Ref. Ares(2026)1087254 - 30/01/2026

European Union Agency for Cybersecurity
Agamemnonos 14
Chalandri | 15231 | Attiki Greece
Tel:+302814409711
email: info@enisa.europa.eu
www.enisa.europa.eu

CALL FOR EXPRESSION OF INTEREST FOR CONTRACT AGENTS FGIV
CYBERSECURITY OFFICERS (CA/FGIV)
REF. ENISA-CA-FGIV-2026-03

Type of contract	**Contract Agents**
Function Group and grade	**FGIV**
Duration of contract	**4 years (renewable)[1]**
Place of Employment	**Athens, Greece / Brussels, Belgium**
Probation period	**9 months**
Reserve list	**31/12/2029**
Deadline for applications	**02/03/2026 at 23:59:59 hrs EET[2] (CET[3] +1)**

1. THE AGENCY

ENISA's mission is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, European Union institutions, industry, academia and EU citizens[4].

ENISA contributes to policy development and implementation, supports capacity building and preparedness, facilitates operational cooperation at Union level, enhances the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enables knowledge sharing, research, innovation and awareness raising, whilst developing cross-border communities and synergies.

ENISA is located in Athens, Greece (the Agency's official seat) with a branch office in Heraklion (Crete), Greece and a Local Office in Brussels, Belgium.

Further information about ENISA is available on the ENISA website: https://www.enisa.europa.eu/.

[1] For contracts related to Contribution Agreements, the duration of the contract is concluded for a limited, non-renewable period linked to the duration of the Contribution Agreement, including any extensions (even if under a different name within the Programme) and upon budget availability or for a maximum duration of four years, whichever comes first.
[2] Eastern European Time
[3] Central European Time
[4] Regulation (EU) 2019/881 - Cybersecurity Act: http://data.europa.eu/eli/reg/2019/881/oj

2. THE JOB

As a Cybersecurity Officer, you will support ENISA's mission to achieve a high common level of cybersecurity across the Union. The role contributes to the implementation of the EU Cybersecurity Act (CSA), the EU Cybersecurity Certification Framework (EUCC), the Cyber Resilience Act (CRA), and EU cybersecurity policy development and implementation.

ENISA is seeking to draw a reserve list for the upcoming SPD period 2026-2028 for all ENISA units. As needs arise, ENISA will search the pool of reserve list candidates and select those that are appropriate to its needs. The established reserve list may be used to cater for other Agency-wide staffing needs.

Depending on the post profile, you will provide technical, analytical, assurance, and policy support across product security, certification, emerging technologies, threat and risk analysis, and market and regulatory developments, supporting evidence-based policymaking and operational trust in the EU cybersecurity ecosystem.

Under the supervision of the Head of Unit and/or Team Leader, the successful candidate will contribute to ENISA's Work Programme activities.

Overall key responsibilities are:

- Coordinate the delivery of cybersecurity services and provide technical guidance with regard to cyber risk, threat assessments, incident response, awareness raising, skills, and pen tests as part of cybersecurity services to ENISA stakeholders and primarily to Union's essential, important or critical entities;
- Cooperate with internal stakeholders including legal, finance, procurement, communication in the implementation of the services;
- Manage relevant stakeholders within Member States and European Union Institutions, Bodies, and Entities (EUIBAs);
- Be responsible for quality assurance on operational cooperation unit deliverables;
- Establish, track and report on key performance indicators of the assigned projects or services;
- Build and maintain general technical templates and guidelines for operation cooperation service offering;
- Manage programme/projects throughout the entire project lifecycle;
- Participate in the continuous improvement and extension of the existing IT systems, services and policies;
- Manage and handle assigned budget and service contracts and follow up throughout the procurement phases and during implementation;
- Participate in procurement/recruitment panels as the needs of the Agency arise;
- Perform any other duties as assigned by the Head of Unit or Head of Sector in the interest of the service.

