European Union Agency for Cybersecurity (ENISA)
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece | info@enisa.europa.eu | www.enisa.europa.eu

Vacancy Notice

Lead Cybersecurity Digital Trust Expert
Ref. ENISA-TA-AD12-2026-08

Type of contract	**Temporary Agent**
Function group and grade	AD12
Duration of contract	4 years, renewable
Area	Market Technology and Product Security (MTPS) Unit
Place of employment	Athens
Probation period	9 months
Reserve list	31/12/2029
Deadline for applications	05/06/2026 23:59:59 EEST[1] (CEST[2] +1)

The European Union Agency for Cybersecurity (ENISA) seeks to recruit motivated, dynamic, flexible and highly qualified staff to support its mission and contribute to the development of the Agency. ENISA's staff are expected to be reasonably mobile in order to respond to the needs of the Member States on the basis of planned as well as ad hoc needs.

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[3].

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] Eastern European Summer Time
[2] Central European Summer Time
[3] Regulation (EU) 2019/881 - Cybersecurity Act: http://data.europa.eu/eli/reg/2019/881/oj

2. The Unit

The Market, Technology and Product Security Unit (MTPS) contributes to fostering the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular for SMEs and start-ups, to reduce dependence from outside and increase the capacity of the Union and to reinforce supply chains to the benefit of the internal market. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation and the adoption of relevant codes of conduct. As such this activity also seeks to lay the ground for an effective role for ENISA in the CRA, notably in terms of market analysis, the preparation of market sweeps, and the collection and analysis of information for the identification of emerging cybersecurity risks in products with digital elements, etc.

Secondly, the Unit contributes to producing analyses and guidelines as well as good practices on cybersecurity and data protection requirements, including eIDAS2 and trust services, facilitating the establishment and take up of European and international standards across applicable areas such as risk management as well as performing regular analyses of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities as well as incidents that have occurred.

Third, the Unit works closely with the Cybersecurity Certification Unit to promote conformity assessment across different legislative streams and in this respect the focus is currently on the development of EU and national cybersecurity certification schemes for digital identity wallets.

The unit comprises one sector covering aspects of market, technology and product security and is in close collaboration with the Cybersecurity Certification Unit, both managed by the same Head of Unit.

3. The job

ENISA is seeking to draw a reserve list from which one Lead Cybersecurity Digital Trust Expert will be recruited, with a place of assignment in Athens, Greece. The established reserve list may also be used to cater for other senior level Agency wide staffing needs, with the place of assignment in Athens, Greece.

The Lead Cybersecurity Digital Trust Expert shall support the Agency and the Cybersecurity Certification Unit in coordinating horizontal operational and strategic matters across the different areas of work of MTPS, ensuring alignment with the work of the Cybersecurity Certification Unit and other policy areas and in representing the Agency in relevant stakeholder engagements. In particular, the job holder shall:

- Advise MTPS HoU and support with ENISA's role in the Cyber Resilience Act (CRA) through market analysis, market sweeps, and risk identification in products with digital element, establishing alignment and coordination with European Cybersecurity Certification Framework and the schemes therein, notably EUCC;
- Lead the promotion and implementation of security by design and security by default in ICT products, services, and processes, including via standardization and/or technical specifications;
- Promote the adoption and visibility of secure and trustworthy ICT solutions within the EU Digital Single Market;

- Lead cybersecurity digital transformation initiatives, incorporating ENISA cybersecurity market analyses, strategic foresight and emerging cybersecurity trends, with the aim of fostering EU cybersecurity market competitiveness;
- Promote a consistent and harmonized conformity assessment strategy across relevant product, services, processes policy initiatives and NLF and charter ENISA's roadmap in supporting the stakeholders' communities and the ecosystem;
- Strengthen partnerships with the private sector and foster collaboration across EU cybersecurity market actors, also promote coordination and stakeholder engagement across the relevant policy ecosystem, including but not limited to CRA Market Surveillance Authorities, Notifying Bodies, European Cybersecurity Certification Framework stakeholders, Conformity Assessment Bodies, Certification Bodies, etc.;
- Ensure consistent coordination, communication and outreach across cybersecurity digital trust communities (notably related to European Cybersecurity Certification Framework, Cyber Resilience Act, etc) on behalf of the MTPS HoU;
- Represent the HoU MTPS in stakeholder engagements and statutory commitments (e.g. CRA Expert Group, CRA ADCO, etc).

