

VACANCY NOTICE - TEMPORARY STAFF 2(f)

Reference number: RCT-2025-00007

Identity and Access Management Services Engineer

Post (business title):		Identity and Access Management Services Engineer (1 post) (a reserve list to be created for 1 post to be filled)
Sector/Unit/Division:		IM/SIM/Digital Services Unit/Digital Operation Sector
Function group / Grade / Post title:		Temporary staff, AD6, 2(f), Identity and Access Management Services Engineer ¹
Grade bracket	for internal mobility ² :	AD5 - AD7
	for inter-agency mobility ³ :	AD5 - AD7
Location:		Warsaw, Poland
Starting date:		Third quarter 2025 (desired)
Level of Security Clearance:		Confidential UE/EU Confidential
Closing date for applications		<u>(MIDDAY) 8 July 2025 at 12:00 h⁴, Warsaw local time</u>

Table of Contents

1.	BACKGROUND	2
2.	THE SECURITY AND INFORMATION MANAGEMENT DIVISION and the DIGITAL SERVICES UNIT	2
3.	DUTIES AND RESPONSIBILITIES LINKED TO THE POSTS	3
4.	ELIGIBILITY CRITERIA	4
4.1.	General/common criteria	4
4.2.	External applicants	5
4.3.	Inter-agency applicants	5
4.4.	Internal applicants	5
5.	SELECTION CRITERIA	5
6.	Equal OPPORTUNITIES, DIVERSITY & INCLUSION	6
7.	SELECTION PROCEDURE	6
8.	APPOINTMENT AND CONDITIONS OF EMPLOYMENT	7
9.	PROTECTION OF PERSONAL DATA	8
10.	REVIEW AND COMPLAINT PROCEDURE	9
11.	APPLICATION PROCEDURE	9

¹ Type of post: Administrator.

² For existing EU temporary staff 2(f) applicants for whom Article 55 the Conditions of Employment of Other Servants of the European Union (CEOS) is applicable.

³ Engagement of an inter-agency applicant in grade higher than AD6 will be possible subject to availability of respective grades in the establishment plan at the moment of appointment.

⁴ Date of publication: 9 June 2025.

1. BACKGROUND

The European Border and Coast Guard Agency (Frontex) has been established under the European Border and Coast Guard Regulation⁵. The agency was created on the foundations of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (established under Council Regulation (EC) No 2007/2004), which has been coordinating operational activities at the EU external border since 2005.

Frontex is located in Warsaw, Poland, and is in the process of significantly increasing the size of its staff to 2,500 to meet its expanding tasks.

The new European Border and Coast Guard Regulation provides for the establishment of a European Border and Coast Guard Standing Corps, which will consist of up to 10,000 operational staff by 2027, and will be deployed along the external land, sea and air borders of the European Union and the Schengen Area.

With the establishment of the Standing Corps - the first European law enforcement uniformed corps - Frontex offers a unique, pioneering opportunity to form part of the EU's operational arm for European integrated border management. The establishment and operations of the Standing Corps gives rise to various novel legal challenges and risks. The selected candidate will have a chance to significantly contribute to the application of the EU law in this area by developing creative legal solutions in cooperation with internal and external partners.

The Agency's key tasks include:

- Operational and technical assistance to the EU member states at their external borders by coordinating joint border control operations including deployment of vessels, aircraft and other equipment and border and coast guards from EU countries;
- Coordination of border surveillance and law enforcement activities being part of maritime security in cooperation with national authorities and EU agencies such as Europol, EMSA and EFCA;
- Situation monitoring of EU's external borders and risk analysis of all aspects of border and coast guard management, including assessment of the EU Member States' border control authorities' ability to face migratory pressure and different challenges at their external borders;
- Assisting Member States in returning nationals of non-EU countries who do not have the right to remain on the territory of the EU;
- Development of training programmes for European border and coast guards;
- Monitoring new technological developments in the field of border control and acting as an interface between research institutions, industry and national border and coast guard authorities;
- Cooperation with EU and international organisations in the area of border and coast guard management, security, and prevention of cross-border crime (including terrorism);
- Assist non-EU countries in the context of technical and operational cooperation on border management including return of non-EU nationals, in the framework of the EU external relations policy.

