FRONTEX

VACANCY NOTICE – TEMPORARY STAFF

Reference number: RCT-2021-00147

ICT Administrators (6 posts)

Post (business title):	**ICT Administrators** *(a reserve list to be created for 6 posts to be filled)*
Sector/Unit/Division:	Digital Services Unit/Financial, Digital and Security Division
Function group / Grade / Post title:	Temporary staff 2(f), AD6, Administrator[4]
Grade bracket for internal mobility[5]:	AD5 – AD12
Grade bracket for inter-agency mobility:	AD5 – AD6
Location:	Warsaw, Poland
Starting date:	October 2022 (desired)
Level of Security Clearance:	SECRET UE / EU SECRET
Closing date for applications	**(MIDDAY) 29 July 2022 at 12:00 h[6], Warsaw local time**

1. BACKGROUND

The European Border and Coast Guard Agency (Frontex) has been established under the European Border and Coast Guard Regulation[7]. 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 2,000 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 raise 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:

---

[4] *Type of post: Administrator.*

[5] *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.*

[6] *Date of publication: 14 June 2022.*

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

- 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.

For more information, please refer to our website: http://www.frontex.europa.eu.

2. DIGITAL SERVICES UNIT

The DIG acts as a centre of expertise and support in the area of information and communication technology. The Unit is responsible to support the Frontex business entities to achieve the strategic goals of Frontex. In particular, the Unit centralises the management of the Frontex ICT infrastructure, services and products delivery and cybersecurity management. To achieve these objectives the Unit is divided in three sectors:

Digital Projects Sector (DPS)

Main tasks

(a) Managing all ICT projects approved by the ED.

(b) Ensuring portfolio management between business entities and DIG.

(c) Ensuring product delivery on time with quality expected.

(d) Ensuring development of new products.

Digital Operations Sector (DOS)

Main tasks

(a) Providing first level ICT support.

(b) Providing field deployment support for Frontex operations, antennas and FLOs.

(c) Providing second and third level support.

(d) Providing the ICT infrastructure for classified and unclassified operating models.

(e) Implementing of the digital modernisation concept using cloud technology.

(f) Ensuring the smooth operations of ICT and business applications.

(g) Maintaining the ICT disaster recovery plan.

Cyber Security Sector (CSS)

Main tasks

(a) Ensuring security of ICT services and product development lifecycle.

(b) Ensuring security monitoring and response capabilities.

(c) Improving internal cybersecurity posture.

(d) Participating in accreditation of European Union Classified Information (EUCI) networks.

3. DUTIES AND RESPONSIBILITIES LINKED TO THE POSTS

3.1. Senior Network Specialist (SNS)

Reporting to the Head of Unit or under the supervision of the respective Head of Sector, the main duties related to this post/position are:

- ➢ Administering Frontex ICT network services according to the agreed service levels, operation and security policies and procedures,
- ➢ Configuring and maintaining the network management systems and monitoring tools,
- ➢ Maintaining the network configuration databases,
- ➢ Writing and reviewing technical documentation and standard operation procedures,
- ➢ Supervising the services provided by external contractors,
- ➢ Cooperation with the external and internal partners and suppliers,
- ➢ Initiating the procurement procedures and overseeing the projects related to ICT network services as well as contributing to other procedures and projects related to ICT infrastructure,
- ➢ Carrying out other tasks as assigned by Head of Sector.

The Digital Operations Sector (DOS) personnel is working on shifts: 8:00-16:30, 09:30-18:00 from Monday until Friday, including 30 minutes lunch break. Due to the nature of the work the personnel also provide paid 24/7 on-call service outside normal working hours.