The Cybersecurity Officer may work in any of the following areas:

2.1.1 Cybersecurity & Certification Standards (CSA, EUCC)

- Contribute to the **implementation and operation of the EU Cybersecurity Certification Framework;**
- Support **certification activities**, including technical analysis, scheme evolution, and stakeholder engagement;
- Apply and interpret **certification and evaluation standards** (e. g. ISO/IEC 17065, ISO/IEC 19896);
- Support conformity assessment, auditing, and assurance activities.

2.1.2 Cyber Resilience Act (CRA)

- Support implementation of **CRA essential cybersecurity requirements;**
- Assess secure-by-design and secure-by-default practices for ICT products;
- Support vulnerability handling, risk-based requirements, and lifecycle security;
- Provide technical input to CRA guidance and implementation support activities.

2.1.3 Threat Landscape, Risk & Situational Awareness

- Produce EU-level cyber threat landscape analysis;
- Support risk assessment and situational awareness;
- Analyse attack trends, vulnerabilities, and threat actors;

- Provide threat-based input to policy and certification work;
- Conduct threat modelling, vulnerability analysis, and risk assessments.

2.1.4 Product, System & Technology Security

- Conduct **cybersecurity risk analysis, threat modelling, and vulnerability assessment;**
- Support security testing activities (e. g. code analysis, penetration testing);
- Assess security of **networked, cloud, embedded, and wireless systems;**
- Support **secure SDLC practices**, including SBOM/HBOM analysis.

2.1.5 Market, Emerging Technology & Foresight

- Analyse cybersecurity implications of **emerging technologies** (AI, IoT, Industry 4.0, UAVs, satellite communications, future networks);
- Support market monitoring, competitive analysis, and trend forecasting;
- Provide evidence-based input to future certification and policy needs.

2.1.6 Cybersecurity Policy, Regulatory & Strategy

- Provide technical input to **EU cybersecurity policy development and implementation;**
- Support policy impact assessments, guidance documents, and consultation processes;
- Contribute to ENISA activities on **capacity building, awareness raising, and best practices;**
- Support cooperation with EU institutions, Member States, industry, and international partners.

2.1.7 Capacity Building & Stakeholder Engagement

- Develop guidelines, best practices, and recommendations;
- Support capacity building across Member States and stakeholders;
- Promote secure-by-design and cybersecurity maturity;
- Produce **technical reports, dashboards, metrics, and policy inputs;**
- Communicate complex technical information to technical and non-technical audiences;
- Represent ENISA in expert groups, workshops, and stakeholder meetings.

3. QUALIFICATIONS AND EXPERIENCE REQUIRED[5]

3.1 ELIGIBILITY CRITERIA

The selection procedure is open to candidates who satisfy the following eligibility criteria on the closing date and time for application:

- Be a national of one of the Member States of the European Union[6] or EFTA[7] countries;
- Be entitled to their full rights as a citizen[8];
- Have fulfilled any obligations imposed by the applicable laws concerning military service;
- Produce appropriate character references as to their suitability for the performance of the duties;
- Be physically fit to perform the duties linked to the post[9];

[5] Candidates must satisfy ALL the eligibility criteria on the closing date for applications. In the event that you do not fulfil all the eligibility criteria, your application will not be further assessed. Candidates should assess and check before submitting their application whether they fulfil all the requirements as specified in the vacancy notice. Please include in the application form only professional experience and academic qualifications for which you hold supporting documents. Candidates must be able to provide supporting documents clearly showing duration and nature of experience upon request.
[6] It should be noted that, due to the withdrawal of the United Kingdom from the European Union on 31/01/2020, British nationals, who do not hold the nationality of another European Union member state, are not eligible for applications at ENISA due to the fact that they do not fulfil the requirements of Article 12.2 of the Conditions of Employment of Other Servants, namely that they do not hold the nationality of an EU Member State.
[7] Iceland, Liechtenstein, Norway, and Switzerland.
[8] Prior to the appointment, the successful candidate will be asked to provide a certificate issued by a competent Member State Authority attesting the absence of any criminal record.
[9] Before appointment, the successful candidate shall be medically examined in line with the requirement of Article 28(e) of the Staff Regulations of Officials of the European Communities.