In all its activities, Frontex enforces actions which are respecting fundamental rights as an overarching component of the European Integrated Border Management. Frontex and its staff are committed to the values of Professionalism, Respect, Cooperation, Accountability and Care.

For more information, please refer to our website under this [link](#).

2. THE SECURITY AND INFORMATION MANAGEMENT DIVISION AND THE DIGITAL SERVICES UNIT

Mission

The mission of the Security and Information Management Division is to provide horizontal business support in the area of digital and security. The Division is responsible for EUROSUR and business capabilities and provides project management capabilities in the Agency.

⁵ Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p.1).

Organisation

The Division is led by the Director of Security and Information Management Division who reports to the Deputy Executive Director for Administration and Information Management.

The Security and Information Management Division (SIM) is composed of the following entities:

- a) Digital Services Unit (DIG)
- b) Security Unit (SEC)
- c) Project Management Office (PROM)

The Digital Services Unit - organisation and main tasks and responsibilities

The Digital Service Unit (DIG) is led by the Head of Unit who reports to the Director of the Division.

The Digital Services Unit composes of the following sectors:

- a) Digital Projects Sector (DPS)
- b) Digital Operations Sector (DOS)
- c) Cyber Security Sector (CSS)
- d) EUROSUR Business Capabilities Sector (EUROSUR)

The main tasks and responsibilities of the Digital Services Unit are as follows:

- a) Acting as centre of expertise and support in the field of digitalisation, information and communication technologies;
- b) Coordinating the implementation of the Information Management Framework and ICT Strategy;
- c) Anticipating and defining the needs of the Agency in terms of capabilities pertaining to information superiority to foster European Union Integrated Border Management;
- d) Centralising the management of the Frontex ICT infrastructure, relevant investments, digital services/business applications, products delivery and cybersecurity management;
- e) Developing and implementing of EUROSUR business capabilities.

Digital Operations Sector - organizations and main tasks and responsibilities

The Digital Operations Sector (DOS) is led by the Head of Sector who reports to the Head of Digital Services Unit.

The main tasks and responsibilities of the Digital Operations Sector are as follows:

- a) Providing ICT support for all Frontex digital services, internal and external stakeholders;
- b) Maintaining the ICT disaster recovery plan;
- c) Managing capacity of maintained systems and deployment of new digital capabilities;
- d) Managing enterprise and solution architecture practice, without prejudice to the Agency-wide responsibility of the Project Management Office.

3. DUTIES AND RESPONSIBILITIES LINKED TO THE POSTS

Reporting to the Head of Digital Operation Sector, the Identity and Access Management Services Engineer will have the following duties:

Design and Implementation:

- Develop and deploy authentication solutions using Microsoft technologies in on-premises, hybrid and cloud environments;
- Design and implement identity governance and administration (IGA) solutions based on SailPoint technologies for cloud and on-premises infrastructures;
- Design, implement, and optimise Joiner-Mover-Leaver (JML) processes to ensure automated and secure organisational identity lifecycle management;
- Contribute to the implementation of Zero Trust Architecture (ZTA) by reinforcing the identity pillar, ensuring that authentication and access controls are based on strong identity verification, least privilege access, and continuous monitoring.

Integration and Infrastructure Management:

- Ensure seamless integration of Active Directory Domain Services (AD DS), Entra ID, Active Directory Federation Services (AD FS), and SailPoint IGA with business applications, network services, IT security, messaging and collaboration tools, remote access, virtualisation, and cloud solutions (IaaS, PaaS, SaaS);
- Administer and monitor Microsoft Active Directory, AD FS and Entra ID;
- Manage and oversee the administration of SailPoint IGA solutions, ensuring efficient access provisioning, de-provisioning, and role-based access control (RBAC);
- Implement strong authentication mechanisms, such as multi-factor authentication (MFA), conditional access policies, in accordance with Zero Trust principles.

Identity Lifecycle, Governance and Zero Trust Security:

- Define and enhance JML processes based on organisational policies to automate user onboarding, role transitions, and access revocation;
- Ensure compliance with security policies, regulatory requirements, and Zero Trust Identity Security best practices;
- Collaborate with cybersecurity and security teams to implement continuous monitoring and risk-based identity validation to prevent unauthorised access;
- Support the adoption of identity protection mechanisms to minimise attack surfaces.