3.2. Directory Services Engineer (DSE)

Reporting to the Head of Unit or under the supervision of the respective Head of Sector, the main duties related to this post/position are:

- ➢ Designing and implementing authentication and authorization solutions based on Microsoft technologies in the hybrid and cloud setups.
- ➢ Ensure the Active Directory or Azure Active Directory infrastructure integrates seamlessly with the following components: network, IT security, messaging and collaboration, remote access, virtualized environments, public cloud solutions in IaaS, PaaS and SaaS model.
- ➢ Administration and monitoring of Microsoft Active Directory, ADLDS, ADFS, Azure Active Directory and its identity and access management features.
- ➢ Active Directory Certificate Service setup, troubleshooting and administration.
- ➢ Prepare the technical documentation and operating procedures.
- ➢ Implementing changes according to Digital Services Unit change management procedures.
- ➢ Other specific duties as assigned by 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.

3.3.   Microsoft 365 Specialist (M365)

Reporting to the Head of Unit or under the supervision of the respective Head of Sector, the main duties related to this post/position are:

- ➢ Administration, support and configuration of Microsoft 365 services (mainly Exchange Online, MS Teams).
- ➢ Administration, support and configuration of an enterprise-level Microsoft Exchange Server infrastructure (including Exchange Hybrid)
- ➢ Administration, support and configuration of an enterprise-level Skype for Business Server infrastructure
- ➢ Proactive monitoring of maintained services to ensure maximum performance, efficiency and availability

- ➢ Oversees the integration of maintained services with other systems, applications and services
- ➢ Sets, recommends and/or enforces standards, methodologies and protocols for the development and administration of maintained services
- ➢ Performing diagnosis and resolution of moderately complex issues
- ➢ Designing processes to eliminate moderately complex and possibly systemic problems
- ➢ Contributing to cybersecurity improvements and investigations
- ➢ Creating and updating technical documentation and operating procedures
- ➢ Supporting Team Leader with the architecture, design of maintained services, including infrastructure requirements
- ➢ Supporting Team Leader with planning, organizing and guiding the work of contractors
- ➢ Participating in change management activities

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

3.4. IT Infrastructure Specialist (IT IS)

Reporting to the Head of Unit or under the supervision of the respective Head of Sector, the main duties related to this post/position are:

- ➢ Administration, support, and configuration of Microsoft Windows Servers (Windows Server 2012 and later).
- ➢ Administration, support, and configuration of VMware vSphere (including ESXi, vCenter, VUM, vROP)
- ➢ Administration, support, and configuration of Veeam Backup and Replication infrastructure
- ➢ Administration, support, and configuration od Disaster Recovery Solutions (based on Veeam and Zerto).
- ➢ Proactive monitoring of maintained services to ensure maximum performance, efficiency, and availability
- ➢ Oversees the integration of maintained services with other systems, applications and services
- ➢ Sets, recommends and/or enforces standards, methodologies and protocols for the development and administration of maintained services
- ➢ Performing diagnosis and resolution of moderately complex issues
- ➢ Designing processes to eliminate moderately complex and possibly systemic problems
- ➢ Contributing to cybersecurity improvements and investigations
- ➢ Creating and updating technical documentation and operating procedures
- ➢ Supporting Team Leader with the architecture, design of maintained services and infrastructure
- ➢ Supporting Team Leader with planning, organising, and guiding the work of contractors
- ➢ Supporting Team Leader with selected administrative tasks, e.g., procurement activities
- ➢ Deputizing Team Leader during his unavailability.
- ➢ Participating in change management activities

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

3.5. Workstation Management Technical Expert (MIW)

Reporting to the Head of Unit or under the supervision of the respective Head of Sector, the main duties related to this post/position are:

- ➢ Planning, designing and constantly improving modern, controlled, high performing, reliable and secure end users' workstations environment, ensuring excellent user experience
- ➢ Implementing and supporting modern, controlled, high performing, reliable and secure end users' workstations environment, ensuring excellent user experience
- ➢ Managing Microsoft Azure AD, Autopilot, Intune, SCCM, MECM

- Managing and being accountable for workstations configurations: preparation and distribution of the operating system images, software distribution, application and security patch, updates and upgrades management, workstations security

- Managing and being accountable for workstations configurations: configuration settings and policies

- Monitoring and reporting the workstation configuration and patching compliance towards agreed configuration standards, the newest software versions and security patches

- Monitoring and reporting software compliance and license usage

- Contributing to projects related with the use of modern ICT workplace

- Contributing to team development and contract management related with the use of modern ICT workplace

- Following and contributing to Frontex ITIL processes and practices

- Creating and maintaining up to date solution documentation including configuration standards, technical specifications, Standard Operating Procedures (SOPs), user manuals, knowledge base articles etc.

