VACANCY NOTICE – 2022-IPR-B6-FGIV-021991

Information security officer – Algorithmic transparency

Type of contract	Member of the European Commission's contract staff, Function Group IV (article 3b of the Conditions of Employment of Other Servants)
Duration of contract	36 months (renewable up to maximum 6 years)
Area	Algorithmic transparency, Trustworthy Artificial Intelligence
Place of employment	Ispra (IT)
Indicative basic salary	3,710.50 € - 5,374.44 € (applicable as of 1st of January 2022) For more detailed information please consult: Working Conditions.

WE ARE

The Joint Research Centre (JRC) is the science and knowledge service of the European Commission: our mission is to support EU policies with independent evidence throughout the whole policy cycle.

The current vacancy is with the newly formed **European Centre for Algorithmic Transparency (ECAT),** which, through its scientific and technical expertise and analyses, will reinforce the European Commission's supervisory role in the context of the **EU Digital Services Act (DSA)** - in close collaboration with the Directorate General for Communication Networks, Content and Technology (DG CONNECT). The ECAT will be established in the second half of 2022 and will be located **in three JRC sites (Seville, Ispra and Brussels)**.

The **EU Digital Services Act (DSA)** is the world's first platform regulation that seeks to comprehensively address the most pressing societal risks emerging from the use of online platforms. Amongst other challenges, it focuses on tackling the dissemination of illegal content, goods and services online, protecting freedom of expression, and addressing disinformation.

It imposes obligations for online intermediaries and platforms (e.g. online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms) according to their role, size and impact in society. It seeks to empower users of digital services – for example by regulating advertising and recommender systems on online platforms – and to protect them, by imposing obligations on digital services and holding them accountable through an unprecedented transparency mechanism.

Since a wider reach is coupled with the most severe risks, very large platforms and search engines with a user base of more than 45 million monthly average users (representing around 10% of the EU population) bear special obligations. Most prominently, they will be subject to a supervised risk management obligation and will need to adapt their service, their

systems and their algorithms to address the societal risks they may pose. They will be subject to external independent auditing and will be under public scrutiny from civil society, vetted researchers and others.

This adaptive and anticipatory legal framework needs strong regulatory supervision and cutting-edge competence within the regulators. The European Commission will lead the supervision and enforcement of obligations for the largest platforms and search engines. This vacancy is part of the Commission's efforts to strengthen its capability and prepare for the enforcement of the rules. The Regulation was proposed by the European Commission in December 2020 and should enter into force in the last quarter of 2022.

We offer:

- a job in a **dynamic, multidisciplinary research field** at the cutting edge of algorithmic systems transparency and trustworthy artificial intelligence, with a tremendous societal impact in Europe and beyond;
- a unique opportunity to **help make the online space safer and more transparent** for all Europeans and to work hands-on on some of the **most exciting and complex challenges brought by online platforms**;
- a family-friendly working environment, with online collaboration and occasional travel for on-site investigations on the premises of online platforms and cooperative work with colleagues in Brussels, Seville or Ispra.

WE PROPOSE

The jobholder will join an interdisciplinary and multicultural team of researchers working in the ECAT and more broadly contribute to the JRC's research portfolio on Trustworthy Artificial Intelligence and algorithmic transparency. S/he will work in close collaboration with a wide range of partners, in particular legal and policy experts in the enforcement units of the European Commission, in DG CONNECT, external researchers and scientists, and other various stakeholders in EU Member States and civil society organisations.

The jobholder will be the overall responsible for the ICT security of ECAT digital infrastructure, both in the cloud and on-premise, including concept definition, requirements, security architecture.

The work may involve:

- Design and implementation of cybersecurity organizational and technical measures, including the deployment and operation of security controls, security monitoring and incident response operations.
- Drafting and managing the security documentation for the ECAT information systems, including scope, business impact assessments, risk assessments and security implementation plans. Acting as the ECAT contact point for JRC and EC cybersecurity stakeholders, e.g. JRC local information security officer (LISO).
- Ensuring compliance with applicable data protection regulations (Regulation (EU) 2018/1725) for the processing and protection of personal data in the ECAT digital infrastructure and information systems, acting as contact point for the JRC and EC data protection stakeholders, e.g. the JRC Data Protection Coordinator.

- Coordinating the operational security (OPSEC) aspects of ECAT activities. Translating concrete security, privacy and anonymity needs of ECAT activities into technical requirements for ICT infrastructures as well as workflows and protocols for ECAT staff.
- Supporting concrete online platform investigations from the ICT and operational security angle. This may include activities such as the definition and implementation of custom ICT infrastructure configurations and automation measures to support audits and inspections, and responsibility for the management of sensitive information handled in the course of investigations.

WE LOOK FOR

For this team, we are looking for **applied researchers and investigators** with a strong motivation to work in a goal-oriented environment for the public good.

Highly motivated outstanding candidates with a keen interest in supporting EU digital policies should have the **following experience/skills (essential)**:

- University degree and 4 years relevant experience in computer engineering, computer science or related field.
- Solid knowledge and working experience in cybersecurity (including cryptography, security controls, incident response, security monitoring, forensics, security auditing, risk management and data protection).
- Very good (C1) knowledge of English.

Any of the following skills and experience would be **desirable**:

- PhD or Msc in the field of cybersecurity or another relevant field.
- Experience in applied investigative work in the context of online platforms, social media, artificial intelligence and/or digital technologies, for example in a public authority or law-enforcement setting.
- Industry certifications in the field of cybersecurity, including CISSP, CISA, CISM, Security+, CEH, GSEC, OCSP, etc.

HOW TO APPLY

If you are **already on a valid CAST FGIV reserve list**, or you **have already applied to one of the calls below**, you can directly submit your application at http://recruitment.jrc.ec.europa.eu/?type=AX.

If not, before applying to this position, **you must register** for one of the two following:

- the Call for Expressions of Interest | EU Careers (europa.eu) (CAST Permanent FGIV), which is used by a wide range of organisations (institutions, bodies, offices and agencies of the European Union), or
- the specialised call for researchers (JRC Call COM/1/2015/GFIV – Research), which is mainly used by the JRC.

Note that each of the calls above has **different minimum eligibility requirements and different selection tests**.

The JRC cultivates a workplace based on respect for other people and the environment, and embraces non-discriminatory practices and equality of opportunity. In case of equal merit, preference will be given to the gender in minority.