Operational Support and Documentation:

- Prepare technical documentation, standard operating procedures (SOPs), and guidelines for IAM operations;
- Implement changes in accordance with the Digital Services Unit's change management processes.

Leadership and Support:

- Assist the ICT Coordinator for Directory Services and Microsoft Databases in designing and maintaining IAM services and infrastructure;
- Support the ICT Coordinator for Directory Services and Microsoft Databases in planning, organising, and guiding the work of consultants;
- Contribute to administrative tasks, including procurement activities and contract execution;
- Act as a deputy for the ICT Coordinator for Directory Services and Microsoft Databases during their absence.

Additional Responsibilities:

- Perform other tasks as assigned by the Head of Frontex Digital Services Unit;

Due to the nature of the work the personnel also provide paid 24/7 on-call service outside normal working hours.

4. ELIGIBILITY CRITERIA

In order to be declared eligible, the applicant must:

4.1. General/common criteria⁶

1. Be a citizen of one of the Member States of the European Union or the Schengen Associated Countries and enjoy full rights as its citizen.
2. Have fulfilled any obligations imposed on him/her by the laws of the country of citizenship concerning military service.
3. Produce the appropriate character references as to his/her suitability for the performance of his/her duties⁷.
4. Be physically fit to perform his/her duties.
5. Produce evidence of thorough knowledge of one of the languages of the European Union and of satisfactory knowledge of another language of the European Union to the extent necessary for the performance of the duties (Common European Framework of Reference for Languages: B2 level).

⁶ Mandatory criteria for the engagement of temporary staff as laid down in Article 12(2) of the CEOS.

⁷ Prior to engagement, the selected applicant will be required to provide appropriate character references as to his/her suitability for the performance of duties (such as a criminal record certificate or equivalent certificate, not older than six months) as well as a compulsory declaration before engagement in Frontex and a declaration in relation to interests that might be considered prejudicial to his/her independence.

4.2. External applicants

Minimum qualifications (university diploma):

Possess a level of education which corresponds to **completed university studies** attested by a diploma when the normal period of university education is **three years or more**.

Only qualifications that have been awarded in EU Member States or that are subject to the equivalence certificates issued by the authorities in EU Member States shall be taken into consideration.

Required professional experience

Possess (by the closing date for applications) at least **3 years** of proven full-time professional experience acquired after the diploma was awarded and (at the same time) after the condition(s) described in the criterion above are fulfilled⁸.

ANY GIVEN PERIOD OF STUDIES OR PROFESSIONAL EXPERIENCE MAY BE COUNTED ONLY ONCE. In order to be calculated as eligible, years of studies or professional experience to be taken into account shall not overlap with other periods of studies or professional experience (e.g. if the applicant had a full-time job and did freelance consultancy work in the evenings and weekends, the days spent on the latter will not be added to the period). In case of part-time work, the professional experience will be calculated pro-rata in line with the workload stated by the applicant. Compulsory military service or equivalent civilian service accomplished before or after achieving the minimum qualification shall be taken into consideration as professional experience subject to provided evidence.

4.3. Inter-agency applicants

1. On the closing date for applications and on the day of filling the vacant post, be engaged as temporary staff under Article 2(f) of CEOS within their agency in a grade and function group corresponding to the published grade bracket.
2. Have at least two years' service within their agency before moving⁹.
3. Have successfully completed the probationary period as provided for in Article 14 of the CEOS in the relevant function group¹⁰.

4.4. Internal applicants

On the closing date for applications and on the day Be a member of temporary staff engaged under Article 2(f) of CEOS at Frontex in grade AD5 - AD7.

5. SELECTION CRITERIA

Suitability of applicants will be assessed against the following criteria in different steps of the selection procedure. Certain criteria will be assessed/scored only for shortlisted applicants during interviews (and or tests).

5.1. Professional qualifications, competences and experienced required:

1. At least 2 years of experience in designing, implementing, and managing IAM solutions using Microsoft and SailPoint technologies in on-premises and hybrid environments.
2. Strong knowledge of Joiner-Mover-Leaver (JML) processes and identity lifecycle management automation.
3. Experience implementing Zero Trust Architecture (ZTA), with a focus on the identity pillar, including multi-factor authentication (MFA), conditional access, and least privilege access controls.
4. Strong knowledge of role-based access control (RBAC), privileged access management (PAM), and identity federation.
5. Experience in IAM policy development, security governance, and compliance (e.g., GDPR, ISO 27001, NIST).