- Participating in the paid on-call support service available 24/7/365, shared with other team members within the same area of expertise

- Other as assign by the reporting officer

3.6.   ICT Service Manager (ITSM)

Reporting to the Head of Unit or under the supervision of the respective Head of Sector, the main duties related to this post/position are:

- Analysing business needs and managing business owner and customers' expectations

- Managing the cooperation between business owner and other internal and external stakeholders

- Managing services throughout the complete service lifecycle

- Negotiating and defining service level agreements, KPIs and other ICT service parameters

- Monitoring, reporting and presenting compliance with service level agreements, KPIs and other service parameters

- Focusing on and coordinating continual service improvement

- Ensuring excellent user experience

- Contributing to product and project management

- Contributing to team development and contract management

- Contributing to the development of the ITSM solution in order to ensure high quality of support

- Following and improving Frontex ITIL processes and practices

- Creating and maintaining up to date solution and processes documentation including Standard Operating Procedures (SOPs), user manuals, knowledge base articles etc.

- Participating in the paid on-call support service available 24/7/365, shared with other team members within the same area of expertise

- Other as assign by the reporting officer

4. QUALIFICATIONS AND EXPERIENCE REQUIRED

4.1.   Eligibility criteria (for external applicants[8])

To be eligible, an applicant shall:

- Possess a level of education which corresponds to **completed university studies** attested by a diploma when the normal period of university education is **four years or more** (of full-time education);

or

---

[8] 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) the eligibility criteria are defined in Article 12(2) of the CEOS.

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 years** (of full-time education);

> *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.*

> *Only the required education will be taken into account.*

● Possess (by the closing date for applications) at least **3 years** of proven full-time professional experience in positions corresponding to the nature of duties of the vacant post acquired after the diploma was awarded and (at the same time) after the condition(s) described in criterion a) above are fulfilled;

> *Professional experience will be taken into account after the award of the minimum qualification certifying the completion of the level of studies required above in the criterion a). Only duly documented professional activity is taken into account.*

> *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 after achieving the minimum qualification stated in the first two bullet points shall be taken into consideration as professional experience if the official documentation is provided.*

● 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);

● 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;

● Have fulfilled any obligations imposed on him/her by the laws of the country of citizenship concerning military service.

4.2.   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):

4.2.1. Motivation of a candidate to take up the duties linked to the post

4.2.2. Professional competences

The candidate will be required to demonstrate that he/she has:

1. At least 2 years of relevant experience dealing with duties related to the areas of responsibilities assigned to the concrete post (please note that there are six required profiles as described in the field "Duties and responsibilities"):
    - operating and supporting enterprise network services (SNS)
    - designing and implementing cross systems authentication and authorization solutions based on MS technology (DSE)
    - administration, support, and configuration of Exchange Server (M365)
    - administration support and configuration of Windows Servers (IT IS)
    - planning, designing, improving, implementing, and supporting medium to large end user workstation environment (MIW)
    - service management based on ITIL (ITSM)

2. At least 2 years of relevant experience dealing with duties related to the areas of responsibilities:
    - configuring and troubleshooting firewalls, routers, and switches (SNS)

- administering Microsoft Active Directory 2012/2016 and Azure Active Directory in enterprise environment (DSE)
- administration, support and configuration of MS Office 365 and Skype for Business Server (M365)
- administration, support, and configuration of VMware vSphere and Disaster Recovery Solutions, including Data Backup and Restore (IT IS)
- managing Microsoft Azure AD, Autopilot, Intune, SCCM, MECM (MIW)
- creating and maintaining up to date solution and processes documentation including Standard Operating Procedures (SOPs), user manuals, knowledge base articles (ITSM)

