

VACANCY NOTICE - TEMPORARY STAFF

Reference number: RCT-2025-00118

Cybersecurity Officer (Senior Cybersecurity Expert)

Post (business title):	Cybersecurity Officer (Senior Cybersecurity Expert) in Cyber Security Sector, Digital Services Unit, Security and Information Management Division (1 post) <i>(a reserve list to be created for 1 post to be filled)</i>
Short job overview:	Cybersecurity Expert plays an important role in the management, communication, and enforcement of relevant cybersecurity protections for the entire ICT infrastructure. This role supports all Digital Services Unit's (DIG) teams and other units in the development, implementation and operation of adequate cybersecurity controls. The role focuses mainly on cybersecurity operations and maintains appropriate contacts with special interest groups, other agencies, CERT-EU, forums or professional associations within cybersecurity domain at EU level.
Sector/Unit/Division:	Cyber Security Sector / Digital Services Unit / Security and Information Management Division
Function group / Grade / Post title:	Temporary staff 2(f), AD7, Cybersecurity Officer (Senior Cybersecurity Expert)
Grade bracket for internal mobility ¹ :	AD5 - AD7
Grade for inter-agency mobility ² :	AD5 - AD7
Location:	Warsaw, Poland
Starting date:	Third quarter 2026 (desired)
Level of Security Clearance:	CONFIDENTIAL UE / EU CONFIDENTIAL
Closing date for applications	<u>(MIDDAY) 13 April 2026 at 12:00 h³, Warsaw local time</u>

Table of Contents

1.	BACKGROUND	2
2.	SECURITY AND INFORMATION MANAGEMENT DIVISION	3
3.	DUTIES AND RESPONSIBILITIES LINKED TO THE POST	4
4.	ELIGIBILITY CRITERIA	5
	4.1. General/common criteria	5
	4.2. External applicants	5
	4.3 Internal applicants	6
	4.4 Inter-agency applicants	6
5.	SELECTION CRITERIA	6
6.	EQUAL OPPORTUNITIES, DIVERSITY & INCLUSION	7
7.	SELECTION PROCEDURE	7
8.	APPOINTMENT AND CONDITIONS OF EMPLOYMENT	8

¹ For existing EU temporary staff 2(f) applicants for whom Article 55 of the Conditions of Employment of Other Servants of the European Union (CEOS) is applicable.

² Ibid 2

³ Date of publication: 5 March 2026.

9. PROTECTION OF PERSONAL DATA	10
10. REVIEW AND COMPLAINT PROCEDURE	10
11. APPLICATION PROCEDURE	11

While Frontex selects its new staff based on their merits and without distinction as to race, political, philosophical or religious beliefs, sex or sexual orientation and without reference to their marital status or family situation, Frontex is a very inclusive workplace that strives to improve the gender and geographical balance⁴ among its staff to the widest possible extent, as well striving to foster diversity, amongst others, in terms of race, ethnic or social origin, genetic features, language, disability, age, etc. Therefore, female candidates as well as candidates with any diverse background that are fulfilling the selection criteria are strongly encouraged to apply.

Frontex is looking for talented women and men to establish a reserve list of experienced professionals with high level of personal integrity, responsibility, confidentiality, adhering to EU values, the principles of equal opportunities and equal treatment as well as fundamental rights.

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 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);

⁴ Under-representation is specifically observed amongst the following nationalities: Austrian, Belgian, Czech, Danish, Dutch, French, German, Icelandic, Irish, Italian, Liechtensteiner, Norwegian, Slovak, Swedish, Swiss.

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

- 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: <http://www.frontex.europa.eu>.

2. SECURITY AND INFORMATION MANAGEMENT DIVISION

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).

Digital Services Unit - organisation and main tasks and responsibilities

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

The Digital Services Unit is composed 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.

Cyber Security Sector - organisation and main tasks and responsibilities

The Cyber Security Sector (CSS) is led by the Head of Sector who reports to the Head of Digital Services Unit.

The main tasks and responsibilities of the Cyber Security Sector are as follows:

- (a) liaising on a regular basis with the Frontex Security Officer and the Local Informatics Security Officer to prepare Security Operating Procedures, perform risk assessments on classified and sensitive non classified Communication and Information Systems (CIS), plan and perform security audits, ensure cyber incidents management, evaluate the cyber threat level;
- (b) defining and implementing cybersecurity strategies, action plans and baselines for all ICT environments managed by DIG;
- (c) ensuring continuous improvement of the cybersecurity posture of the Agency in view of the constantly changing cyberthreat landscape;
- (d) ensuring compliance with cybersecurity regulations and other applicable regulatory frameworks concerning ICT security matters;
- (e) managing of the Security Operations Centre (SOC) and ensuring cybersecurity monitoring and incident response capabilities for all units utilising DIG services;
- (f) maintaining and operating of IT vulnerability management services;

