

**Vacancy notice and establishment of a reserve list
for the post of Local Cybersecurity Officer
(Contract Agent – Function Group IV)
Ref. BEREC/2025/03**

Function group and grade	Contract Agent FG IV
Duration of contract	3 years (with the possibility of extension)
Place of employment	Riga, Latvia
Deadline for applications	24/10/2025 at 12:00 (midday), Riga time

Applications are invited for the vacancy and establishment of a reserve list for the post of Local Cybersecurity Officer at the Agency for Support for BEREC.

1. Agency for Support for BEREC ('BEREC Office', 'Agency')

The BEREC Office, an Agency of the European Union located in Riga, Latvia, offers a unique opportunity to be part of a dedicated team of professionals contributing to the future of digital communications in Europe. As the EU Agency supporting BEREC – the Body of European Regulators for Electronic Communications – the BEREC Office plays a significant role in facilitating the consistent development and implementation of electronic communications regulation across the EU. It is achieved by delivering high-quality administrative and professional support, guided by the core values of professionalism, efficiency, effectiveness, accountability, teamwork, and diversity.

Working in a highly professional, dynamic, and international environment, staff at the BEREC Office collaborate closely with national regulatory authorities (NRAs) and the European Commission to help ensure that Europe's telecom markets remain competitive, fair, and fit for the future. The work is diverse and forward-looking, encompassing the collection and exchange of information from NRAs, the dissemination of regulatory best practices, support to the BEREC Chair, and the coordination of Expert Working Groups. Staff also manage administrative, financial, procurement, and ICT tasks, as well as support communications and organise high-level meetings and events.

The BEREC Office offers a stimulating professional setting where the main asset of the organization is people, where innovation and expertise are valued, and supported through

continuous learning and development opportunities. Employees benefit from the attractive working conditions of EU institutions, including attractive remuneration, comprehensive social security coverage, and a strong work-life balance - all while living and working in Riga, a vibrant, dynamic, and welcoming European capital.

For further information about BEREC or the BEREC Office, please visit our website: <https://www.berec.europa.eu/en>

2. The post

The job holder will be responsible, among others, for the following tasks:

- Identify, assess, and mitigate cybersecurity risks in accordance with Regulation (EU, Euratom) 2023/2841;
- Conduct regular cybersecurity risk assessments, develop and implement risk mitigation strategies to address identified risks;
- Report on risk management activities to senior management;
- Ensure compliance with all relevant cybersecurity regulations and standards;
- Develop and maintain cybersecurity governance frameworks, policies, and procedures, in line with Regulation (EU, Euratom) 2023/284;
- Ensure compliance with all relevant cybersecurity regulations and standards;
- Define security measures by evaluating business strategies and requirements and implement security solutions that protect the organization against cyber threats;
- Develop and implement incident response plans to address and manage cybersecurity incidents;
- Coordinate with relevant stakeholders to ensure timely and effective response to incidents;
- Conduct post-incident analysis and reporting to identify lessons learned and improve incident response processes;
- Promote cybersecurity awareness and provide training to employees on best practices and regulatory requirements. Foster a culture of security within the organization;
- Develop and deliver cybersecurity awareness training programs and provide regular updates and best practices on emerging cybersecurity threats;
- Monitor the organization's information systems for security breaches and vulnerabilities;
- Work closely with IT, management, and other departments to ensure a holistic approach to cybersecurity;
- Acting as the contact point for external counterparts, such as the Cybersecurity Service for the Union entities (CERT-EU), the Interinstitutional Cybersecurity Board (IICB), and act as the primary point of contact for cybersecurity matters within the BEREC Office.

The above tasks and responsibilities will be conducted mainly in the English language.

The jobholder will work under the supervision of his/her line manager at the BEREC Office located in Riga, Latvia and may be assigned other duties appropriate to the grade in the interest of the service.

3. Eligibility criteria

Candidates will be eligible for this selection procedure if they fulfil the following formal criteria at the time of the application deadline:

- 3.1. Be a national of a Member State of the EU and enjoy his or her full rights as a citizen;
- 3.2. Have fulfilled any obligations imposed by applicable laws concerning military service;
- 3.3. Be physically fit to perform the duties linked to the post¹;
- 3.4. Produce the appropriate character references as to suitability for the performance of the duties²;
- 3.5. Languages: Have a thorough knowledge of one of the official EU languages and a satisfactory knowledge of a second EU language to the extent necessary for the performance of his/her duties;
- 3.6. Qualifications and work experience: Completed university studies of at least three years attested by a diploma.