4. Qualifications and experience required[4]

4.1 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[5] or EFTA[6] countries;
- Be entitled to their full rights as a citizen[7];
- 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[8];
- Have a level of education which corresponds to completed university studies of at least four (4) years attested by a diploma[9], OR have a level of education which corresponds to

[4] 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.
[5] 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.
[6] Iceland, Liechtenstein, Norway, and Switzerland.
[7] 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.
[8] 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.
[9] Only diplomas issued by EU M ember 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

completed university studies of at least three (3) years attested by a diploma and, after having obtained the university diploma[10], at least one year of appropriate professional experience;

- In addition to the above, at least 15 years of proven full-time professional experience[10] relevant to the duties concerned after the award of the university degree, out of which at least 10 years' experience in a managerial position (Head of Sector/Unit/Department or equivalent) covering cybersecurity certification OR product security OR cybersecurity digital trust or related fields;

- 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[11].

4.2 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 following skills and competencies:

Strategic advisory and coordination skills

- Track-record of providing impactful strategic policy advice to policy makers, coupled with an ability to translate complex technical topics to high added-value policy recommendations;
- Excellent ability to represent the strategic interest of an organisation within a varied stakeholder environment with a capacity to develop and maintain excellent relationships with national cybersecurity authorities (preferably focusing on cybersecurity certification and/or market surveillance and/or product security), with the Commission and other EU Institutions, bodies and agencies;
- Proven capacity to motivate and coordinate the work of a number of staff members simultaneously.

Specialist skills and experience

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.

[10] Professional experience connected with the Agency's areas of activities shall be taken into account and is counted only from the time the candidate obtained the certificate or diploma required for admission to the selection procedure.

[11] 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 Ref erence 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.

- In depth experience with and knowledge of cybersecurity principles, policies at EU and national level and key technological, market and digital transformation aspects;
- Proven understanding and ability to address the challenges facing Member States in applying EU cybersecurity policies and legislation in the area of product security and/or cybersecurity certification (e.g. CRA, RED, CSA/ECCF, EUCC);
- Proven experience with conformity assessment procedures, accreditation, standardisations and relevant stakeholder ecosystem.

Personal qualities

- A growth-orientated mindset with strong self-drive (work independently) and ability to change;
- A cooperative and can-do approach to achieving the Agency's mission in close cooperation with the Member States and the EUIBAs;
- Strong communication and inter-personal skills with the ability to communicate efficiently with internal and external stakeholders, drive internal and external negotiations with a view to building consensus;
- Excellent analytical skills, capacity to identify key points from large data sets, develop and generate strategic goals and translate them into practical proposals for action.

Core competences

Required competences:

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

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.

5. 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 (CEST+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.

6. Selection procedure

A Selection Board is appointed by the ENISA Executive Director. The name 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:

6.1 Phase 1 – Preparatory phase & screening of applications

Each Selection Board member (including the observer(s), should there be any), 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.

6.2 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.

6.3 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[12]. 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 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.

6.4 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.

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

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 request 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 (ED) 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[13].

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.

6.5 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 take place in quarter three of 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.

7. Conditions of employment

The successful candidate(s) will be recruited as member(s) of the temporary staff, pursuant to Article 2(f) 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. After at least 2 years in grade (and provided that the performance is satisfactory), the successful candidate could be reclassified as Adviser AD13[14].

If a successful candidate from the external selection procedure is already a member of temporary staff 2(f) in another EU Agency, the relevant provisions of the Management Board decision 2016/12 on the general implementing provisions on the procedure governing the engagement and use of temporary staff under Article 2(f) of the CEOS will apply.

Successful candidates, who are offered a contract of employment, will be graded on entry into service in step 1 or 2 of the relevant grade (AD12). The step will be determined in accordance with the number

[13] In compliance with Article 11 of the Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union.
[14] Decision No MB/2018/7 of the Management Board of the European Union Agency for Network and Information Security (ENISA) adopting Implementing rules concerning the function of adviser

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.

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.

The certificate of good conduct does not substitute a valid security clearance required for ENISA staff. Failure to obtain the requisite security clearance in reasonable time may be cause for termination of the employment contract. ENISA may at any time terminate the employment contract if the result of the security screening is not positive and the necessary clearance level is not granted or extended.

The requested level of security clearance for this post is: **SECRET UE/EU SECRET**.

The candidates included in this reserve list may be offered an employment contract of a different/shorter 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.

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

The salaries of staff members are subject to a Community tax deducted at 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.

8. 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.

9. 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:

9.1 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 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.

9.2 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.

Please note 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.

9.3 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 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.

9.4 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.

9.5 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.

10. 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 selections.