- Have a level of education which corresponds to completed university studies of at least three years attested by a diploma[10], OR, where justified in the interest of the service, professional training of an equivalent level[11] with at least 3 years of relevant professional experience, OR proven knowledge and skills corresponding to profiles of ECSF[12];
- Thorough knowledge of one of the official languages of the European Union (at C1 level) and a satisfactory knowledge of another official European language of the Union (at B2 level) to the extent necessary for the performance of their duties[13].

3.2 SELECTION CRITERIA

Only eligible candidates, who fulfil the above eligibility criteria, will be further assessed by the Selection Board against the selection criteria, solely based on the information provided by the candidates in their application form and the talent screening questions. Candidates must provide concrete results and/or actions they undertook in demonstrating the below criteria and their relevant competencies in their application form.

Candidates must demonstrate and will be assessed on the skills and competencies listed below. In their application, candidates should indicate (and provide evidence) on which of the skills listed below they possess. It is important to note that ENISA does not expect applicants to possess all these skills but to indicate the ones they possess and can demonstrate that they suit one or more of the areas covered under the Work Activity areas mentioned above:

Technical skills and experience for the different post profiles

- Demonstrable experience and knowledge in cybersecurity analysis, risk assessment, or security assurance with EU or international cybersecurity standards and frameworks;
- Demonstrable experience in supporting or assessing certification, conformity assessment, or auditing activities;
- Demonstrable experience in analysing cyber threats, vulnerabilities, and system security;
- Demonstrable experience contributing to EU cybersecurity policy, regulatory implementation, or technical guidance;
- Demonstrable experience producing high-quality technical or analytical reports;
- Demonstrable experience working with multiple stakeholders in complex or international environments;
- A strong command of English (oral and written) at a minimum C1 level, with the ability to communicate complex topics clearly and professionally.

Examples of technical skills and experience (not exhaustive), are provided below:

- Proficiency in penetration testing methodologies, tools, and techniques, with the ability to understand and validate the findings and recommendations made in the provided reports.
- Strong understanding of cybersecurity principles, technical controls, common vulnerabilities, threats, tactics, techniques and attack vectors, enabling the identification and assessment of the reported security issues in the provided reports.
- Ability to create training material and operating manuals for the service providers.

[10] Only diplomas issued by EU Member State authorities and diplomas recognised as equivalent by the relevant EU Member State bodies are accepted. If the main studies took place outside the European Union, the candidate's qualification must have been recognised by a body delegated officially for the purpose by one of the European Union Member States (such as a national Ministry of Education) and a document attesting so must be submitted if you have been invited for an interview. This will enable the selection board to assess accurately the level of the qualifications. Diplomas awarded in the UK until 31/12/2020 are accepted without further recognition. For diplomas awarded after this date (from 01/01/2021), a NARIC recognition is required: https://www.enic-naric.net/. Candidates must meet this requirement on the closing date for applications.

[11] Professional accredited training certification (following an exam) such as but not limited to: PMP, CISSP, SANS trainings, ISACA trainings, etc.

[12] European Cybersecurity Skills Framework Role Profiles — ENISA (europa.eu)

[13] Please note that the minimum levels required above must apply to each linguistic ability (speaking, writing, reading and listening). You must have knowledge of at least two official EU languages: language 1 at minimum C1 level (thorough knowledge) and language 2 at minimum B2 level (satisfactory knowledge). These abilities reflect the Common European Framework of Reference for Languages: https://europass.cedefop.europa.eu/resources/european-language-levels-cefr. The official languages of the European Union are: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, and Swedish. The languages referred to in Article 129(1) of the EEA Agreement shall also be considered as languages of the Union.

