European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2026-0009 European Job Days Mobile Application (EJD Mobile App)

1 PART 1: PUBLIC - RECORD (ARTICLE 31[1])

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2026-0009
Title of the processing operation	European Job Days Mobile Application (EJD Mobile App)
Controller entity	European Labour Authority, Operations Department, Information and EURES Unit, EURES Sector
Joint controllers	☒ N/A ☐ YES, fill in details below
Processor(s)	☐ N/A ☒ YES, fill in details below
Internal organisation(s)/entity(ies) Names and contact details	☒ N/A ☐ YES
External organisation(s)/entity(ies) Names and contact details	☐ N/A ☒ YES **WAAT Poland Sp. z o.o.** Telewizyjna 48 01-492 Warsaw Poland WAAT Poland Sp. z o.o. acts as an external processor supporting the operation, maintenance and technical development of the European Job Days platform and the EJD Mobile App. The European Labour Authority's contractors are bound by a specific contractual clause for any processing operations of personal data on behalf of the European Labour Authority, and by the confidentiality obligations deriving from the General Data Protection Regulation.
Data Protection Officer Name and contact details	Daniela QATAM BENETIN ELA Data Protection Officer Landererova 12, 811 09 Bratislava I Slovakia Email: data-protection@ela.europa.eu
Corporate Record	☐ Yes ☒ No
Language of the record	English

[1] *Pursuant to **article 31** of the new data protection regulation for EU institutions and bodies (**Regulation (EU) 2018/1725**) each controller and processor have to maintain a **record of processing activities** under its responsibility that contains at least the information listed under that article.*

1.2 PURPOSE AND DESCRIPTION OF THE PROCESSING

1.2.1 Purpose

The European Labour Authority, Information and EURES Unit, collects and processes personal data to support intra-EU labour mobility by facilitating cross-border matching between jobseekers and employers and enabling participation in virtual and on-site recruitment events within the EURES framework.

The purpose of the processing through the EJD Mobile App is to provide jobseekers with mobile access to selected services of the European Job Days platform. Personal data are processed to enable users to create and manage accounts, profiles and CVs, search and apply for vacancies, register for and participate in EJD events, communicate with employers and access EURES support services.

Personal data are also processed to authenticate users, ensure the security, maintenance and proper functioning of the application, resolve technical issues and produce authorised usage statistics.

1.2.2 Description

The EJD platform and Mobile App:

The EJD website is a platform for virtual (online) and on-site job fairs where employers can publish their company profiles and current job opportunities. Jobseekers can indicate their interest in specific job offers by making their user profile and CV visible to the employers they have selected. In virtual events, presentations can be streamed online, and jobseekers, employers and EURES staff can communicate with each other via live chats. Specific information regarding the processing and protection of data submitted in chats is provided in connection with the chat functionality.

The EJD Mobile App provides jobseekers with mobile access to selected services of the EJD platform and uses the same user-account and jobseeker database as the EJD website. Through the application, users can browse vacancies and events, create or log in to their EJD account, manage their profile and CV, apply for vacancies, participate in European Job Days events and contact EURES support services. Users may also browse vacancies and events and access publicly available information without creating an account.

Job vacancies displayed in the EJD Mobile Application are retrieved through the EURES Job Vacancy API. Vacancy records may contain personal data relating to employers or employer representatives, such as contact names, email addresses or telephone numbers. These data are not collected directly by ELA through the EJD Mobile Application but are provided through the EURES network by authorised data providers. EURES Members, Partners and other vacancy providers are responsible for ensuring that any personal data contained in vacancy records are published and shared in compliance with applicable data protection legislation and that any necessary permissions or consents have been obtained before the data are made available through EURES.

Account registration, profiles and applications:

Jobseekers and employers who register for a European Job Day event obtain a user account on the EJD website for that event.

Jobseekers can create their personal profile, specify their preferences, and upload and manage their CVs either through the EJD website or directly through the EJD Mobile App. They can apply directly for job vacancies and, where the relevant functionalities are available, schedule online or face-to-face interviews with employers and communicate with them through live chat.

Employers registered on the EJD website can access a jobseeker's CV and other profile information only where the jobseeker has expressed an interest in that employer or has applied for one of its vacancies.

EURES Advisers, as members of the EURES network, may access jobseekers' profiles and CVs where necessary to provide support and facilitate European Job Days events in the organising and co-organising countries. This access enables them to provide guidance, facilitate candidate-employer matching and present relevant profiles during events. Access is limited to authorised persons with a legitimate need to process the information within the EURES framework.