⁸ Professional experience will be taken into account after the award of the minimum qualification certifying the completion of the level of studies required. Only duly documented professional activity is taken into account.

⁹ Any decision derogating from that principle shall be taken jointly by the two agencies concerned, having regard to the interest of the service of both agencies.

¹⁰ Where, in exceptional circumstances, Frontex would engage a member of temporary staff engaged under Article 2(f) of CEOS who does not meet that condition, such member shall serve a full probationary period in Frontex, and the new contract will not be considered as a renewal of contract but an ex-novo contract.

5.2. Besides, the following attributes would be considered advantageous:

6. Possession of Microsoft Certified Identity and Access Administrator Associate certification.
7. Possession of SailPoint Certified Identity Now Professional certification.
8. Experience working in large-scale enterprise IAM deployments.
9. Proven experience in and/or good understanding of Microsoft 365 technologies.
10. Experience in IAM-related procurement, contract execution, and vendor management.

5.3. Personal qualities and competences

11. Excellent communication skills in English (at minimum B2 level), both orally and in writing to technical and non-technical audiences in a multicultural environment, and respect for fundamental rights.
12. Excellent time management, planning and organization skills, ability to make sound decisions, prioritize and work to deadlines under minimal supervision on multiple tasks.
13. Strong collaboration skills to work with security teams, HR, IT operations, and business stakeholders.

6. EQUAL OPPORTUNITIES, DIVERSITY & INCLUSION

Frontex applies an equal opportunities policy and, subject to the limitations imposed by law, accepts applications without distinction on grounds of age, race, colour, ethnic or social origin, genetic features, language, political, philosophical, religious or any other conviction, sex or sexual orientation and regardless of disabilities, marital status or family situation.

Frontex encourages and invites to apply professionals of different backgrounds and origins who want to play an active role in a dynamic team in a multicultural organisation that is contributing to increased European safety.

7. SELECTION PROCEDURE

The selection procedure includes the following steps:

- After registration, each application is checked in order to verify whether it meets the eligibility criteria;
- All the pre-eligible applications are evaluated by an appointed Selection Committee based on a combination of certain selection criteria defined in the vacancy notice (some criteria will be assessed/scored only for shortlisted applicants during interviews and/or tests; (in case of high number of applicants there might be an entry-level eliminatory written test). Certain selection criteria may be assessed/scored jointly, and some criteria may be assessed/scored in two or more steps of the selection procedure; advantageous criteria will only be assessed at the last stages of the procedure. Order of tests or assessments may be subject to changes aiming at ensuring efficient processing of high number of applications;
- Best-qualified applicants who obtain the highest number of points within the application evaluation and who are matching best the evaluated selection criteria will be shortlisted and invited for a competency test and an interview; the names of the members of the Selection Committee will be disclosed to the applicants invited for the test and interview. Only shortlisted candidates will be contacted;
- The test and interview will be conducted in English;
- During the interviews and tests, the Selection Committee will examine the profiles of shortlisted applicants and assess their relevance for the post in question. Certain selection criteria may be assessed/scored jointly, and some criteria may be assessed/scored in two or more steps of the selection procedure. At least one part of the qualifying written test will be assessed based on anonymized answers;
- As a result of the interview and test, the Selection Committee will recommend the most suitable applicant(s) for the post in question to the Appointing Authority of Frontex. An additional interview with the Appointing Authority and/or another relevant manager may be arranged before the Appointing Authority takes the final decision;
- Suitable applicants will be proposed for a reserve list, which may also be used to fill similar vacant posts depending on the needs of Frontex. This reserve list will be valid for at least 1 year (the validity period may be extended). Applicants should note that the placement on the reserve list does not guarantee an employment offer.

Each interviewed applicant will be notified in writing on outcome of his/her application. **We expect all applicants to adhere to the principles of Professionalism, Respect, Cooperation, Accountability and Care when communicating with us.**

The work and deliberations of the Selection Committee are strictly confidential and any contact of an applicant with its members in view of this procedure is strictly forbidden.

Applicants may be requested to present, at any stage of the selection, documents which will support the information contained in their application form such as originals of their diploma(s), evidence of professional experience clearly indicating the starting, finishing dates and scope of work and workload. Failure to provide such evidence may lead to disqualification of the applicant.