4. Selection criteria

If the eligibility criteria set out in the section “Eligibility criteria” are met, the candidates’ application forms, CVs and motivation letters will be evaluated on the basis of the selection criteria below. The most suitable candidates will be invited to an interview and written test.

When filling in the application form, candidates are expected to include elements that demonstrate that their profile matches the requirements below.

4.1. Essential:

- 4.1.1. One year of relevant professional experience in relation to the tasks assigned to the post;
- 4.1.2. Knowledge in the area of cloud architectures and security as well as data protection regulations;
- 4.1.3. Knowledge in the area of cybersecurity risk management, governance, and compliance;
- 4.1.4. Knowledge of Regulation (EU, Euratom) 2023/2841 and other relevant cybersecurity regulations and standards;
- 4.1.5. Thorough knowledge of written and spoken English.³

¹ Before being hired, a contract agent shall be medically examined by one of the institution's medical officers to verify if (s)he fulfils the requirements of the Conditions of employment of other servants of the EU.

² Prior to appointment, successful candidates will be asked to provide a certificate issued by a competent authority attesting the absence of a criminal record.

³ Level C1 or above of the Common European Framework of Reference for Languages (CEFR). As established in the BEREC Office Management Committee Decision MC/2016/02, the working language of the BEREC Office is English.

4.2. Advantageous:

- 4.2.1. Experience with cybersecurity frameworks such as ISO/IEC 27001, NIST, or similar;
- 4.2.2. Proven knowledge of security architecture reference models and security solutions;
- 4.2.3. Experience working in a CSIRT (Computer Security Incident Response Team).

4.3. Evaluation during interviewing and written test process

Candidates invited to the interview and written test will be evaluated based on their professional and personal competencies, as well as their knowledge of English the working language and their motivation and commitment to work for the BEREC Office in Latvia.

5. **Stages in the selection procedure**

The BEREC Office sets up a Selection Committee. This Committee will make a comparative assessment of all eligible applications, and identify a number of candidates whose profiles best match the selection criteria listed above. These candidates will be invited for a written test and an interview with the Selection Committee.

The selection procedure will be organised in accordance with the following steps:

5.1. Admission to the selection procedure

After the deadline for applications, the complete applications submitted (application forms, CVs and motivation letters) will be checked against the eligibility criteria. Only eligible applications will be then assessed against the selection criteria (essential and advantageous).

5.2. Assessment of eligible applications

The Selection Committee will analyse the motivation letters, together with the application forms and the CVs of eligible applicants with reference to the elements indicated in the selection criteria section (essential and advantageous). In addition, the Selection Committee will assess the motivation and the overall suitability of each eligible application on the basis of the requirements of the post.

5.3. Interview and written test

Upon completion of the assessment of eligible applications, the most suitable candidates will be invited for a written test and an interview. The maximum number of candidates invited to attend the interview and written test will be 12⁴. The interview and written test may take place either remotely or at the Agency's seat in Riga. The practicalities about the interview and written test will be communicated in writing to the candidates invited to attend the written test and interview.

Candidates are kindly invited to indicate in their application any special arrangements that may be required, if invited to attend the written test and interview.

The interview will aim to assess the suitability of the candidates to perform their duties, their

⁴ Where a number of candidates tie for the last available place in the list of candidates to be invited for interviews, they will all be invited.

professional knowledge, their skills and competencies relevant to the post and their motivation. The interview shall cover an analysis of the language abilities and the personal and professional competences of each applicant. The interview will be held in English. Candidates with English as their mother tongue will be tested in another official EU language to check that the eligibility criteria is met (i.e. satisfactory knowledge of a second official EU language).

The written test will be in English. It will be related to the tasks and responsibilities related to the post, and be designed to test candidates' ability to communicate in written English, and their job-related knowledge and competences.

The content of the questions asked during the interviews will be set in accordance with the level and profile of the position advertised.

6. Outcome of the selection procedure

On the basis of the outcome of the interviews and written tests, the Selection Committee will propose to the Director of the BEREC Office to offer the job to the successful candidate.

The Selection Committee may also establish a reserve list of approximately five suitable candidates to be approved by the Director of the BEREC Office with a validity until 31 December 2026. This reserve list may be used for filling in the post of Local Cybersecurity Office in the future or other posts with similar profiles at the BEREC Office⁵. In the context of the inter-agency cooperation, the reserve list may also be shared with other EU Agencies in case of service needs. The validity of the reserve list may be extended.

