# EEAS Personal Data Processing Record

Ref. Article 31 of Regulation (EU) 2018/1725 - Legal obligation for maintaining records

| | | |
|---|---|---|
| 1 | Title of the processing activity | **Incident reporting** |
| 2 | Update of the record (last modification date) | 03/01/2024 |
| 3 | Register reference number | 3261 |
| 4 | Identity and contact details of the<br>Data Controller<br>Joint Controller (if applicable)<br>Data Processor (if applicable) | European External Action Service<br>Rond Point Schuman 9A, 1046 Brussels, Belgium<br>Data Controller contact entity:<br>Field Security and HQ Security and EEAS Security Policy<br>Functional mailbox: SG-CRC-3@eeas.europa.eu<br>EEAS-SECURITY-INVESTIGATIONS@eeas.europa.eu<br>Responsible entity for implementation: EU Delegations/EEAS Divisions |
| 5 | Identity and contact details of<br>the Data Protection Officer | EEAS Data Protection Officer (DPO):<br>Emese Savoia-Keleti.<br>SG.AFFGEN.DPO<br>Functional Mailbox of the DPO:<br>DATA-PROTECTION@eeas.europa.eu |
| 6 | Purpose of the processing activity | The purpose of the processing is to record incidents that have a negative impact on the EEAS security interests affecting staff, the Delegation's premises, physical assets and information, both in EU Delegations (Delegation staff, dependants of expatriate staff forming part of their household, professional visitors), and in HQ. EEAS HQ staff going on mission to third countries can also report incidents.<br>Description: The incident reporting via de @HelloAdmin portal will be done by staff posted in EU Delegations (for themselves or on behalf of others, when so specified) and by EEAS HQ staff. The incident reports will be evaluated and followed up by HQ security staff who will also prepare regular reports. Reports on behalf of individuals not having access to the portal (including non-EU official visitors and dependants) will be registered by Delegation staff with proper authorisation. |
| 7 | Legal basis and lawfulness | The processing of personal data is necessary for the performance of a task carried out by the European External Action Service in the public interest, in particular for management andfunctioning ofthe EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725] as referred to in Recital 22 thereof.<br>It is also necessary for compliance with a legal obligation (Article 5 (1) b), and Article 7 on security incidents and emergencies of the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service - ADMIN(2017) 10.<br>Other legal reference: Council Decision of 26 July 2010 establishing the organisation and functioning of the EEAS (2010/427/EU) – OJ L 201, 3/8/2010, p. 30. |

# EEAS Personal Data Processing Record

Ref. Article 31 of Regulation (EU) 2018/1725 - Legal obligation for maintaining records

| | | |
|---|---|---|
| 8 | Categories of individuals whose data is processed - Data subjects | Staff in EU Delegation,<br><br>Dependants of expatriate staff forming part of their household,<br><br>EEAS or other EU institution staff in HQ who report an incident when in HQ or when going on mission,<br><br>Visitors to the EEAS premises who report an incident. |
| 9 | Categories of data - Data processed | - First Name/Last Name of the colleague reporting the incident<br>- Staff position<br>- Incident details :<br><br>Category and subcategory, if any<br><br>Date when it took place or when it was discovered<br><br>Location: country, place, latitude, longitude<br><br>Person affected (if different from reporter), including status, gender (could be anonymous)<br><br>Impact on the affected person and on the EU Delegation<br><br>Short description<br><br>Actions taken and/or required |