8. APPOINTMENT AND CONDITIONS OF EMPLOYMENT

The most successful applicant (considering the interests of Frontex) will be selected and appointed¹¹ by the Appointing Authority of Frontex.

In order to be engaged, the appointed applicant shall:

- Be available for the job at short notice (not later than 4 months after the job offer is made);
- Produce documents which support the information contained in his/her application;
- Produce appropriate character references (such as a criminal record certificate or equivalent certificate, not older than six months) and specific declarations prior to his/her engagement to finally assess his/her up-to-date suitability (or limitations) for the performance of duties;
- Be physically fit to perform his/her duties¹².

The appointed external applicant will be engaged as temporary staff pursuant to Article 2(f) of the CEOS in function group and grade **AD6**¹³. A contract of employment will be offered for a period of five years, with a probationary period of nine months. The contract may be renewed.

The staff member's remuneration consists of a basic salary and allowances. The staff member may be entitled to various allowances, in particular to an expatriation (16 % of basic gross salary) or to a foreign residence allowance (4 % of basic gross salary) - depending on particular situation, and to family allowances (depending on personal situation) such as household allowance, dependent child allowance, pre-school allowance, education allowance.

The final net calculation (amount payable) is as follows:

Function group, grade and step	AD6 Step 1	AD6 Step 2
1. Basic net/payable salary (<i>after all deductions, contributions and taxes are applied</i>)	4 083 EUR 17 633 PLN	4 234 EUR 18 289 PLN
2. Other possible monthly entitlements/allowances, depending on the personal situation of the candidate (<i>expressed as gross amount weighted by 78.80% correction coefficient applicable for Poland</i>):		
b. Household allowance	291 EUR 1 257 PLN	296 EUR 1 276 PLN
c. Expatriation allowance	852 - 1 092 EUR 3 680 - 4 717 PLN	888 - 1 129 EUR 3 835 - 4 875 PLN
d. Dependent child allowances for each child	403 EUR 1 742 PLN	403 EUR 1 742 PLN
e. Preschool allowance	99 EUR 425 PLN	99 EUR 425 PLN
f. Education allowance for each child up to	547 EUR 2 363 PLN	547 EUR 2 363 PLN

The remuneration is expressed in EUR, after the compulsory deductions set out in the Staff Regulations of Officials (the "Staff Regulations")¹⁴ or in any implementing regulations is weighted by the correction coefficient for Poland (currently 78.80). It can be paid either in EUR or in PLN according to a fixed exchange rate (currently 4.3190 PLN/EUR).

¹¹ Engagement of an inter-agency applicant in grade higher than AD6 is conditional upon the availability of respective grades in Frontex' Establishment Plan at the moment of appointment.

¹² Before the engagement, the successful applicant shall be medically examined by the EU medical service to fulfil the requirement of Article 13 of CEOS.

¹³ For existing EU temporary staff 2(f) the classification in grade and step should be established in line with Article 55 of the CEOS.

¹⁴ Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ P 45, 14.6.1962, p. 1385), as last amended.

The remuneration of the staff members, the correction coefficient and the exchange rate are updated annually before the end of each year, with retroactive effect from 1 July, in accordance with Annex XI of the Staff Regulations.

Staff pays an EU tax at source and deductions are also made for medical insurance, pension and unemployment insurance. Salaries are exempt from national taxes. The rate of the solidarity levy is 6 %. Our package of benefits also includes: sickness and medical insurance, a competitive EU pension scheme, reimbursement for sports and fitness club memberships, language classes and an assistance from the expatriate services team. Find out more about benefits at Frontex by following this [link](#).

Staff is entitled to an annual leave of two working days per each complete calendar month of service and to additional days of leave depending on the grade and age. Moreover, two and a half leave days are granted every year to the staff members entitled to the expatriation or foreign residence allowance for the purpose of visiting their home country. In addition, there are on average 18 public holidays per year. Special leave is granted for certain circumstances such as marriage, birth or adoption of a child.