- Good understanding of IT service management frameworks (e.g. ITIL, ISO/IEC 20000) and experience applying them to operational or service delivery contexts.
- Knowledge of standards and experience in applying them: Deep knowledge of the applicable security requirements, evaluation standards (e.g., ISO/IEC 17065, ISO/IEC 19896), and EU harmonization legislation (such as the CRA) is required.
- Experience with threat intelligence: A thorough understanding of the current cyber threat landscape is essential. This includes knowing common attack vectors, malware analysis techniques, and vulnerability assessment methodologies.
- Experience with EU Cybersecurity Certification Framework (as per CSA, e.g. EUCC) or in general with cybersecurity certification schemes is desirable.
- Experience with eliciting security requirements for complex systems and identifying methodologies and criteria for their auditable evaluation.
- Experience with security analysis: Conducting vulnerability assessments, penetration testing, and code analysis to identify and exploit security weaknesses.
- Experience with risk management: Performing threat modelling and risk evaluations to proactively identify potential threats.
- Experience with network and cloud security: Securing wired and wireless networks, as well as cloud environments and their specific vulnerabilities.
- Experience with advanced and future-proof encryption technologies
- Current understanding and knowledge on new and evolving technologies such as AI / ML in cybersecurity, blockchain security, and Internet of Things (IoT) security to assess future market trends
- Experience with forecasting and trend analysis, desirably on cybersecurity: anticipate future developments based on current data and trends, informing security recommendations and identifying emerging market segments.
- Proficiency with project management and service management methodology (PMP or similar).
- Critical thinking combined with ability to perform data collection, analysis and create reports including use of tools (e.g., Power BI or similar) to generate statistics and analysis.
- Ability to synthesise the progress and prepare short briefings on the progress of the project or programme
- Relevant training (e.g., SANS courses or similar) and/or certifications (e.g., CISSP, CISM) is considered advantageous.
- Familiarity with the handling of classified/sensitive information.
- Experience in engaging/guiding contractors in order to ensure the expected quality.

Personal qualities

- **Adaptability & growth orientation:**

  Demonstrate flexibility, proactive problem-solving, and the ability to learn from feedback and evolving regulatory contexts. Self-motivated and organised, able to manage tasks independently and make autonomous decisions. Able to determine priorities, results-oriented, showing accuracy and autonomy in performing assigned tasks, handle confidential matters responsibly, and meet deadlines under pressure. Able to self- reflect and learn from failures, experiment and demonstrate an ‘agile’ mindset (being agile). Ability to think critically and advise stakeholders accordingly, ability to be resourceful and solve problems constructively.

- **Collaborative & service focus:**

  Build effective working relationships, support colleagues with clear and professional communication, and contribute to a positive, client-focused environment. Able to manage upwards and manage expectations in a timely manner. Experience working in small teams with multiple stakeholders, demonstrating effective coordination and inter-institutional cooperation. Able to maintain professional composure and demeanour and

enhance and promote the unit's vision and goals. Aptitude for working in a multidisciplinary, multicultural and fast paced environment.

Core competences

Required competences: Foundation or higher

- Cybersecurity technical competence: Intermediate
- Network and community development: Foundation
- Data analytics and reporting: Foundation
- Policy advising: Foundation
- Communication: Foundation

In addition, the successful candidate should act and abide by ENISA's core values. An outline of the ENISA's core values, as well as a full description of the **ENISA's competencies** is available here.

NB: Candidates will be assessed in line with the ENISA's 5 competences and above selection criteria. Candidates are advised to demonstrate with concrete examples in their application how they possess the above competences at the required level.

4. SUBMISSION OF APPLICATIONS

To apply for this vacancy, please use ENISA's e-recruitment system, complete all required sections of the application and submit it. ENISA does not accept applications submitted by e-mail, mail or any other means. The application must be submitted in the English language, which is the working language of ENISA.

