LARGE SCALE IT SYSTEMS SECURITY INCIDENTS NOTIFICATIONS

DATA PROTECTION NOTICE

Under specific legal frameworks, European Union Institutions, Bodies, and Agencies (EUIs) - including eu-LISA, Europol, and Frontex and, in certain cases, Member State Authorities (MS), are required to notify the European Data Protection Supervisor (EDPS) of any security incidents related to designated Large-Scale IT Systems (LSITs) operating within the European Union in the Area of Freedom, Security, and Justice (AFSJ). These obligations are established in various regulations, including:

- Article 45 of Regulation (EU) 2018/1861 and Article 60 of Regulation (EU) 2018/1862 on the Schengen Information System (SIS),
- Article 34 of Regulation (EU) No 603/2013 on Eurodac,
- Article 60 of Regulation (EU) 2018/1240 on the European Travel Information and Authorisation System (ETIAS),
- Article 44 Regulation (EU) 2017/2226 on the Entry/Exit System (EES),
- Article 43 of both Regulations (EU) 2019/817 and 2019/816 on the interoperability framework.

The EDPS maintains a dedicated register to collect and document security incident notifications. Notifying authorities must provide, at a minimum, the following details: a) a description of the incident, including the affected LSIT, b) the nature and timeline of the incident, c) an impact assessment and measures taken to mitigate associated risks, and d) contact details of the reporting officer. To facilitate compliance, the EDPS has developed a standardized reporting form to guide notifying authorities in submitting incident reports.

The LSITs Security Incidents Notification register enables the EDPS to enhance data protection oversight of LSITs and the data they process, in accordance with its legal mandates under Regulation (EU) 2018/1725 and the specific LSIT regulations.

The EDPS records the received notifications and utilizes this information in its supervisory activities related to eu-LISA, including audits and recommendations. Furthermore, the EDPS may share security incident details within its cooperation framework with other Data Protection Authorities (DPAs) and through the Coordinated

Supervision Committee (CSC), in line with Article 62 of Regulation (EU) 2018/1725.

All security incident notifications and any additional information submitted by mandated authorities are processed and stored in the EDPS Case Management System (CMS) within a structured, designated directory.

In cases where classified information is received, the EDPS employs appropriate mechanisms for handling such data. A reference to these mechanisms and the classification status of the information is documented in the CMS. Notifying authorities should refrain from including classified information in their notifications unless strictly necessary for the purpose of the report.

Personal data is processed in accordance with Regulation (EU) 2018/1725 (hereinafter 'the Regulation'). We provide the information that follows based on Articles 15 and 16 of the Regulation.

Who is the controller?
The controller is the European Data Protection Supervisor (EDPS).

Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
Telephone: +32 2 283 19 00
Email: edps@edps.europa.eu

Responsible department or role:
Technology and Privacy Unit: tech-privacy@edps.europa.eu
Systems Oversight and Technology Audits Sector (SOTA)

Functional mailbox for LSITs security incident notifications: LSIT-security-incident@edps.europa.eu

Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/about-edps/contact_en.

For more information on the EDPS please consult our website: https://edps.europa.eu.

What personal data do we process and who has access to this personal data?
The personal data we process includes the information provided in the Security Incident Notification Form, specifically the name and contact details of the designated reporting officer responsible for submitting the security incident notification. This data is essential for ensuring effective supervision and compliance with the EDPS's legal obligations.

When submitting a notification via email, we process the additional personal data included in the email, such as: the sender's email address and signature, any email addresses copied in the correspondence.

In specific circumstances, also as part of the follow-up questions, the reporting Authority may provide information that contain further personal data. Examples include providing copies of communications to other relevant Authorities, containing names and contact details of the relevant contact points, or copies of investigation/audit reports, including the name, contact details and potential signature of the report author. EDPS in principle does not require to receive such data and reporting authorities should abstain from sharing such documents unless necessary, and/or remove the personal data they include.

Access to this data is strictly limited to authorized EDPS staff responsible for managing data breach notifications, handling cases, and ensuring compliance with supervisory and enforcement obligations.

In specific circumstances, where coordinated supervision actions are conducted via the European Data Protection Board (EDPB) Coordinated Supervision Committee, in accordance with Article 62 of Regulation (EU) 2018/1725, relevant data may be shared with your national Supervisory Authority. This applies only to notifications submitted by Member State Authorities.

Where did we get your personal data?

We process only the personal data included in the Security Incident Notification Form and the respective email communications.

Why do we process your personal data and under what legal basis?

We process the personal data following the notification legal obligations, according to the respective provisions for notification in the legal frameworks related to specific Large-Scale IT Systems (LSITs) operating in the European Union, in the area of Freedom, Security and Justice (ASFJ).

How long do we keep your personal data?

We keep your personal data for ten years after closure of the case. We may keep it for longer if circumstances such as investigations, appeals or legal proceedings are ongoing at the planned expiration date.

Inadmissible notifications[1] that do not concern the above legal obligations will not be treated and will be deleted at the end of the year proceeding the year of submission.

[1] *Inadmissible notifications are notifications that originate from an EUI or competent national authority that does not concern a security incident included in the above regulations or notifications that originate from other entities, not competent according to the above regulations.*

What are your rights regarding your personal data?
You have the right to request access to your personal data and to relevant information concerning how we use it. You have the right to request rectification of your personal data. You have the right to ask for the erasure of your personal data or to restrict its processing.

Please note that, in certain cases, as provided in Article 25 of the Regulation, restrictions of data subjects' rights may apply.

We will consider your request, take a decision and communicate it to you. The time limit for treating your request is one (1) month. This period may be extended by two (2) further months where necessary, taking into account the complexity and the number of the requests. In those cases, the EDPS will inform you of the extension within one (1) month of receipt of your request and will provide reasons for the delay.

You can send your request to the EDPS electronically or by post (see section on contact details below).

Automated decision-making
Your personal data is not subject to automated decision-making.

You have the right to lodge a complaint
If you have any remarks or complaints regarding the way EDPS processes your personal data, we invite you to contact the responsible department or role or the EDPS DPO (see section on contact details on the first page and below)

You have, in any case, the right to lodge a complaint with the EDPS as a supervisory authority: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en.

Contact details for enquiries regarding your personal data
We encourage you to contact us using the EDPS contact form, selecting 'My personal data' as the relevant subject: https://edps.europa.eu/about-edps/contact_en.

If you wish to contact the EDPS DPO personally, you can send an e-mail to DPO@edps.europa.eu or a letter to the EDPS postal address marked for the attention of the EDPS DPO.

EDPS postal address: European Data Protection Supervisor, Rue Wiertz 60, B-1047 Brussels, Belgium

You can also find contact information on the EDPS website: https://edps.europa.eu/about-edps/contact_en.