An [accredited European School](#)¹⁵ operates in Warsaw to allow dependent children of all Frontex statutory staff (including Polish nationals) to attend a (tuition-free) European-type multilingual education. The school offers the complete education cycle (from Nursery to Secondary level finishing with the European Baccalaureate exam). Frontex staff children enjoy priority admission to this school, however it may happen that the required class/level is full at the moment of admission and the school cannot enroll the child. In such a case, education allowance may be granted up to a single ceiling provided that an enrolment took place at another fee-paying school. The admission process is exclusively being handled by the school and it's subject to school's internal policies¹⁶; therefore, it is strongly advisable that parents interested get promptly in contact directly with the school to receive thorough information¹⁷.

Moreover, the Headquarters Agreement signed between the Agency and the Polish authorities¹⁸ in 2017, the Polish authorities may provide benefits to Frontex expatriate staff¹⁹, which are available after starting the employment at Frontex, and after certain eligibility criteria are met:

- (a) reimbursement of VAT on purchases of household goods and furniture to assist a newcomer to settle in Warsaw;
- (b) reimbursement of VAT and excise tax (if applicable) on a purchase of motor-vehicle.

Frontex requires selected applicants to undergo a vetting procedure executed by the National Security Authority of the applicants' state of citizenship in order to obtain a personnel security clearance. The level of the latter depends on the specific post/position. For this post, the **required level of clearance is specified on the title page of the Vacancy Notice**. Applicants who currently hold a valid personnel security clearance at the above-mentioned level (or higher) may not need to obtain a new one, pending confirmation from their respective National Security Authority. The National Security Authority of the applicant shall provide Frontex, with an opinion or a personnel security clearance in accordance with relevant national legislation. In case selected applicants do not currently hold a valid security clearance at the above-mentioned level, Frontex will request such from the National Security Authority of the applicants' state of citizenship. In case of a failure to obtain the required personnel security clearance or if the National Security Agency issues a negative opinion at the above-mentioned level after the signature of the contract of employment Frontex has the right to terminate the contract of employment.

9. PROTECTION OF PERSONAL DATA

Frontex ensures that applicants' personal data are processed in accordance with 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.

Please note that Frontex will not return applications to applicants. This is due, in particular, to the confidentiality and security of such data.

¹⁵ More details on the European Schools system available here: [About the Accredited European Schools](#) (eursc.eu).

¹⁶ E.g. the school may require the pupil concerned to set language competency exams, etc.

¹⁷ You may find contact details by accessing: [International European School*Warsaw](#)

¹⁸ Headquarters Agreement between the Republic of Poland and the European Border and Coast Guard Agency (Frontex) (Polish Official Journal of 2017, item 1939).

¹⁹ Polish citizens and permanent residence holders are excluded.

The respective privacy statement can be accessed [here](#). The legal basis for the selection procedures of temporary staff is defined in the CEOS²⁰, in the Management Board Decision No 14/2019²¹ and in the Decision of the Executive Director No R-ED-2022-17²².

The purpose of processing personal data is to enable to properly carry out selection procedures.

The selection procedure is conducted under the responsibility of the Human Resources Unit within the HR and Corporate Services Division. The data controller for personal data protection purposes is the Head of the Human Resources Unit.

The information provided by applicants will be accessible to a strictly limited number of staff within the Human Resources, to the members of the Selection Committee and to Frontex management. If necessary, it will be provided to the staff of the Legal and Procurement Unit, of the Inspection and Control Office, external parties directly involved in the selection process or to respective ICT experts. For the purposes of safeguarding the financial interests of the Union, your personal data may be processed by the Frontex Internal Audit Capability, the Internal Audit Service of the European Commission, the European Court of Auditors, the Financial Irregularities Panel and/or the European Anti-Fraud Office (OLAF).

There will be no automated decision-making or profiling based on the applicants' data.

No data will be transferred to a third country or an international organisation.

Processing begins on the date of receipt of the application. Data storage policy is as follows:

- For applications received from non-selected applicants: the data are filed and stored in archives for **5 years** and after this time the data are destroyed;
- For applicants placed on a reserve list but not recruited: the data are kept for the period of validity of the **reserve list** and after this time the data are destroyed;
- For recruited applicants: the data are kept for a period of **10 years** after the termination of employment and after this time the data are destroyed.