Candidates must send their application within the set deadline. In order to be considered, applications must be received **by 23:59:59 EET (Greek time (CET+1))** on the closing date. Once you have submitted your application, you will receive an automatic e-mail message confirming receipt of your application. Please ensure that the email address you provide for your applicant account is correct and that you check your email and spam/junk folders regularly.

Applicants are strongly advised to submit their applications well in advance of the deadline, since heavy internet traffic or fault with the internet connection could lead to difficulties in last-minute submission. ENISA cannot be held responsible for any delay related to internet connection issues etc.

At this stage of the selection procedure, candidates are not required to send any additional supporting documents with the application (i.e., copies of your ID-card, educational certificates, evidence of previous professional experience etc.). For any questions on the recruitment process or other technical issues, feel free to reach out via email to recruitment@enisa.europa.eu.

5. SELECTION PROCEDURE

A Selection Board is appointed by the ENISA Executive Director. The names of the Selection Board members (and/or observers, if applicable) are published on the ENISA website, once the Selection Board is established. It is strictly forbidden for the candidates to make any contact with the Selection Board, either directly or indirectly. Any infringement to this rule will disqualify the candidate from the competition.

The selection procedure comprises of three consecutive phases:

5.1 PHASE 1 – PREPARATORY PHASE & SCREENING OF APPLICATIONS

Each Selection Board member (including the observer(s), should there be any one) signs a declaration with regard to confidentiality. The Selection Board's work and deliberations are bound by the principle of confidentiality as per Article 6 of Annex III of Staff Regulations. The Selection Board adheres strictly to the conditions of admission laid down in the vacancy notice.

Before having access to candidates' applications, the Selection Board pre-decides on the assessment methodology under each stage of the selection process: expected indicators and marks on how candidates' applications will be assessed, interview and written test questions and duration, expected indicators and thresholds for the respective assessments, along with the reserve list ceiling.

Once having access to applications, the members of the Selection Board fill in a declaration with reference to conflict of interest and confirm that they have no conflict of interest or bias whatsoever in regard to the individual candidates.

All applications received are checked against the eligibility criteria set out in the vacancy notice.

5.2 PHASE 2 - EVALUATION OF APPLICATIONS

Only eligible candidates will be further assessed by the Selection Board against the selection criteria and competences outlined in the vacancy. Candidates admitted to a previous selection procedure will not be automatically eligible.

The selection process will be based on the assessment of candidates' merits against the criteria and competences outlined in the vacancy. Therefore, candidates are recommended to give evidence of their knowledge and professional experience by using specific examples and/or detailed professional experience, specific skills, knowledge and competences in their application, in order to be evaluated in the best possible way. Selection will be made solely on the basis of the candidate's information provided in the application and the talent screening questions.

The Selection Board will carry out an objective assessment of the candidates' merits. Should the Selection Board discover at any stage in the procedure that the candidate does not meet one or more of the general or special conditions for admission to the selection procedure, or that the information on the application form does not correspond to the supporting documents, the candidate will be disqualified.

5.3 PHASE 3 – SHORTLISTING

The applicants, who obtained the highest number of evaluation points in phase 2, are invited to undertake a written test or assignment and interview, aimed at assessing the practical application of the experience and knowledge of the candidates.

Candidates shall be informed that interviews and written tests or assignments may be organised online[14]. Specific instructions will be provided to shortlisted candidates.

An outcome notification will be provided to all candidates who are not invited to the next phase.

The written assignments and interviews are conducted in English. In case English is the mother tongue of an applicant, some interview questions may be asked in the language they indicate on the application form as their second EU

[14] Additionally, candidates shall be informed that the written test may be organised by a third party online and/or may be proctored.

language. Candidates invited for an interview will be required to submit electronically relevant supporting documentation demonstrating their educational qualifications and work experience. Shortlisted candidates may also be required to provide work-related references upon request of the Agency.