| | | |
|---|---|---|
| 10 | Recipients of data – Access to data | For security incidents at HQ<br>- A link to the case (also known as back office) will be sent to the Security Investigations Sector in the HQ Security and EEAS Security Policy Division.<br>- If the security incident is in the category Espionage, a link to the case will be sent to the Counter-Intelligence team in the HQ Security and EEAS Security Policy Division.<br>- If the security incident is in the category Health, a link to the case will be sent to the Medical Service.<br>- If the security incident reports any impact on health of the affected person/people, a link to the case will be sent to the Medical Service.<br>- If the security incident is in the category Safety, a link to the case will be sent to the Real Estate, Safety and Greening Division.<br>- If the security incident reports any impact on the organisation with regards to health safety of personnel and/or physical assets financial losses other than none or negligible, a link to the case will be sent to the Real Estate, Safety and Greening Division.<br>- The Director for Security and Corporate Services and the Head of Division of HQ Security and EEAS Security Policy Division will be able to read the incident report too.<br>- Designated staff of the EEAS and other EU institutions, bodies and agencies, whose staff can be affected by the incident, in particular the European Commission; and contractors involved in the handling of incidents, including follow-up, complaints and litigation, on a strict need to know basis.<br><br>For security incidents in Delegations or on mission (including Delegation staff on mission to HQ)<br>- A link to the case will be sent to the Head of Delegation in the relevant country.<br>- A link to the case will be sent to the responsible Regional Security Officer (RSO), or Regional Security Advisor (RSA).<br>- A link to the case will be sent to the relevant geographical team of the Operations Sector of the Field Security Division.<br>- A link to the case will be sent to the Security Investigations Sector in the HQ Security and EEAS Security Policy Division.<br>- If the security incident is in the category Espionage, a link to the case will be sent to the Counter-Intelligence team in the HQ Security and EEAS Security Policy Division.<br>- If the security incident is in the category Health, a link to the case will be sent to the Medical Service.<br>- If the security incident reports any impact on health of the affected person/people, a link to the case will be sent to the Medical Service.<br>- If the security incident is in the category Safety, a link to the case will be sent to the Real Estate, Safety and Greening Division.<br>- If the security incident reports any impact on the organisation with regards to health safety of personnel and/or physical assets financial losses other than none or negligible, a link to the case will be sent to the Real Estate, Safety and Greening Division.<br>- The Director of the Crisis Response Centre and the Head of Division of the Field Security Division will be able to read the incident report too.<br>- In case the affected person's affiliation is from a European Commission Directorate General (DG), the Duty of Care correspondent in the relevant DG will be notified of the incident report who may share it further with relevant services<br>- Designated EEAS staff and contractors involved in the handling of incidents, including follow-up, complaints and litigation, on a strict need to know basis.<br><br>Important remarks<br>- The reports of security incidents that occur in countries without an EU Delegation but outside the EU, will be redirected to the Head of Delegation and RSO/RSA from the Delegation that covers for country in question by the Strategy Sector of the Field Security Division.<br>- The reports of security incidents that occur in countries without an EU Delegation but with a Representation in the EU, are automatically sent to the Europe and Central Asia team in the Operations Sector of the Field Security Division.<br>- Security incident reports mentioning any issues with or damage to security equipment (such as Armoured Vehicles, Personal Protective Equipment, satellite phones or radios) will be forwarded to the Resources and Logistics sector of the Field Security Division by the relevant geographical team of the Operations Sector of the same Division. |

| | | |
|---|---|---|
| 11 | Transfer to Third Countries<br>or International Organizations (IOs)<br>and suitable safeguards (if applicable) | N/A |
| 12 | Time limit for keeping the data<br>- Retention period | The data will be stored in the @HelloAdmin platform. The platform will automatically delete the information once the period of 5 years is over, unless the information has been flagged for a potential investigation.<br><br>Personal data may be kept for information and historical, statistical or scientific purposes for a longer period of time including the publication on the EEAS Intranet with appropriate safeguards in place. Archiving shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of individuals. Reports and other material containing personal data are archived according to e -Domec policy.<br><br>In case of an incident or event giving rise to an enquiry by authorities, data subjects' or other concerned individuals' personal data will be preserved as long as the legal claims arising from the investigations expire or any follow-up action is due. This includes pending cases, appeals and court judgments t o allow for the exhaustion of all appeal and other channels of legal remedies. In any case, p ersonal data will not be kept longer than 5 years after the judgment on the pending case is final.<br><br>When appropriate, personal data contained in supporting documents should be deleted where possible, not later than 1 year after evaluation and follow-up of the incident was closed if that data is not necessary for audit, inspection or other control purposes. |
| 13 | Data Storage | The data will be stored in the @HelloAdmin platform. The platform will automatically delete the information once the period of 5 years is over unless the information has been flagged for a potential investigation. |
| 14 | General description of security measures | Access to @HelloAdmin IT tool is protected by a userID and password. Data collected via @HelloAdmin is processed by assigned EEAS staff members. Access to specific files requires authorisation. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. General access to personal data is only possible to recipients with a UserID/ Password. |

| | | |
|---|---|---|
| 15 | Rights of individuals | Data subjects have the right of access to their personal data and the right to correct any inaccurate or incomplete personal data. The right of rectification can only apply to factual data processed. Under certain conditions, data subjects have the right to ask the deletion of their personal data or restrict their use as well as to object at any time to the processing of their personal data on grounds relating to their particular situation.<br>The EEAS will consider the request, take a decision and communicate it to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary . Data subjects are informed in the Privacy Statement that they can find more information in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725.<br>In specific cases, restrictions under Article 25 of the Regulation may apply. If data subjects wish to exercise their rights or have questions concerning the processing of their personal data, they may address them to the functional mailbox provided.<br><br>If data subjects wish to exercise their rights or have questions concerning the processing of their personal data they may address them to Field Security, or HQ Security and EEAS Security Policy contacting the data controllers via the following email addresses:<br>SG-CRC-3@eeas.europa.eu (incidents outside HQ)<br>RM-SCS-3@eeas.europa.eu (incidents in HQ) |
| 16 | Information to data subjects | Individuals will be informed during the collection of data, as they will have to complete and send the incident reporting in which they are informed about data protection provisions applied in the processing of personal data. A link to the Privacy statement on the EEAS Intranet will be visible on the incident reporting page. |