Inclusion in the reserve list does not imply any entitlement to employment at the BEREC Office.

7. Verification of documents and scrutiny

Before recruitment, the information provided in the applications of the successful candidates will be checked against the supporting documents to confirm its accuracy and eligibility.

If, at any stage in the procedure, it is discovered that the information given in an application has been knowingly falsified, the candidate will be disqualified from the selection process.

Candidates will also be disqualified if they:

- do not meet all eligibility criteria;
- do not provide all the required supporting documents, including to substantiate the facts and statements in their applications.

8. Conditions of employment

The Local Cybersecurity Officer will be hired as a contract agent in function group IV pursuant to Article 3a of the Conditions of employment of other servants of the European Communities for a period of three years. The duration of the employment contracts maybe renewed

⁵ The CVs and motivation letters of the candidates on the reserve list will be assessed towards the requirements of the vacant post. A second interview with the AACC and/or one or more delegated staff member(s) may be organised.

according to the modalities of the relevant general implementing rules of the BEREC Office. The period of engagement cannot exceed the lifetime of the BEREC Office.

The remuneration of the staff members consists of a **basic salary** and possible allowances paid in Euro weighted down by the correction coefficient for Latvia currently 84,1%. Both the remuneration and the correction coefficient are subject to annual revision.

In the table below there is a projection of the monthly remuneration for a staff member who has two dependent children:

Function group and grade	FGIV, grade 13 less than 5 years of documented professional experience	FGIV, grade 14 Between 5 and 17 years of documented professional experience	FGIV, grade 16 More than 17 years of documented professional experience
Basic net salary	4,319.72 EUR	4,887.55 EUR	6,256.88 EUR
Household allowance	320,57 EUR	331.93 EUR	359,32 EUR
Dependent child allowance for two dependant children	1,023.42 EUR	1,023.42 EUR	1,023.42 EUR
Expatriation allowance ⁶	906.19 EUR	998.86 EUR	1,222.34 EUR
Total net (after all deductions, contributions and taxes are applied)	4,934.90 EUR	5390.19 EUR	6,464.82 EUR

In addition to the monthly remuneration, the BEREC Office pays the full tuition costs for enrolment of dependent children in international schools accredited in Latvia where the language of tuition can be English, French or German. Currently the BEREC Office has concluded 6 agreements with different international schools accredited in Latvia.

Under certain circumstances, in particular where the selected candidate is obliged to change his/her place of residence in order to take up employment, the Agency may reimburse some expenses incurred, notably removal expenses.

From the commencement of employment staff members are covered against sickness and accident through the EU Joint Sickness Insurance Scheme.

More detailed information on the working conditions can be found [here](#).

9. Application procedure

9.1. Submission of applications

For their applications to be valid, candidates must submit:

1. A covering letter outlining their reasons for applying;
2. A curriculum vitae (CV), preferably drafted using the Europass CV format⁷;

⁶ An expatriation allowance equal to 16 % of the total of the basic salary shall be paid to:

- staff who are not and have never been nationals of Latvia, and who have not habitually (during period of 5 years ending 6 months before entering into service) lived or carried out their main professional activity in the territory of the Latvia;
- staff who are or have been nationals of Latvia and who have habitually resided (during the 10-year period ending when they entered into service) outside Latvia, for a reason other than the performance of duties in the service of Latvia or in an international organisation.

⁷ The Europass CV can be downloaded from the website <http://europass.cedefop.europa.eu>.

3. The application form in the annex.

Applicants are explicitly requested to highlight and give a brief account of their experience and expertise relevant to the job (incl. the start and end dates of employment contracts). Applicants are invited to indicate, apart from the duration of studies, the legal length of the diplomas that they hold.

Applications will not be assessed if the dossier is incomplete or submitted after the deadline.

Supporting documents (e.g. certified copies of degrees/diplomas, diploma supplement, references, proof of experience, etc.) should not be sent at this point but must be submitted at a later stage of the procedure, when requested.

Applications, preferably in English, should be sent only by e-mail to: recruitment@berec.europa.eu.

The reference (BEREC/2025/03 Local Cybersecurity Officer) must always be indicated in the subject line of e-mails.

Candidates are asked to report any potential change of address in writing without delay to the address above.

9.2. Closing date for applications

Applications must be sent by email. The deadline is **24/10/2025 at 12:00 (midday) Riga time** (11:00 a.m. Central European Time). The Agency strongly advises candidates not to wait until the last few days before the deadline to apply. It is the sole responsibility of each applicant to submit his/her completed application by the deadline for submission. Any information or documentation provided after the deadline will not be taken into account.