5.4 RESERVE LIST

The activity of the Selection Board ends with the drawing of a reserve list of suitable applicants to occupy the position advertised. The reserve list is unranked and is drawn alphabetically. Candidates should note that inclusion in the reserve list does not guarantee recruitment.

In addition, reserve listed candidates may be asked to undergo a second interview prior to any recruitment, for which they will be informed in advance. The interview will focus on the specific match of the candidate for the specific post covering the related motivation, and relevant technical and behavioural competencies.

The reserve list will be valid until **31/12/2029**. Candidates invited to an interview will be informed by e-mail whether or not they have been placed on the reserve list. Upon completion of the selection procedure, all candidates will receive an outcome letter. It may be that other EU Institutions, Agencies or Bodies approach ENISA to request for the CVs of candidates on the reserve list. Candidates, who are on the reserve list, will be informed by HR to inquire if they are interested in a similar post in another agency. If so, they will be invited to send their (updated) resume/CV to the requesting agency. The requesting agency will then contact the candidate for their vacancy.

The Authority Empowered to Conclude Contracts (the Executive Director – ED of the Agency) will ultimately decide on the successful candidate to be appointed to the post, based on the needs of the Agency. The appointed candidates will be asked to fill a specific form informing the Appointing Authority of any actual or potential conflict of interest[15].

If an offer letter is issued, the candidate must undergo a compulsory medical examination to establish that they meet the standard of physical fitness necessary to perform the duties involved and the candidate must provide original or certified copies of all relevant documents that prove the educational and professional qualifications stated in their application.

5.5 SELECTION PROCEDURE TIMELINES

The Agency manages its selection procedures depending on the availability of the Selection Board members and its resource capacity. It is envisaged that the interviews and potential other written assignments will tentatively take place in Q2 2026. Please note that the selection process may take some time to be completed and that no information will be released during this period. The selection procedure status will be displayed on ENISA's career page and applicants are requested to visit regularly the page for update on the procedure.

Due to the Agency's operational requirements, the successful candidate will be required to be available at the shortest possible notice.

6. CONDITIONS OF EMPLOYMENT

The successful candidate(s) will be recruited as member(s) of the contractual staff, pursuant to Article 3(a) of the Conditions of Employment of Other Servants of the European Union. The initial contract will be, in principle, concluded for a period of four (4) years. The contract may be renewed, in principle, for a period of four (4) years. Any further renewal shall be for an indefinite duration. The appointment will be in Function Group FGIV.

Successful candidates, who are offered a contract of employment, will be graded on entry into service in step 1 of the relevant grade (13, 14 or 16 for FGIV). The grade will be determined in accordance with the number of years of professional experience of the successful candidate. In addition, successful candidates, who are recruited, shall undergo an initial probation period of nine (9) months.

The candidates included in this reserve list may be offered an engagement under the conditions stipulated in Article 3a of the Conditions of Employment of Other Servants (CEOS) for Contract Agents, and/or may be offered an employment

[15] In compliance with Article 11 of the Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union.

contract of a shorter / fixed-term duration and/or in a different location (Athens or Brussels) than the one stated in the vacancy notice, in accordance with the business needs and subject to agreement with the candidate. In such cases, for contracts related to Contribution Agreements, the duration of the contract is concluded for a limited, non-renewable period linked to the duration of the Contribution Agreement, including any extensions (even if under a different name within the Programme) and upon budget availability or for a maximum duration of four years, whichever comes first.

The CVs of the candidates in the reserve list might also be shared with other Agencies and EU Institutions or bodies. In any of these cases, the Agency will contact the candidate in the reserve list and ask their interest/approval.

The summary of the financial entitlements is available under "BENEFITS" here.