Event Organisers, who may also be EURES Advisers, may access personal data, including relevant CV information, where necessary to organise and manage a specific European Job Day event. This may include coordinating candidate–employer matches, interviews, chats and presentations. CV information is made available to Event Organisers only to the extent necessary for event organisation and facilitation. It may also be made available to authorised EURES members in the relevant countries and verified employers, subject to the access conditions described above.

In cases where an employer further processes personal data obtained through the EJD platform for its own recruitment purposes, the employer will be considered a separate controller and will be responsible for complying with Regulation (EU) 2016/679 (GDPR), including the obligation to provide the relevant information to data subjects under Articles 13 and 14 and, where applicable, to maintain records of processing activities under Article 30.

1.2.3 Processing for further purposes

☐ Archiving in the public interest
☐ Scientific or historical research purposes
☒ Statistical purposes

Safeguards in place to ensure data minimisation
☐ Pseudonymisation
☒ Any other, specify

Statistical and analytical processing is limited to the data necessary to monitor application usage and performance and improve the service. Statistical outputs are produced in aggregated form. Access to the underlying personal data is restricted to authorised persons on a need-to-know basis, and those data are retained in accordance with the applicable retention periods. Where consent is required for analytics, data are collected only after the user has provided that consent.

1.2.4 Modes of processing

1. ☒ Automated processing (Article 24)
   a. ☒ Computer/machine
      i. ☐ automated individual decision-making, including profiling
      ii. ☒ Online form/feedback
      iii. ☒ Any other, specify

Mobile application processing, user authentication, database operations, account and profile management, document upload and retrieval, vacancy and event browsing, application submission, usage analytics, diagnostic logging and crash monitoring.

The modes of processing include both automated and manual processing. Automated processing is used only to provide and operate the functionalities of the EJD platform and the EJD Mobile App.

Certain functionalities use information contained in a jobseeker's profile, CV and selected preferences to identify potentially relevant vacancies or facilitate matching with employers. Information such as education, skills, languages, work experience, sectors of interest and preferred occupations is compared with job requirements using predefined rules to generate a rule-based matching score indicating how closely the jobseeker's profile aligns with a given vacancy. This automated evaluation may constitute profiling.

The matching score supports also jobseekers in identifying potentially relevant vacancies, for example by highlighting or ordering job offers according to their compatibility with the jobseeker's profile. Employers may also see the score when reviewing an application. In both contexts, the score serves an informational purpose and does not, in itself, determine application or recruitment outcomes.

Therefore, the EJD platform and the EJD Mobile App do not take decisions based solely on automated processing, including profiling, that produce legal effects concerning users or similarly significantly affect them within the meaning of Article 24(1) of Regulation (EU) 2018/1725. Automated functionalities are used only to support the identification of potentially relevant opportunities or candidates. Any subsequent decisions remain the

responsibility of the employer and jobseeker and involve continuous human assessment, with the matching score provided for information only.

2. ☒ Manual processing
    a. ☐ Word documents
    b. ☐ Excel sheet
    c. ☒ Any other, specify

Manual processing includes the review and handling of relevant information by authorised ELA staff, authorised personnel of the external processor, EURES Advisers, Event Organisers and verified employers, within their respective roles and access rights. These activities may include providing support, facilitating events, reviewing applications, managing interactions and troubleshooting technical issues. Access is limited to the information necessary for each activity and is subject to the applicable access conditions and, where relevant, the jobseeker's actions and preferences. The Information and EURES Unit does not have access to jobseekers' profiles.

3. ☐ Any other mode, specify

Description

The EJD Mobile App is connected to the EJD backend infrastructure and uses the same jobseeker database as the EJD website.

1.2.5 Storage medium

1. ☐ Paper
2. ☒ Electronic
    a. ☒ Digital (MS documents (Word, excel, Powerpoint), Adobe pdf, Audiovisual/multimedia assets, Image files (.JPEG, .PNG, etc.))
    b. ☒ Databases
    c. ☒ Servers
    d. ☒ Cloud
3. ☒ External contractor premises
4. ☒ Others, specify

Locally stored application data and cache files on users' mobile devices, where necessary for the operation and performance of the application.

