



**EUROPEAN  
DATA PROTECTION  
SUPERVISOR**

**VACANCY  
NOTICE**

The EDPS is looking for a

## **Data Breach Notification and Investigation Officer**

<b>Vacancy notice n°</b>	02/2024-EDPS-CA
<b>Type of post/type of contract</b>	Contract Agent (1 year renewable)
<b>Grade/function group</b>	FGIV
<b>Publication under</b>	Article 3b of the CEOS
<b>Place of employment</b>	Brussels (Belgium)
<b>Deadline for applications</b>	07/06/2024 (Brussels time GMT+1) at 12:00 midday

### **WHO ARE WE?**

#### **The EDPS - a young and dynamic institution**

The European Data Protection Supervisor (EDPS), a young EU institution established in 2004, in Brussels, Belgium, is the independent data protection authority of the EU institutions and the advisor of the EU legislator on data protection matters. We strive to be an impartial centre of excellence in order to embed a strong data protection culture in the EU institutions and the legislation emanating from them. We also closely follow technological developments and try to anticipate their impact on the privacy of individuals. Our organisation employs about 120 staff members, most of whom are EU officials, but we also welcome Contract Agents and Seconded National Experts, working full-time or part-time.

#### **The EDPS - a great place to work**

We value a strong culture of respect, flat hierarchical structures and an open door policy to foster innovative ideas and a strong collaboration between colleagues. To ensure our staff's well-being and motivation, we believe that it is essential to create a healthy organisational climate and to strike a good work-life balance. To achieve this, we offer various flexible working arrangements, as well as learning and development opportunities, such as job-shadowing and training programmes.

## WHO ARE WE LOOKING FOR?

Someone who

- fits in an informal and friendly yet professional working environment;
- appreciates working collaboratively with other colleagues on a variety of different projects;
- brings their creativity and initiative to the table;
- engages constructively with stakeholders, based on our core values: integrity, impartiality, transparency and pragmatism.

## ABOUT THE POSITION

Our job vacancy is in the Systems Oversight and Technology Audits Sector (SOTA Sector) of the **Technology and Privacy Unit**. The unit provides expertise at the intersection of policy and information technology by generating in-depth knowledge about the impact of technology on privacy and data protection, including the forecast of future trends.

The Regulation 1725/2018 introduces a duty on all EU Institutions and bodies to report certain types of personal data breach to the EDPS. They must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, they must also inform those individuals without undue delay.

In the EDPS, the SOTA Sector is in charge for handling personal data breaches notifications received from the Union institutions, bodies, offices and agencies (EUIs). As an indicative number, the EDPS receives around 100 notifications per year. The Sector is also in charge for the most efficient development of the internal procedures and the technical architecture for the management of the personal data breaches.

The SOTA Sector leads the technical audits of IT systems carrying out data processing operations and in particular the Large Scale IT systems of EU Institutions (EUIs), such as SIS II, Eurodac, VIS, etc. In these audits the EDPS follows the requirements of specific legal instruments and international standards and controls and ensures that personal data breaches are effectively handled by the EUIs in charge. The SOTA Sector is also responsible for the handling of the notifications of security incidents that affect these Large Scale IT Systems.

As a Data Breach Notification and Investigation Officer you will be the main responsible of the area of management of personal data breach notifications. This will include the following responsibilities:

- Establish the strategy to improve the compliance in terms of personal data breach notification and management in EUIs. This will include:
  - Design the personal data breach management process with particular emphasis on the workflows including the legal templates to be used in each of the steps and data retention approach;
  - Nudge campaigns, interviews with DPOs, carry out surveys, prepare trainings;
  - Raise awareness in EUIs by preparing training documentation (such as factsheets, videos or guidelines) and delivering training sessions on personal data breach management;
  - Prepare reports including statistics on personal data breaches;
  - Monitor the personal data breaches received with the objective of making the necessary processing;
- Manage the operations associated to the personal data breach handling in the EDPS:
  - Acknowledge to the EUI the reception of the notifications they send;

- Open a case and make the analysis of the completeness of the information received verifying the legal requirements;
  - Request information when necessary, assess severity and propose a course of action;
  - Take immediate actions to consult the EDPS on whether ordering the controller to inform the data subjects when appropriate and follow-up if necessary (by taking part in investigations, audits and even if necessary, exercise supervision powers);
  - Propose mitigating actions to the controllers to avoid similar incidents in the future;
  - Organize weekly meetings on the Personal Data Breaches and keep minutes;
  - Prepare monthly reports to the Management;
  - Record all information including the correspondence with the EUIs in the EDPS Document Management System;
- Participate as an IT business analyst in the development of IT tools for the handling of personal data breaches:
    - Definition in use cases of the business requirements to be implemented
    - Act as liaison with DG DIGIT for the on-boarding of this process in an electronic Workflow management tool
    - Implement programmatically the process model defined in the electronic workflow system platform by configuring it or coding it
    - Participate in the meetings with the development team
    - Support the development of the relevant workflows
    - Participate in user acceptance tests
  - Participate in audits, investigations and pre-investigations following the analysis of personal data breaches
  - You may also be required to carry out additional tasks when necessary and in the interest of the service.