The salaries of staff members are subject to a Community tax deducted at the source. They are exempt from national tax on salary and staff members are members of the Community social security and pension schemes.

For additional information about salaries, deductions and allowances please consult the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union.

Successful candidates, who have been recruited to a post at ENISA, are required to furnish a valid certificate of good conduct before the start of their employment. The certificate of good conduct must be provided to ENISA prior to the signature of the employment contract. The certificate of good conduct must be issued by the relevant authorities of the country of nationality of the candidate and must not be older than three months at the time of submission to ENISA. ENISA reserves the right not to proceed with the signature of the contract based on the content of the certificate or if the candidate fails to provide the certificate to ENISA.

For specific posts, the successful candidate(s) will be required to hold, or be in a position to obtain, a valid Personnel Security Clearance Certificate (national or EU PSC at SECRET UE/EU SECRET level). Personnel Security Clearance Certificate (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid national or EU Personnel Security Clearance (PSC), and which shows the level of EU Confidential Information (EUCI) to which that individual may be granted access (SECRET UE/EU SECRET), the date of validity of the relevant PSC and the date of expiry of the certificate itself. Note that the necessary procedure for obtaining a PSCC can be initiated on request of the employer only, and not by the individual candidate. ENISA reserves the right to terminate a contract based on the result of the security clearance process.

7. EQUAL OPPORTUNITY

As a European Union Agency, ENISA is committed to providing equal opportunities to all its employees and applicants for employment. As an employer, ENISA is committed to ensuring gender equality and to preventing discrimination on any grounds. It actively welcomes applications from all qualified candidates from diverse backgrounds, across all abilities, without any distinction on any ground such as sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age, marital status or other family situation or sexual orientation, and from the broadest possible geographical basis amongst the EU Member States. In particular, ENISA encourages the applications of women for the positions where they are currently under-represented.

If you have a disability or medical condition that may hinder ability to sit the interview or written test, please indicate this in your application and let us know the type of special arrangements you need. If the disability or medical condition is developed after the deadline for the applications, you must notify us via email to recruitment@enisa.europa.eu. Overall, ENISA strives to select recruit, develop and retain, diverse talent workforce.

8. REQUESTS, COMPLAINTS AND APPEALS

Candidates, who consider that their interests have been prejudiced by any decision related to the selection procedure, can take the following actions:

8.1 REQUESTS FOR FEEDBACK:

Candidates to a selection procedure can request feedback regarding their results **within ten (10) calendar days** from the communication of their results. They should expect to receive an answer from ENISA at the latest within fifteen (15) working days from the request. Please note that the request for feedback does not extend the deadlines to submit a request for internal review or administrative complaint under Article 90(2) of the Staff Regulations.

Candidates should send an email to the following email address recruitment@enisa.europa.eu by clearly indicating on the subject line: "Request for feedback of (name of candidate) for the vacancy notice reference number (vacancy notice reference number)" and clearly stating their request on the content of the email.

8.2 REQUESTS FOR INTERNAL REVIEW OF THE DECISIONS TAKEN BY THE SELECTION BOARD:

Candidates, who feel that an error has been made in relation to their non-admission to the selection procedure (i.e., not eligible) or to their exclusion from the selection procedure (i.e., not invited for an interview/written test) may request a review **within ten (10) calendar days** from the date on which they are notified about the decision. Requests for internal review may be based on one or more of the following reasons:

i) a material irregularity in the competition process;
ii) non-compliance, by the Selection Board or ENISA, with the Staff Regulations and relevant implementing rules, the vacancy notice, its annex and/or case-law.

We bring to your attention that candidates are not allowed to challenge the validity of the Selection Board's assessment concerning the quality of their performance in a test or the relevance of their qualifications and professional experience. This assessment is a value judgment made by the Selection Board and disagreement with the Selection Board evaluation of the tests, experience and/or qualifications does not prove that it has made an error. Requests for review submitted on this basis will not lead to a positive outcome.