- (g) ensuring operation and maintenance of services supporting IT endpoints security, antimalware protection, network security, IT systems secure authentication and authorisation, web access security management, cybersecurity evaluations and assessments, secure software development and cryptographic services (internal Public Key Infrastructure; email encryption services);
- (h) participation in accreditation of European Union Classified Information (EUCI) networks managed by the Agency;
- (i) providing SEC with technical / ICT input for security risk assessments and maintaining cybersecurity risk register;
- (j) supporting data controllers and processors in order to ensure that technical cybersecurity measures are in place for the purpose of compliance with the EU Personal Data Protection Regulation;
- (k) ensuring execution of the function of Cybersecurity Officer and Incident Managers (24/7) as per relevant and applicable cybersecurity regulations.

3. DUTIES AND RESPONSIBILITIES LINKED TO THE POST

The Cybersecurity Officer (Senior Cybersecurity Expert) strengthens the security, resilience and compliance of the Agency's ICT environments by leading and supporting assigned cybersecurity operations, risk-based security engineering, and the implementation of controls required under the EU Cybersecurity Regulation for EU Institutions and internal cybersecurity plans. Working across all Digital Services Unit teams and with other Agency stakeholders, the Expert ensures the protection of ICT systems (classified and unclassified), contributes to secure architecture design, oversees threat and vulnerability management, and maintains operational cooperation with CERT-EU, EU agencies and relevant cybersecurity communities. The role drives continuous improvement of the Agency's cybersecurity posture through risk analysis, security testing, incident management and the implementation of technical and organisational safeguards.

Tasks and responsibilities:

1. Contribute to the definition, maintenance and implementation of cybersecurity programmes, strategies, baselines and action plans for all ICT environments, including cloud and hybrid infrastructures.
2. Support the Unit in the design, review and validation of secure architectures, ensuring appropriate security controls are correctly implemented and aligned with Agency policies and EU regulatory frameworks.
3. Provide expert input to cybersecurity risk assessments (including threat modelling), ensuring risk treatment options are defined and integrated into the system lifecycle.
4. Participate in system specification, procurement and development processes to ensure cybersecurity requirements are correctly defined, documented and enforced.
5. Identify, assess and prioritise cybersecurity threats, vulnerabilities and emerging risks relevant to the Agency's operational and geopolitical context.
6. Contribute to planning and execution of security testing, including vulnerability scanning, penetration testing, red team exercises and configuration reviews.
7. Provide ownership and expert support for assigned security operations services including privileged access management, secret management, endpoint security, application security operations and network detection and response.
8. Act as Cybersecurity Incident Manager in accordance with the Incident Response Plans, leading assigned incident triage, containment, eradication, recovery and reporting activities.
9. Collaborate with CERT-EU, internal CSIRT members and system owners in responding to cybersecurity incidents, including those involving unclassified sensitive and classified data.
10. Participate in the validation of ICT changes to ensure they do not compromise confidentiality, integrity or availability of Agency assets and that security requirements are met prior to deployment.
11. Contribute to internal posture assessments, benchmarking, and audit activities demonstrating compliance with EU cybersecurity regulation and internal Agency rules.
12. Provide expertise regarding the operational security of AI systems, cryptographic services and systems processing sensitive or operational personal data.
13. Liaise with EU institutions, CERT-EU, EU agencies and internal stakeholders on cybersecurity matters, ensuring effective information exchange and operational alignment.
14. Participate in relevant cybersecurity communities of practice and threat-intelligence networks, sharing knowledge and maintaining situational awareness.
15. Lead the development and continuous improvement of SIEM/SOAR use cases, ensuring coverage of high-risk scenarios and hybrid-threat vectors.

16. Contribute to the alignment with the 'zero-trust principles' and implementation of related operational controls
17. Contribute to business continuity, disaster recovery exercises and cyber crisis management planning.

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).

4.2. External applicants

Minimum qualifications (university diploma)

1. Possess a level of education which corresponds to **completed university studies** attested by a diploma when the normal period of university education is **four years⁸ or more**.
or

Possess a level of education which corresponds to completed university studies attested by a diploma followed by at least one year full-time professional experience, when the normal period of university education is at least three years⁹.

Required professional experience

2. Possess (by the closing date for applications) at least **6 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 fulfilled¹⁰.

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.

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.

⁸ Diploma recognized by any EU Member State to be at EQF levels 6 or 7; 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 will be taken into consideration.

⁹ Diploma recognized by any EU Member State to be at EQF level 6; 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 will be taken into consideration.

¹⁰ Professional experience will be taken into account after the award of the minimum qualification certifying the completion of the level of studies or professional training required. Only duly documented professional activity is taken into account.