Description:

Personal data are stored electronically in the EJD backend infrastructure and the database shared between the EJD platform and the EJD Mobile Application. Account information, profiles, CVs, applications, event registrations and related records may be stored in databases and on servers operated by ELA or its authorised contractors.

Users may upload CVs and supporting documents from their mobile devices. Limited application data or cache files may also be stored locally on the user's device until deleted by the user, the application or the operating system.

Crash reports and diagnostic information are processed through Sentry. Usage analytics are processed using Matomo and aggregated statistics from the Android and iOS application stores.

1.2.6 Comments on the processing of the data

The EJD Mobile App provides mobile access to selected EJD platform services and shares the same jobseeker database as the EJD website. Existing EJD users may access their account, profile and CV through the application.

Users can browse European Job Days vacancies, EURES-flagged vacancies and European Job Days events, create or access an EJD account, manage their profile and CV, apply for vacancies, register for and participate in events, and contact EURES support services.

Users who are not logged in may browse publicly available vacancies, events and other public information without creating an account. They may also apply for selected EURES vacancies using their email client.

Personal data are processed according to the functionalities used, including to authenticate users, manage profiles, CVs and applications, and support communication and event participation.

Access to CVs and profile information is role-based. Verified employers may access a jobseeker's CV and profile information only where the jobseeker has indicated an interest in that employer or applied for one of its vacancies, subject to the applicable EJD access rules. EURES Advisers and Event Organisers may access relevant information where necessary for support and event facilitation.

The application also processes technical and diagnostic information necessary for security, maintenance, performance monitoring and troubleshooting. Matomo is used for usage analytics and Sentry for crash monitoring.

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	☒ Yes	Data subjects - Authorised ELA staff whose professional contact details, user identifiers or activity records are processed in connection with the administration, monitoring, security, support or oversight of the EJD Mobile Application.
2.External to organisation	☒ Yes	Data subjects -Jobseekers: Individuals who create an EJD account or access an existing account through the EJD Mobile App. -Other application users and enquirers: Individuals who browse publicly available information without logging in or submit enquiries to EURES support services, insofar as their personal data are processed. -EURES Advisers whose professional details are available through the service. -Event Organisers -Employers and their authorised representatives

1.3.2 Data categories/fields

Indicate the categories of data that will be processed
Description: The following categories of personal data may be processed, depending on the user's role and the functionalities used.

Account and identification data: First name, last name, username, authentication information, account identifiers, preferred language, nationality.

Contact data: Email address, telephone number, where collected, contact details included by the user in a profile or/and CV.

Jobseeker profile and professional data: Country of residence, age group, gender, level and field of education, employment status, language skills, professional skills, sector, occupation, employment preferences and other

information voluntarily included in the profile. Gender, age group, level of education and country of residence are collected for statistical purposes.

CV and supporting-document data: Uploaded CVs and their contents, supporting documents, and files or profile content selected or captured by the user through the device's file storage, photo gallery or camera.

Vacancy and application data: Vacancies viewed or selected, applications submitted, indications of interest in employers or vacancies, and information relating to interviews or other recruitment interactions, where the relevant functionality is used.

Event and communication data: Event registrations and participation information, enquiries submitted to EURES support services, chat or communication information, contact details exchanged through the applicable EJD functionality.

Employer and organisation data: First and last name of the representative, email address, telephone number, organisation name, description and type, country, sector, organisation logo, where it identifies or relates to an individual. Names, email addresses and telephone numbers of employers or employer representatives included in job vacancies displayed in the EJD Mobile App are obtained through the EURES Job Vacancy API from authorised data providers within the EURES network and are not collected directly from employers through the application.

EURES Adviser and Event Organiser data: First name, last name, username, email address, telephone number, country, professional role and organisation-related information.

Technical, device and application data: Device and application identifiers, application version, operating-system information, authentication information, application settings and user preferences, IP address, network connection information, security, diagnostic and error logs, crash reports, application performance information, and locally stored application data and cache files.

Usage and analytics data: Interactions with the application, sections visited, technical characteristics of the device, application performance metrics, Matomo analytics data and aggregated statistics from Android and iOS application stores, insofar as these constitute personal data.

Mobile-device permissions and access: Where enabled by the user: access to the camera, photo gallery and file storage for uploading documents or profile content, microphone access where audio functionality is available.

