);
- to comply with legal regulations, including compliance with government authority requests for information and tax compliance;
- to support the work relationship with the Agency;
- to comply with external/internal reporting and audit regulations.

The Agency may sometimes need to process personal data for a purpose not originally considered at the time the data was collected. In these cases, the Agency will notify you of this new use before processing your personal data.

Legal bases for processing personal data

The Agency relies on the following legal bases for processing your personal data under the GDPR:

- General personal data: Article 6 (1)
- Sensitive personal data: Article 9 (2)
- Criminal record: Article 10.

Sharing personal data with third parties

The Agency may have to share your personal data with third parties. The Agency requires third parties to respect the security of individuals' personal data and to treat it in accordance with the law.

The Agency may share your personal data with third parties where required by law (for example, auditors, tax authorities, etc.), where it is necessary to administer the work relationship with people working with or for the Agency or where the Agency has another legitimate interest in doing so.

Third parties include third-party service providers. The following activities are carried out by third-party service providers: payroll, benefits provision and administration, information technology (IT) services, travel services and recruitment services.

All the Agency's third-party service providers are contractually committed to take appropriate security measures to protect personal data in line with Agency policies. The Agency does not allow its third-party service providers to use personal data for their own purposes. The Agency only permits them to process personal data for specified purposes and in accordance with its instructions.

The Agency may also share your personal data with third parties, such as hotels, restaurants, etc., related to your participation in Agency activities (for example, meetings and events). The Agency will ask these third parties to document their GDPR compliance.

Securing personal data

The Agency is committed to protecting the personal data it collects about you against the risks of loss or unauthorised use or access. It has implemented reasonable and appropriate technical, physical and administrative controls to protect your personal data.

In general, access to personal data is restricted to people working for the Agency who need it for the purposes listed in this Privacy Policy or where otherwise required by law. This includes members of the Agency's management, Human Resources and Financial Departments. Limited access may be granted on a strict need-to-know basis to other people working for the Agency, such as to support your work with and for the Agency and your participation in Agency activities, meetings, etc.

The Agency may disclose personal data to protect the vital interests of people working with or for the Agency (such as in response to a security incident or to medical workers in the event of a life-threatening emergency), to protect the Agency's legitimate interests (such as IT and network security) or if the Agency judges the disclosure necessary to comply with applicable legal obligations.

The Agency has procedures in place to deal with any suspected data security breach. The Agency will notify you and any applicable regulator of a suspected breach where it is legally required to do so.

Personal data retention

The Agency will only retain your personal data for as long as necessary to fulfil the purposes for which it was collected. This includes to satisfy any legal, accounting or reporting requirements. To determine the appropriate retention period for personal data, the Agency considers:

- the amount, nature and sensitivity of the personal data;
- the potential risk of harm from unauthorised use or disclosure of personal data;
- the purposes for which personal data is processed and whether the Agency can achieve those purposes by other means;
- the applicable legal requirements.

For the duration of your work relationship with or for the Agency, your personal data will be processed in accordance with this Privacy Policy.

Once you are no longer working with or for the Agency and it is no longer necessary to retain your personal data, the Agency will securely destroy the data.

Revisions to the Agency Privacy Policy

The Agency reserves the right to update this Privacy Policy at any time. The Agency will not diminish your rights under this Privacy Policy or under applicable data protection laws in the jurisdictions in which the Agency operates. If the changes to the Privacy Policy are significant, the Agency will provide a more prominent notice when required to do so by applicable law. Please review this Privacy Policy from time to time to stay updated on any changes.

Definitions

Personal data

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 3 (1), Regulation (EU) 2018/1725).

Special categories of personal data

'Special categories' of personal data include sensitive data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sexual orientation (Article 9, GDPR).