4.3 Internal applicants

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

4.4 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 CEOS¹¹ 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 moving¹².
3. Have successfully completed the probationary period as provided for in Article 14 of the CEOS in the relevant function group¹³.

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).

Professional qualifications, competencies and experience required:

1. University degree or post-graduate degree in information technology or information / cybersecurity management and being holder of a relevant certification in ICT security (CISSP, CISM, CISA and similar);
2. At least 5 years, following the award of the diploma, of professional experience acquired in positions of the Information Security / Cybersecurity Officer or similar role;
3. Good knowledge and practical experience in delivering technical controls guided by NIST CSF, ISO/IEC 27000 family standards and other well-known Information / cybersecurity frameworks;
4. Detailed knowledge of system security vulnerabilities, threats and exploit mechanisms, penetration testing and remediation techniques; and experience in direct management of security monitoring, application security operations, forensic oversight, endpoints and cloud security, privileged access and cybersecurity aspects of AI and Data Privacy.
5. Experience in defining and implementing 'zero-trust architecture' type cybersecurity controls for governmental organisations and practical knowledge and understanding of various security architectures within EUCI environments with different classification levels.

Besides, the following attributes would be considered advantageous:

6. Experience in working and defining cybersecurity strategies and ICT policy frameworks within the governmental agency environments and/or international organisations (i.e. NATO, EU, UNO);
7. Good knowledge of a cyber risk analysis methodologies and threat modelling and professional experience in monitoring, testing and evaluating cybersecurity controls' effectiveness, system security accreditation processes;
8. Experience in the design, implementation and/or supervision of the processes leading to tailoring / fine tuning of security detection and correlation rules specific to ICT systems of EU agencies or other governmental bodies;

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

¹² 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.

¹³ 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.

9. Practical knowledge and understanding of encryption mechanisms in various governmental environments with different classification levels.

Personal qualities and competences:

10. Excellent workload- and self-management skills; flexibility and adaptability, ability to multitask effectively and coordinate a wide range of activities with minimal supervision and to remain stress resistant and effective even under heavy workload;
11. Very good planning and organization skills; ability to independently execute ICT projects through the complete project lifecycle; Flexible and service-oriented attitude;
12. Ability to translate given goals into detailed action plans to deliver expected results on time;
13. Accuracy and attention to details and quality while performing assigned tasks;
14. Ability and confidence to communicate, build and maintain effective working relationships within a multicultural team and with stakeholders at all levels, internally and externally.

6. EQUAL OPPORTUNITIES, DIVERSITY & INCLUSION

Frontex applies an equal opportunities policy and accepts applications without distinction on grounds of age, race, political, philosophical or religious 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 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). Certain selection criteria may be assessed/scored jointly, and some criteria may be assessed/scored in two or more steps of the selection procedure;
- Up to 20 applicants who are best matching the evaluated selection criteria and who have achieved minimum 60% during CV screening will be invited for a written competency test and interview. At least one part of the qualifying written test will be assessed based on anonymised answers. A separate threshold of 50% achieved on the written test is required. Candidates who will not meet this threshold will not be considered for placement on the reserve list;
- 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;
- The most suitable applicant(s) for the post (s) who have achieved minimum 60% of the total competency test and interview score will be proposed for a reserve list. An additional interview with the Appointing Authority and/or another relevant manager may be arranged before the Appointing Authority takes the final decision;
- A reserve list 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 is absolutely 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 respective part of the application.

8. APPOINTMENT AND CONDITIONS OF EMPLOYMENT

The most successful applicant will be selected and appointed 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 the appropriate character references as to his/her suitability for the performance of duties (a criminal record certificate or equivalent certificate, not older than six months) and a declaration in relation to interests that might be considered prejudicial to his/her independence;
- Be physically fit to perform the duties¹⁴.

The successful external applicant will be engaged as temporary staff pursuant to Article 2(f) of the Conditions of Employment of Other Servants of the European Communities (CEOS). The temporary post in question is placed in the following function group and grade: **AD7**¹⁵.

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	AD7 Step 1	AD7 Step 2
1. Basic net/payable salary (after all deductions, contributions and taxes are applied)	4 846 EUR 20 535 PLN	5 022 EUR 21 281 PLN
2. Other possible monthly entitlements/allowances, depending on the personal situation of the candidate (expressed as gross amount weighted by 82.30% correction coefficient applicable for Poland):		
a) Household allowance	328 EUR 1 391 PLN	334 EUR 1 414 PLN
b) Expatriation allowance	1 037 - 1 298 EUR 4 395 - 5 500 PLN	1 081 - 1 342 EUR 4 580 - 5 688 PLN
c) Dependent child allowances for each child	434 EUR 1 838 PLN	434 EUR 1 838 PLN
d) Preschool allowance	106 EUR 449 PLN	106 EUR 449 PLN
e) Education allowance for each child up to	589 EUR 2 495 PLN	589 EUR 2 495 PLN

The remuneration is expressed in EUR, after the compulsory deductions set out in the Staff Regulations or in any implementing regulations is weighted by the correction coefficient for Poland (currently 82.30%). It can be paid either in EUR or in PLN according to a fixed exchange rate (currently 4.2378 PLN/EUR).