Where enabled by the user, camera and microphone access supports audio and video calls through ***Whereby.*** *Whereby may process live audio and video streams through its infrastructure to transmit the call, without storing them beyond the temporary processing necessary for transmission. Further information is available in* ***Whereby Privacy Policy.***

1.3.2.1 Special categories of personal data

Indicate if the processing operation concerns any 'special categories of data' which fall(s) under Article 10(1), which shall be probhibited unless any of the reasons under article 10(2) applies:

☐ **Yes , the processing concerns the following special category(ies):**

Data revealing

☐ racial or ethnic origin,
☐ political opinions,
☐ religious or philosophical beliefs,
☐ trade union membership,

Or/and,

☐ Genetic data, biometric data for the purpose of uniquely identifying a natural person,

☐ Data concerning health,

☐ Data concerning a natural person's sex life or sexual orientation.

☒ **N/A**

If applicable, indicate the reasons under article 10(2) allowing the processing of the special categories of data:

(a) ☐ The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, […].

(b) ☐ 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[…].

(c) ☐ Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

(d) ☐ Processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Union institution or body and with a political, philosophical, religious or trade-union aim […].

(e) ☐ Processing relates to personal data which are manifestly made public by the data subject.

(f) ☐ Processing is necessary for the establishment, exercise or defense of legal claims or whenever the Court of Justice of the European Union is acting in its judicial capacity.

(g) ☐ Processing is necessary for reasons of substantial public interest, […]

(h) ☐ Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services […]

(i) ☐ Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices […].

(j) ☐ Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes […].

Additional information
Users may upload free-text CVs and supporting documents. Such documents may incidentally contain special categories of personal data voluntarily included by the user, even though users are instructed not to include such data and the EJD Mobile App does not request or require them through its structured fields.

1.3.2.2 Data related to 'criminal convictions and offences'

The data being processed contain sensitive data which fall(s) under Article 11 'criminal convictions and offences'	**N/A** ☒ **Yes** ☐

1.4 RETENTION PERIOD

Indicate the administrative time limit(s) for keeping the personal data per data category, and if known, specify the start/end date, or describe the specific start/end moment of each time limit:

Data category	Retention period	*Optional*	
		Start date/moment	***End date/moment***
EJD account and associated data	For as long as the corresponding account remains active. These data are deleted after 5 consecutive years of inactivity, counted from the date of the last account activity, unless deleted earlier by the account holder	Date of the last account activity	Deletion by the user or expiry of 5 consecutive years of account inactivity
Locally cached application data	Until deleted by the user, application or operating system	Creation of the local cache or application data	Deletion by the user, application or operating system
Usage analytics associated with a user account	Until the user account is deleted or until the user opts out of analytics	Collection through use of the application	Deletion of the user account or withdrawal of consent to analytics
Crash reports, security, technical and diagnostic logs processed through Sentry	90 days	Creation of the log or crash report	Automatic deletion after 90 days

Description

Personal data are retained according to their category and purpose. Account, identification, profile, CV, vacancy-application and event-related data are retained while the account remains active and deleted after five consecutive years of inactivity. Usage analytics associated with an account are retained until the account is deleted or the user opts out of analytics or withdraws consent. Crash reports and security, technical and diagnostic logs processed through Sentry are automatically deleted 90 days after their creation. Locally cached application data remain on the device until deleted by the user, application or operating system.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. ☒ Within the EU organization	Recipients Authorised ELA staff responsible for the governance, administration, security, oversight and support of the processing operation, with access restricted according to the need-to-know principle.
2. ☒ Outside the EU organization	Recipients - EJD Mobile App users, including users without an account. - EURES Advisers and EURES Members involved in organising or co-organising events and providing support.

	- Event Organisers involved in managing and facilitating specific events. - Verified and accepted employers, subject to the user's indication of interest or application and the applicable EJD access rules. - Authorised personnel of the external contractor acting on behalf of ELA to operate, maintain and support the EJD platform and EJD Mobile App, with access limited to what is necessary for their tasks on a need-to-know basis.

Categories of the data recipients

1. ☒ A natural or legal person
2. ☒ Public authority
3. ☐ Agency
4. ☒ Any other third party, specify

Specify who has access to which parts of the data:

-**Authorised ELA staff** has only access to the contact details of the event organisers and aggregated data related to the event through a specific form.

- **EJD Mobile App users**, including those without an account, may access the professional contact details of EURES Advisers. They may also view names, email addresses and telephone numbers of employers or employer representatives where these are included in publicly available vacancies retrieved through the EURES Job Vacancy API and displayed in the application. Jobseekers and employers may request each other's contact details.

