European Data Protection Supervisor

SECURITY INCIDENT[[1]](#footnote-1) notification

*[As required per Article 45 of* [*Regulation 2018/1861*](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1861) *and Article 60 of* [*Regulation 2018/1862*](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1862) *for SIS, Article 34 of* [*Regulation 603/2013*](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0603) *for Eurodac, Article 60 of* [*Regulation 2018/1240*](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1240) *for ETIAS, Article 44 of* [*Regulation 2017/2226*](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2226) *for Entry Exit System and Article 43 of* [*Regulation 2019/817*](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0817) *and* [*Regulation 2019/818*](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0818) *for the framework of interoperability. Notifying Authorities should avoid the inclusion of classified information in the notification to the EDPS, unless strictly necessary for the purpose of the notification]*

**DATE:** Click here to enter a date.

YOUR REFERENCE NUMBER Click here to enter text.

**A. AFFECTED SYSTEM**

A.1 SIS  A.2 EURODAC  A.3 ETIAS  A.4 EES

A.5 Interoperability Components:

i. sBMS  ii. CRRS  iii. CIR  iv. MID  v. ESP

**B. REPORTING UNION ENTITY:**

B.1 MEMBER STATE Click here to enter text.

B.2. eu-LISA  B.3. EUROPOL  B.4 FRONTEX  B.5. Eurojust

B.6 NAME/DEPARTMENT OF THE UNION ENTITY : Click here to enter text.

B.7 REPORTING OFFICER NAME: Click here to enter text.

B.8 REPORTING OFFICER ROLE: Click here to enter text.

B.9 ADDRESS: Click here to enter text.

B.10 TELEPHONE: Click here to enter text. B.11 EMAIL: Click here to enter text.

**D. SECURITY INCIDENT SECTION**

D.1 Briefly explain the type of security incident and how it was detected:

Click here to enter text.

D.2 Security criteria affected *(tick one or more boxes that apply and provide impact level):*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Criteria** | | **Impact Level** | | |
| **Low** | **Medium** | **High** |
| I | Confidentiality |  |  |  |
| II | Integrity |  |  |  |
| III | Availability |  |  |  |
| IV | Malicious Code |  |  |  |
| V | Fraud |  |  |  |
| VI | Intrusion Attempts |  |  |  |
| VII | Intrusion |  |  |  |
| VIII | Suspected Data Breach |  |  |  |
| IX | Other (please specify): |  |  |  |

D.3 Timeline of the incident. Please provide the exact date or period that the incident took place:

Click here to enter text.

D.4 Please provide information on the detection of the incident (Date and by whom was detected) :

Click here to enter text.

D.5 Who did you inform of the incident and when?:

* National Competent Authority  Date Click here to enter text.
* European Commission  Date Click here to enter text.
* eu-LISA  Date: Click here to enter text.
* CERT-EU  Date: Click here to enter text.

Please provide more details: Click here to enter text.

D.6 Initial impact assessment. Please provide an initial analysis of the impact of the incident and indicate the severity of the incident, including the scope and business implications, such as the extent of data compromised, and potential harm to individuals or the operations:

Click here to enter text.

The Severity of the incident is *(please click the risk level following your assessment)* : Low  Medium  High

D.7 Personal data have been affected by the security incident?

Yes  No

If yes, please provide more information:

D.7.1. Have you informed the Data Protection Officer

Yes  No

D.7.2. Have you recorded the security incident as a personal data breach and reported to the Supervisory Authority?

Yes  No

D.8 Which actions and measures have you taken to contain the incident, address the risks and limit its impact?:

Click here to enter text.

D.9 Have you launched a security incident investigation:

Yes  No

if no, motivate why not: Click here to enter text.

D.10 Can you provide information on which was the root cause of the incident (*e.g. software vulnerability, human error, external attack )*:

# Click here to enter text.

1. For the SIS Regulation a security incident is “*Any event that has or may have an impact on the security of SIS or may cause damage or loss to SIS data or to the supplementary information shall be considered to be a security incident, especially where unlawful access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.”*

   For the EES Regulation a security incident is: “*Any event that has or may have an impact on the security of the EES and may cause damage or loss to data stored in the EES shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.”* [↑](#footnote-ref-1)