3. Sound knowledge and experience in the field of (as per requested profile):
    - TCP/IP and Ethernet protocols and technologies (SNS)
    - Active Directory and/or Azure Active Directory delegation, security models and PowerShell use (DSE)
    - Change and Release management processes (M365) (IT IS)
    - implementing workstations security solutions (including but not limited to Bitlocker) and performing configurations, monitoring, reporting and patching compliance (MIW)
    - defining, negotiating, monitoring, and reporting compliance with service level agreements, KPIs and other ICT service parameters (ITSM)
4. General knowledge and understanding of complex enterprise scale ICT Systems and their interoperability

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

5. Certification in:
    - CCNA, CompTIA Network+ or other equivalent (SNS)
    - Microsoft Certified Azure Administrator Associate, Microsoft Certified Identity and Access Administrator Associate or equivalent (DSE)
    - Microsoft 365 Certified Messaging Administrator Associate or Microsoft 365 Certified Teams Administrator Associate or equivalent (M365)
    - VCP - VMware Certified Professional or equivalent (IT IS)
    - ITIL 4 Foundation or equivalent (MIW) (IT SM)

6. Proven experience in and/or good understanding of:
    - Web application protocols, traffic management solutions (SNS)
    - Microsoft 365 technologies (DSE)
    - Cybersecurity and networking – IP, DNS, SMTP (M365, IT IS, MIW)
    - ServiceNow platform for IT service management (ITSM)

7. Proven experience in and/or good understanding of:
    - Software-defined network solutions and/or public cloud network services (SNS)
    - AWS cloud technologies (DSE)
    - IT Service 1st and 2nd level support (M365, IT IS)
    - Microsoft 365 technologies (MIW)
    - Project management (PM2, Prince 2 or equivalent) (ITSM)

4.2.4. Personal qualities and competences

8. Demonstrate excellent communication skills in English (at minimum B2 level[9]), both orally and in writing to technical and non-technical audiences in a multicultural environment
9. Excellent time management, planning and organization skills, ability to make sound decisions, prioritize and work to deadlines under minimal supervision on multiple tasks

---

[9] *As defined by the Common European Framework of Reference for Languages*
(https://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr)

5. INDEPENDENCE AND DECLARATION OF INTEREST

The selected applicant(s) will be required to make a declaration of commitment to act independently in Union's interest and to make a declaration in relation to interests that might be considered prejudicial to his/her independence.

6. EQUAL OPPORTUNITIES

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.

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;

• 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 relevancy 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. Certain general competencies will not be tested for internal applicants interested in an internal mobility and for applicants from other EU Agencies interested in an inter-agency mobility. 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 Executive Director of Frontex. An additional interview with the Executive Director and/or another relevant manager may be arranged before the Executive Director 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. 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.

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 an 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 Executive Director 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 duties[10].

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: **AD6**[11].

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** *(after all deductions, contributions and taxes are applied)*	**3 123 EUR** **14 115 PLN**	**3 238 EUR** **14 633 PLN**
2. Other **possible monthly entitlements/allowances**, depending on the personal situation of the candidate *(expressed as gross amount weighted by 70.6 correction coefficient applicable for Poland)*:		
b. Household allowance	219 EUR 989 PLN	222 EUR 1 004 PLN
c. Expatriation allowance	640 – 821 EUR 2 894 – 3 710 PLN	667 – 848 EUR 3 016 – 3 834 PLN
d. Dependent child allowances for each child	303 EUR 1 370 PLN	303 EUR 1 370 PLN
e. Preschool allowance	74 EUR 335 PLN	74 EUR 335 PLN
f. Education allowance for each child up to	411 EUR 1 858 PLN	411 EUR 1 858 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 70.6). It can be paid either in EUR or in PLN according to a fixed exchange rate (currently 4.519 PLN/EUR).

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 %.

An accredited European School[12] will operate in Warsaw as of September 2021 to allow dependent children of all Frontex statutory staff (including Polish nationals) to attend a (tuition-free) European-type multilingual education. The school is opening gradually, and the complete education cycle (from Nursery to Secondary level finishing with the European Baccalaureate exam) will be available in September 2024.

