# EDPS Record of Processing Activity

Record of EDPS activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

| Nr. | Item | Description |
|---|---|---|
| | **INFORMATION SECURITY ACTIVITIES** | |
| 1. | Last update of this record | 02/02/2021 |
| 2. | Reference number | 50 |
| | **Part 1 - Article 31 Record** | |
| 3. | Name and contact details of controller | European Data Protection Supervisor (EDPS)<br>**Postal address**: Rue Wiertz 60, B-1047 Brussels<br>**Office address**: Rue Montoyer 30, B-1000 Brussels<br>**Telephone:** +32 2 283 19 00<br>**Email:** edps@edps.europa.eu<br><br>Responsible department or role:<br>EDPS Local Information Security Officer (LISO) function - edps-it-security@edps.europa.eu<br><br>Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/node/759 |
| 4. | Name and contact details of DPO | DPO@edps.europa.eu |
| 5. | Name and contact details of joint controller (where applicable) | |

| Nr. | Item | Description |
|---|---|---|
| 6. | Name and contact details of processor (where applicable) | CERT-EU<br><br>Contact: services@cert.europa.eu |
| 7. | Short description and purpose of the processing | This record covers the data processing activities performed in the context of Information Security, and in particular:<br><br>• investigation of information security incidents<br>• information security awareness activities, including cybersecurity awareness<br><br>Information security is a vital domain not only for EDPS but for every Organisation. Security incident management and security awareness are amongst the critical Organizational security controls, according to the current best practices on Information Security[1].<br><br>The lack of such controls would significantly increase the risk of security incidents to be materialized with potential devastating impact for the reputation and the integrity-availability-confidentiality of critical business functions of EDPS. |
| 8. | Description of categories of persons whose data the EDPS processes and list of data categories | EDPS staff, persons outside of EDPS, involved in security incidents |
| 9. | Time limit for keeping the data | A. For investigation of information security incidents: up to 5 years<br><br>B. For information security awareness activities, including cybersecurity awareness:<br><br>CERT-EU keeps the data as long as a security awareness activity is ongoing and deletes all processed data after a security awareness activity is completed. EDPS maintains a list of active staff members that have received security awareness training in the current year. When the end of the year has been reached, this list is deleted. After a specific security awareness activity is completed, the EDPS keeps a record of the percentage of staff who have attended (for example: 60% attended the training of February 2021, 80% attended the training of June 2022). |

[1] Center for Internet Security, top 20 critical controls: https://www.cisecurity.org/controls/cis-controls-list/

| Nr. | Item | Description |
|---|---|---|
| 10. | Recipients of the data | A. For investigation of information security incidents:<br><br>Depending on the nature of the incident and strictly following the need to know principle: EDPS staff members, CERT-EU or IT service providers (e.g. the European Parliament).<br><br>B. For information security awareness activities, including cybersecurity awareness:<br><br>The list of active staff members who have received security awareness training in the current year remains within the LISO function. The records of percentage of EDPS staff who have attended specific security awareness activities is sent to the top management. |
| 11. | Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards? | Not such transfers are taking place |
| 12. | General description of security measures, where possible. | A. For investigation of information security incidents:<br><br>• all information is collected and processed under the sole control of the LISO function<br>• files are stored in the EDPS Case Management System (CMS) and the corporate computer of the LISO function<br>• the LISO related CMS cases are only accessible to the LISO function staff and the CMS administrators<br>• sensitive personal data are kept in encrypted zip files and only the LISO can decrypt them<br>• the principle of data minimization is applied: only data relevant to the security incident are collected and processed. Where possible, data are anonymized.<br><br>B. For information security awareness activities, including cybersecurity awareness:<br><br>• Awareness activities will be mainly training sessions and cybersecurity exercises.<br>• Cybersecurity exercises are announced before their implementation, to reduce the risk of inadvertent exposure of real personal data by EDPS staff, e.g. during phishing exercises, and to respect the obligation to inform data subjects. |

| Nr. | Item | Description |
|---|---|---|
| | | • The LISO function will mantain a register of attendance to training sessions to ensure all EDPS staff is covered by the training activities. Conversely, the results of the cybersecurity exercises will be, to the extent possible, anonymous.<br>• when EDPS staff expose their personal or corporate information during cybersecurity exercises, the involved IT systems will not store temporarily or permanently such information, but they will flag that such information was introduced by the user.<br>• when the IT systems involved in such activities absolutely need to temporarily use personal data related identifiers (cookies, IP address, MAC address, etc), such information will only be used temporarily as long as it is needed by the system, and it will be deleted afterwards.<br>• the principle of data minimization is applied in a strict fashion: the only information that needs to be reported by such activities is the anonymized performance of EDPS staff (e.g. 40% of users clicked on the malicious link, 23% of users shared their personal information, etc). All the other information will be deleted or become fully anonymized. |
| 13. | For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice: | Data protection notice available internally |