¹⁴ Before the engagement, the successful applicant shall be medically examined by the EU medical service to fulfil the requirement of Article 13 of Conditions of Employment of Other Servants of the European Communities (OJ L 56, 4.3.1968, p. 10), as lastly amended.

¹⁵ Specific conditions about grading are defined on the title page of the Vacancy Notice. For existing EU temporary staff 2(f) the classification in grade and step should be established in line with Article 55 of the CEOS.

The remuneration of the staff members, the correction coefficient and the exchange rate are updated, in principle, 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 %.

Staff is entitled to 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 days per year. Special leave is granted for certain circumstances such as marriage, birth or adoption of a child, etc.

An accredited European School¹⁶ 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 enrol 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 policies¹⁷; therefore, it is strongly advisable that parents interested get promptly in contact directly with the school to receive thorough information¹⁸.

Moreover, under the Headquarters Agreement signed between the Agency and Polish authorities¹⁹ in 2017, the Polish authorities may provide benefits to Frontex expatriate staff²⁰, 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 a motor-vehicle.

Frontex being a knowledge-based organization acknowledges the importance of training provided to its staff. Frontex provides general and technical nature training as well as professional development opportunities that are discussed annually during the staff performance appraisal.

Throughout the period of service staff is a member of the EU pension scheme. The pension is granted after completing a minimum of 10 years' service and after reaching the pensionable age of 66 years. Pension rights acquired in one or more national schemes before starting to work at Frontex may be transferred into the EU pension system.

Staff is covered 24/7 and worldwide by the Joint Sickness Insurance Scheme (JSIS). Staff is insured against sickness, the risk of occupational disease and accident as well as entitled under certain conditions to a monthly unemployment allowance, the right to receive payment of invalidity allowance and travel insurance.

For further information on working conditions please refer to the Staff Regulations and the CEOS.

Frontex requires selected candidates to undergo a vetting procedure executed by the National Security Authority of the candidates' 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**. Candidates 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 candidate shall provide Frontex, with an opinion or a personnel security clearance in accordance with relevant national legislation. In case selected candidates do not currently hold a valid security clearance at the above-mentioned level, Frontex will request such from the National Security Authority of the candidates' state of citizenship. In case of a failure to obtain the required personnel security clearance or if the National Security Agency issues a negative

¹⁶ More details on the European Schools system available here: *About the Accredited European Schools* (eursc.eu).

¹⁷ E.g. the school may require the pupil concerned to set language competency exams, etc.

¹⁸ You may find contact details by accessing: *International European School*Warsaw*

¹⁹ *Headquarters Agreement between the Republic of Poland and the European Border and Coast Guard Agency (Frontex) (Polish Official Journal of 2017, item 1939).*

²⁰ Polish citizens and permanent residence holders are excluded.

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 Article 5(1)(a) of 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.

The legal basis for the selection procedures of temporary staff is defined in the CEOS²¹.

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 Human Resources and Corporate Services Division of Frontex. The controller for personal data protection purposes is Frontex, the responsible Unit being the Human Resources Unit.

The information provided by applicants will be accessible to strictly limited number of staff in Human Resources, to the Selection Committee members and to Frontex management. If necessary, it will be provided to the staff of Legal Services and Procurement Unit, Inspection and Control Office, external parties directly involved in the selection process or to respective experts in ICT (in case of technical issues with the application). 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 upon applicants' data.

No data is transferred to a third country or international organisation.

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

- For applications received from not-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 concerning the data subject or, where applicable, the right to object to 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 a consent to such data processing operations would result in exclusion of the candidate 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 HR 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.

²¹ In particular the provisions governing conditions of engagement in Title II, Chapter 3.

- After Frontex takes a formal decision on candidate's application, he/she may lodge a complaint.

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 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:

- 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 2021.001.20155. You may download a free version here: <https://get.adobe.com/uk/reader/>).
- **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.
- 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.
- Be saved and named as follows: 'SURNAME_RCT-2025-00118'.
- **Be submitted to Frontex - after saving - by uploading it to this URL link:**
<https://microsite.frontex.europa.eu/en/recruitments/RCT-2025-00118>
- 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 clearly indicating in the subject of the email the reference number of the post/position and the post (business) title.

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.

Applicants shortlisted for an interview will be requested to supply documentary evidence in support of the statements made in the application. Do not, however, 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 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.