Candidates should send an email to the email address recruitment@enisa.europa.eu, clearly indicating on the subject line: "Request for internal review (name of candidate) for the vacancy notice reference number (vacancy notice reference number)". The candidates shall clearly indicate the decision they wish to contest and on what grounds. **Requests received after the deadlines will not be taken into account.**

Candidates having requested a review will receive an acknowledgment of receipt within fifteen (15) working days. The instance, which took the contested decision (either the Selection Board or ENISA), will analyse and decide on the requests and candidates will receive a reasoned reply in accordance with ENISA's Code of good administrative behaviour as soon as possible. If the outcome is positive, candidates will be re-entered in the selection procedure at the stage at which they were excluded, regardless of how far the selection has progressed in the meantime.

8.3 ADMINISTRATIVE COMPLAINTS:

Candidates to a selection procedure, who consider they have been adversely affected by a particular decision of the Selection Board, have the right to lodge an administrative complaint, within the time limits provided for, under Article 90(2) of the Staff Regulations to the Executive Director of ENISA. A complaint can be submitted against any decision, or lack thereof, that directly and immediately affects the legal status as a candidate. Candidates should note that a complaint to the Executive Director against a decision of the Selection Board cannot result in overturning a value judgment made by the latter related to the scores given to candidates' assessment of the relevance of their qualifications and professional experience and of their performance in a test.

Candidates shall submit an email to the following email address recruitment@enisa.europa.eu by clearly indicating on the subject line: "Complaint under Article 90(2) of the SR of (name of candidate) for the vacancy notice reference number (vacancy notice reference number)". Complaints shall be addressed to the Executive Director of ENISA, Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri 15231, Attiki, Greece. The complainant shall indicate clearly the decision they wish to contest and on what grounds. Complaints received after the deadline will not be taken into account.

8.4 JUDICIAL APPEALS:

Should the complaint under article 90(2) be rejected, candidates to a selection procedure have the right to submit a judicial appeal to the General Court, under Article 270 of the Treaty of the Functioning of the European Union and Article 91 of the Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union. Please note that appeals against decisions taken by ENISA will not be admissible before the General Court, unless an administrative complaint under Article 90(2) of the Staff Regulations has first been submitted and rejected by express decision or by implied decision.

The General Court has consistently held that the wide discretion enjoyed by Selection Boards is not subject to review by The General Court, unless rules, which govern the proceedings of Selection Boards, have been infringed. For details on how to submit an appeal, please consult the website of the Court of Justice of the European Union: http://curia.europa.eu.

8.5 EUROPEAN OMBUDSMAN:

All EU citizens and residents can make a complaint to the European Ombudsman pursuant to Article 228 (1) of the Treaty on the Functioning of the European Union, as well as the Statute of the Ombudsman and the implementing Provisions adopted by the Ombudsman under Article 14 of the Statute. Before submitting a complaint to the Ombudsman, candidates must first make the appropriate administrative approaches to the institutions and bodies concerned.

Please note that complaints made to the Ombudsman have no suspensive effect on the period laid down in Articles 90 (2) and 91 of the Staff Regulations for lodging complaints or for submitting appeals to the General Court pursuant to Article 270 of the Treaty of the Functioning of the European Union. Please note also that 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 the institutions and bodies concerned.

For details of how to submit a complaint, please consult the website of the European Ombudsman: http://www.ombudsman.europa.eu.

9. DATA PROTECTION

All personal data shall be processed in accordance with Regulation (EU) No 2018/1725 of the European Parliament and of the Council (OJ L 295, 21.11.2018, p. 39–98) 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. ENISA is supervised by EDPS, http://www.edps.europa.eu . For any further enquiries you may contact the Data Protection Officer at: dataprotection@enisa.europa.eu.

Candidates are invited to consult the privacy statement, which explains how ENISA processes personal data in relation to recruitment selection.