Moreover, the headquarters agreement with the Polish authorities is effective as of 1 November 2017. Under this agreement the Polish authorities may provide the following main benefits to Frontex expatriate staff[13]:

(a) in case the appropriate education level is not available yet for a child in the accredited European School in Warsaw - reimbursement of tuition cost of each dependent child attending a school (up to and including secondary school) on Polish territory up to a limit of 35 000 PLN per school year;

(b) reimbursement of VAT on purchases of main household effects to assist a newcomer to settle in Warsaw;

---

[10] 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.

[11] 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.

[12] More detail on the European Schools system available here About the Accredited European Schools (eursc.eu).

[13] Staff of non-Polish nationality and non-permanent residents.

(c) reimbursement of VAT on a purchase of a private car (this entitlement is renewable after 36 months).

An (accredited[14]) European School is gradually being set-up in Warsaw to allow dependent children of all Frontex staff (including Polish nationals) to attend a (tuition-free) European-type multilingual education.

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

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. The pensionable age for staff recruited before 1 January 2014 varies between 60 and 65 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 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 are defined in the CEOS[15].

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 Governance Support Centre of Frontex. The controller for personal data protection purposes is the Head of 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 and Procurement Unit, external parties directly involved in the selection process or to respective experts in ICT (in case of technical issues with the application).

There will be no automated decision making or profiling upon applicants' data.

---

[14] *The process of accreditation is ongoing.*

[15] *In particular the provisions governing conditions of engagement in Title II, Chapter 3.*

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 **2 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 + 1 year 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 or as of the last pension payment **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. APPEAL PROCEDURE

Each applicant may request feedback on assessment of his or her applications as established by the Selection Committee and, if deemed appropriate, ask for a formal review/reassessment by writing to jobs@frontex.europa.eu. Please note that the Selection Committee may only assess the information provided in the application form (during the screening phase) or your performance during the test and interview (we must disregard any other opinions such as reference letters or your own perception of your past achievements). We may not provide you with any data related to other applicants.

If an applicant considers that he/she has been adversely affected by a particular decision related to the selection procedure, he/she can lodge a complaint under Article 90(2) of the Staff Regulations of Officials of the European Union and Conditions of Employment of Other Servants of the European Union, laid down by Council Regulation (EEC, Euratom, ECSC No 259/68)[16], mentioning the reference number of the selection procedure, at the following address:

> Frontex
> Human Resources Unit
> Plac Europejski 6
> 00-844 Warsaw
> Poland

The complaint must be lodged within 3 months. The time limit for initiating this type of procedure starts to run from the time the applicant is notified of the act adversely affecting him/her or from the date of publication of final outcome on Frontex website.

Applicants also have a possibility to complain to the European Ombudsman. Please note that complaints made to the European Ombudsman have no direct effect on the decision taken by Frontex in regard to your application and on the time period laid down in Article 91 of the Staff Regulations. Under Article 2(4) of the general conditions governing the performance of the Ombudsman's duties any complaint lodged with the Ombudsman must be preceded by the appropriate administrative approaches to Frontex.

---

[16] *OJ L 56, 4.3.1968, p. 1, as last amended by Regulation (EU, Euratom) No 1023/2013 of the European Parliament and of the Council of 22 October 2013, OJ L 287, 29.10.2013, p.15.*

11. APPLICATION PROCEDURE

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

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

provided next to the Reference Number of the post/position. This digital application form is <u>specifically created only for this selection procedure</u> (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/).*

- **<u>Not</u>** be manipulated or altered. The form is digitally signed and protected against any manipulation or changes. Therefore, applicants shall <u>not try to manipulate and/or alter it</u> – 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-2021-00147.

- **Be submitted to Frontex – after saving - by uploading it to this URL link:**

    https://microsite.frontex.europa.eu/en/recruitments/RCT-2021-00147

- 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, <u>Frontex will</u> only assess the latest one and will automatically <u>disregard all your previous applications</u>.

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 <u>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.</u>

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 <u>not to wait until the last day</u> 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.