9.3. Approximate timetable

The selection process may take several months; information will be released at the end of each stage.

10. Equal opportunities

The BEREC Office applies a policy of equal opportunities and non-discrimination in accordance with Article 1d of the Staff Regulations.

11. Protection of personal data

The BEREC Office respects the privacy of its candidates and processes their personal data as required by [Regulation \(EU\) 2018/1725](#). For more information please follow this [link](#).

12. Requests for information

Any applicant who would like further information, or considers that (s)he has grounds for a complaint concerning a particular decision may, at any point in the selection procedure, email a request for further information to recruitment@berec.europa.eu.

APPLICATION FORM

FOR THE VACANCY AND ESTABLISHMENT OF A RESERVE LIST FOR THE POST OF
LOCAL CYBERSECURITY OFFICER AT THE BEREC OFFICE

BEREC/2025/03

1. Surname⁸

2. Forename: Title: (e.g. Mr, Ms, Dr)

3. Date of birth: dd/mm/yyyy

4. Gender: Male Female

5. Address for correspondence⁹:

Street, No, etc.:	
Postal code:	Town:
Country:	
Office Telephone N°:	Mobile N°:
E-mail address: Professional:	
E-mail address: Personal:	

⁸ IMPORTANT: your application will be registered under this name. Please use it in all correspondence. Any other name (e.g. maiden name) appearing on diplomas or certificates accompanying this application should be indicated below:

⁹ Please inform recruitment@berec.europa.eu of any change of address.

6. Nationality (please circle or mark):

BE	BG	CY	CZ	DK	DE	EL	ES	EE	FR	HU	HR	IE	IT
LT	LU	LV	MT	NL	AT	PL	PT	RO	FI	SE	SK	SI	

7. University degree:

8. Other studies:

9. Knowledge of languages:

Place the following numbers (1, 2 or 3) in the appropriate box or boxes:

1 - mother tongue or thorough knowledge;

2 - very good knowledge;

3 - satisfactory knowledge.

BG	CZ	DK	DE	EL	EN	ES	EE	FI	FR	GA	HR
HU	IT	LT	LV	MT	NL	PL	PT	RO	SI	SE	SK

Other language(s):

10. Current employer (indicate if you are self-employed or unemployed):

Name	
Address	
Position	

Information to be used for the evaluation of the selection criteria

A. Essential:

11. Please provide an example from a project or responsibility you handled that directly aligns with the requirements of the role of the Local Cybersecurity Officer and explain your knowledge in the area of Regulation (EU, Euratom) 2023/2841 and/or any other relevant cybersecurity regulations and standards (800 words max.):

12. Please explain your knowledge by describing a situation where you had to design or work with a cloud-based system while ensuring compliance with IT security and data protection regulations (800 words max.):

13. Please provide example(s) from a project or responsibility you handled involving one, two, or all the following 3 areas: cybersecurity risk management, governance, and compliance (800 words max.):

B. Advantageous:

14. Please provide an example where you worked with cybersecurity frameworks such as ISO/IEC 27001, NIST, or similar (500 words max.):

15. Please provide an example where you applied a security architecture reference model to design or assess a security solution (500 words max.):

16. Please briefly explain your responsibilities working in a Computer Security Incident Response Team (CSIRT) (500 words max.):

Additional information concerning the application

17. Give details of anything else you consider relevant to your application:

18. If you have a recognised disability, which necessitates any special arrangements in the context of this selection procedure, please indicate below:

19. Declaration:

1. I declare on my word of honour that the information provided above is true and complete and I am aware that any incorrect statement may invalidate my application at any point in the selection process.
2. I further declare on my word of honour that:
 - (i) I am a national of one of the Member States of the European Union and enjoy my full rights as a citizen;
 - (ii) I have fulfilled any obligations imposed on me by laws concerning military service.
3. I undertake to produce on request documents to support my application and accept that failure to do so may invalidate my application.
4. I confirm that I am willing to make complete declarations of any direct or indirect interests that might be considered prejudicial to my independence.
5. If my name will be placed on the reserve list for this selection procedure, I give my consent that in the context of the inter-agency cooperation my name and application form can be shared with other EU Agencies which might contact me in the context of its own staff selection and recruitment procedures.

Date and name:

Signature:

Along with this application form, candidates must submit:

- A covering letter describing the reasons and their motivation for the application
- A CV preferably drafted using the Europass CV format which can be found at: <http://www.europass.cedefop.europa.eu>