## OUR ELIGIBILITY AND SELECTION CRITERIA

### Eligibility criteria

For your application to be considered eligible, you must be a national of a Member State of the European Union and meet the following criteria by the deadline for submitting applications<sup>1</sup>:

Qualifications<sup>2</sup>:

- A University degree, in the field of Information Technologies and/or Law attested by a diploma;
- Appropriate professional experience with the technological aspects of personal data protection and/or development of IT systems, preferably in an IT department or other department highly involved with the development of IT applications of at least 5 years. This should include elements such security, business process modelling-definition and development of front end and backend systems.

<sup>1</sup> In case you will be offered the job, you must have completed any compulsory military service; provide appropriate character references (have no criminal record); pass the EU institutions' medical examination; be fluent in one of the EU languages and be able to work in a second EU language.

<sup>2</sup> Only qualifications awarded by EU Member State authorities or qualifications recognised as equivalent by the relevant authorities will be taken into consideration. Qualifications/diplomas awarded until 31/12/2020 in the United Kingdom are accepted without further recognition.

- Appropriate professional experience with the legal and procedure aspects associated to personal data breaches, preferably as DPO or working in another department highly involved with personal data processing (such risk assessment and compliance) of at least 5 years;
- Candidates for this Contract Agent position must have passed the EPSO Permanent CAST by the end of the recruitment process and are therefore encouraged to create a corresponding EPSO profile already with their application.

## Selection criteria

For this job vacancy, we are looking for someone with the following essential and advantageous skills and experience:

### Essential

- Good knowledge of the applicable legislation in what concerns data breach notifications. In particular, Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive 216/680;
- Knowledge of Information Technologies and Information Security;
- Very good ability of multi-tasking and completing several simultaneous projects within a deadline, as well as being able to demonstrate flexibility and willingness to work on diverse type of tasks;
- Extensive capacity for analysis, good communication and writing skills in a structured way. Proven experience working and managing cases/contracts or similar, where it is essential to have a control of the full workflow of activities needed to close a case;
- Experience as IT Business analyst in the definition of requirements for the development of Business processes in IT tools;
- Experience with user acceptance testing both using “user interface” and REST services;
- Experience in procedural work and electronic workflow systems associated to document management involvement, follow-up of cases across different states applying strict procedures (for instance the application of the procedure established in a Regulation);
- Very good organisational and prioritising skills in a very varied workload with demanding deadlines;
- Excellent computer skills with sound knowledge of MS Office package (in particular Excel);
- Very good knowledge of written and spoken English and French;
- Ability to work autonomously, but also a strong sense of teamwork;
- Sense of responsibility, organisation, initiative, human relations and communication.

### Advantageous

- Certifications in International Standards such ISO in the area of Security and/or compliance;
- Knowledge of other EU languages;
- Experience in the development of IT projects;
- Experience in the handling of investigations and audits;
- Very good knowledge of the structure and functioning of the European Union and its Institutions in relation to the position;

- Good knowledge of the legislation and its implications concerning data protection and privacy with regard to Union institutions, offices, bodies and agencies;

## HOW TO APPLY?

Interested in this position? Please apply via the following link by **07/06/2024 at 12:00 midday (Brussels time)**:

[https://ec.europa.eu/eusurvey/runner/Application\\_form\\_VN\\_02\\_2024\\_EDPS\\_CA\\_TP\\_Data\\_Breach\\_Notification\\_and\\_Investigation\\_Officer](https://ec.europa.eu/eusurvey/runner/Application_form_VN_02_2024_EDPS_CA_TP_Data_Breach_Notification_and_Investigation_Officer)

You will have to **complete the online application form and upload the following documents**:

- Cover letter detailing why you are suitable for this role (PDF format of maximum size of 1MB);
- CV (preferably in Europass format);
- Optional: All supporting documents, such as references, certificates, must be merged into one single PDF document of a maximum size of 1MB.

Do not hesitate to contact [edps-selections@edps.europa.eu](mailto:edps-selections@edps.europa.eu) in case you have any questions.

## OUR SELECTION PROCEDURE

All eligible applications will be scrutinised by a selection panel. Candidates whose applications best match the selection criteria will be invited for an interview during which the selection panel will assess each candidate's performance. In addition, a second interview or written tests may be carried out. At the EDPS we aim for all selection panels to have a gender-balanced composition.

## OTHER IMPORTANT INFORMATION

### Equal opportunities

The EDPS is committed to promoting diversity, inclusion, and giving everyone equal opportunities to succeed.

As such, the EDPS welcomes all applications without discrimination on grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of national minority, property, disability, age, gender identity or sexual orientation.

If you require any special arrangements (due to a disability) to take part in this selection procedure, please indicate this on your application.

### Data protection

A data protection notice detailing how the EDPS processes candidates' personal data in the context of recruitment can be found [here](#)

Join us in shaping a safer digital future!