Applicants have the right to request access to and rectification or restriction of processing of their personal data or, where applicable, the right to object to that processing or the right to data portability. In case of identification data, applicants can rectify those data at any time during the procedure. In the case of data related to the eligibility or selection criteria, the right of rectification can only be exercised by submitting/uploading a new application and it cannot be exercised after the closing date for submission of applications. Withdrawal of the consent to such data processing operations will result in the exclusion of the applicant from the recruitment and from the selection procedure.

Should an applicant have any query concerning the processing of his/her personal data and has substantiated request, he/she shall address them to the Human Resources Unit at jobs@frontex.europa.eu or Frontex Data Protection Officer at dataprotectionoffice@frontex.europa.eu.

Applicants may have recourse at any time to the European Data Protection Supervisor (edps@edps.europa.eu).

10. REVIEW AND COMPLAINT PROCEDURE

- Each candidate may request feedback on assessment of his or her application as established by the Selection Committee.
- If deemed appropriate, he/she may ask for a formal review/reassessment of the original assessment.
- After Frontex takes a formal decision on candidate's application, he/she may lodge a complaint against an act adversely affecting him/her.

Details of these procedures are provided [here](#).

11. APPLICATION PROCEDURE

Note: It is required to upload the digital application form saved in its original electronic dynamic PDF format (not scanned). Do not use any e-mail communication to submit your application (for exceptional circumstances see point 6 below) - such an application will be automatically disregarded and will not be recorded and further processed.

Frontex Application Form is to be downloaded (as a dynamic PDF form) from Frontex website under the link provided

²⁰ In particular the provisions governing conditions of engagement in Title II, Chapter 3.

²¹ Management Board Decision No 14/2019 of 18 July 2019 laying down general implementing provisions on the procedure governing the engagement and use of temporary staff under Article 2(f) of the Conditions of Employment of Other Servants of the European Union.

²² Decision of the Executive Director No R-ED-2022-17 on the recruitment and selection of temporary staff under Article 2(f) CEOS.

next to the Reference Number of the post/position. This digital application form is specifically created only for this selection procedure (and shall not be reused for another procedure).

The Frontex Application Form must:

1. Be opened in a PDF reader in a MS Windows equipped computer - the recommended version of the PDF reader is Adobe Acrobat Reader DC (version 2023.008.20555. You may download a free version here: <https://get.adobe.com/uk/reader/>).
2. **Not** be manipulated or altered. The form is digitally signed and protected against any manipulation or changes. Therefore, applicants shall not try to manipulate and/or alter it - in such a case the digital signature will disappear, and the application form will become invalid for subsequent processing resulting in an automatic rejection of such submission.
3. Be completed in English. Fields, where you may enter your input, are highlighted in light blue colour. Fields marked with an asterisk (*) indicate a required input. You should be concise, the space for your input is limited by the size of the text boxes.
4. Be saved and named as follows: 'SURNAME_RCT-2025-00007'.
5. **Be submitted to Frontex - after saving - by uploading it to this URL link:**

<https://microsite.frontex.europa.eu/en/recruitments/RCT-2025-00007>

6. In case you have technical issues with filling/saving/uploading your electronic application form, you may write to us (in advance of the closing date for submission of applications) at jobs@frontex.europa.eu.

In case you submit more than one application for this procedure, Frontex will only assess the latest one and will automatically disregard all your previous applications.

If at any stage of the selection procedure it is established that any of the requested information provided by an applicant is false or misleading, the applicant in question will be disqualified.

Do not attach any supporting or supplementary documentation with your application until you have been asked to do so by Frontex.

Incomplete applications, applications uploaded after the deadline, sent by e-mail without prior consent of Frontex HR or applications using inappropriate, or altered/manipulated application forms will be automatically disregarded by the system and will **not** be processed further.

Due to the large volume of applications, Frontex regrets that only applicants invited for the test and interview will be notified about the outcomes. The status of the selection procedure is to be found on Frontex website.

Due to high volume of selection procedures handled by Frontex, the period between the closing date for the submission of applications and the final shortlisting of applicants for an interview may take more than two months.

The closing date (and time) for the submission of applications is provided on the title page of the Vacancy Notice.

Please keep a copy of the automatically generated submission code that proves that you have submitted/uploaded your application to Frontex.

Applicants are strongly recommended not to wait until the last day to submit their applications.

Frontex cannot be held responsible for any last-minute malfunction due to an overload of the system or for other technical issues applicants may eventually encounter in the very last moment before the deadline.