-EURES Advisers and EURES Members: EURES Advisers, as members of the EURES network, may access jobseekers' profiles and CVs where necessary to provide support and facilitate European Job Days events in the organising and co-organising countries. This access enables them to provide guidance, facilitate candidate–employer matching and present relevant profiles during events. Access is limited to authorised persons with a legitimate need to process the information within the EURES framework.
Information on jobseekers' CVs is made available, for display purposes, to EURES Members of the organising and co-organising countries.

-**Event Organisers:** Event Organisers, who may also be EURES Advisers, may access personal data, including relevant CV information, where necessary to organise and manage a specific European Job Day event. This may include coordinating candidate–employer matches, interviews, chats and presentations. CV information is made available to Event Organisers only to the extent necessary for event organisation and facilitation and may also be shared, where appropriate, with authorised EURES Members in the relevant countries and verified employers.

-Verified and accepted employers: Employers registered on the EJD website may access a jobseeker's CV and other profile information only where the jobseeker has expressed an interest in that employer or has applied for one of its vacancies.

-Authorised personnel of the external contractor: Access is granted solely for the performance of assigned operational, maintenance and support tasks and is restricted according to assigned roles and the need-to-know principle.

1.6 INTERNATIONAL DATA TRANSFERS

Transfer to third countries or international organisations of personal data	
1. Transfer outside of the EU or EEA ☐ N/A, transfers do not occur and are not planned to occur ☒ YES,	
Country(ies) to which the data is transferred:	**Switzerland**
2. Transfer to international organisation(s) ☒ N/A, transfers do not occur and are not planned to occur ☐ Yes, specify further details about the transfer below	
3. Legal base for the data transfer ☒ Transfer on the basis of the European Commission's **adequacy decision** *(Article 47*)	
4. Derogations for specific situations (Article 50.1 (a) –(g)) ☒ N /A ☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply (ies).	

Description

Personal data may be transferred to recipients in Switzerland in accordance with Article 47 of Regulation (EU) 2018/1725, on the basis of **Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland**. No transfers to international organisations are envisaged under this processing operation, and no derogations under Article 50 of Regulation (EU) 2018/1725 are relied upon.

1.7 INFORMATION TO DATA SUBJECTS ON THEIR RIGHTS

Rights of the data subjects
Article 17 – Right of access by the data subject
Article 18 – Right to rectification
Article 19 – Right to erasure (right to be forgotten)
Article 20 – Right to restriction of processing
Article 21 – Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 22 – Right to data portability
Article 23 – Right to object
Article 24 – Rights related to Automated individual decision-making, including profiling

1.7.1 Privacy statement

☒ The data subjects are informed about their rights and how to exercise them in the form of the privacy statement attached to this record.

Publication of the privacy statement

☒ Published on website

Web location:

- ELA internal website ☒ (URL: Sharepoint on Personal data protection)
- External website ☒(URL: **https://www.ela.europa.eu/en/privacy-policy)**

☒ Other form of publication, specify
The privacy statement is accessible within the EJD Mobile App.

☒ Guidance for Data subjects which explains how and where to consult the privacy statement is available and will be provided at the beginning of the processing operation**.**

Description:
The privacy statement is made accessible from the EJD Mobile Application.

Data subjects are informed through the EJD Mobile Application privacy statement. The notice explains the identity of the Controller, purposes and legal basis of the processing, categories of personal data, recipients, retention periods, international transfers, data-subject rights, withdrawal of consent, and the contact details of the Controller, ELA DPO and EDPS.
The privacy statement is made available before or at the time personal data are collected. It is accessible through the mobile application. Where a mobile-device permission is requested, the operating-system permission request is supplemented by appropriate information about why the access is needed.

1.8 SECURITY MEASURES

Short summary of overall Technical and Organizational Measures implemented to ensure Information Security:
Description:
All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Labour Authority or of its contractors.

ELA's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of ELA, in accordance with Regulation (EU) 2018/1725 and the applicable data protection obligations imposed on processors acting on behalf of Union institutions, bodies, offices and agencies.
In order to protect your personal data, ELA has put in place a number of technical and organisational measures in place. 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.

Communications between the EJD Mobile App and the EJD backend systems are protected through secure communication protocols. Appropriate technical and organisational measures are also implemented to protect authentication credentials, uploaded documents and other personal data processed through the application.