# EEAS Personal Data Processing Record

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

| | | |
|---|---|---|
| 1 | Title of the processing activity | **Health Insurance for Local Agents in EU Delegations (administration, authorisation and reimbursement) and related personal data processing operations** |
| 2 | Update of the record (last modification date) | 16/12/2020 |
| 3 | Register reference number | 2222 |
| 4 | Identity and contact details of the Data Controller<br>Joint Controller (if applicable)<br>Data Processor (if applicable) | Data Controller:<br><br>European External Action Service<br>Rond Point Schuman 9A, 1046 Brussels, Belgium<br>Data Controller contact entity: BA.HR.5 Local Agents Division<br>Functional mailbox: LOCAL-AGENTS@eeas.europa.eu<br>Based on a framework contract, independent dental and medical advisors process data on behalf of BA.HR.5.<br><br>EEAS Data Protection Officer:<br>DATA-PROTECTION@eeas.europa.eu |
| 5 | Identity and contact details of 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 | Administrative management of the health insurance scheme for local agents and their beneficiaries in EU Delegations.<br><br>Description:<br><br>At Headquarters' level the task involves:<br>- Administrative management of affiliation rights<br>- Administrative decisions on loss of earnings benefits for incapacity for work<br>- Granting prior authorisations for specific medical treatments<br>- Medical data processing by medical/dental advisers to issue medical opinions<br>- Administrative decisions to grant reimbursement at 100% in certain specific conditions (for example accidents at work/ occupational diseases or high medical costs)<br>- Verification of reimbursements<br>- Statistics.<br>At Delegation's level / RCE the following tasks are included:<br>- Collection and verification of supporting documents (affiliation rights and medical expenses)<br>- Reimbursement of medical costs incurred by the affiliated members and their beneficiaries<br>- Issuance of a letter of guarantee or direct billing in case of hospitalisation<br>- Issuance of lists of persons covered by the health insurance for the purpose of ensuring access to medical establishments. |

# EEAS Personal Data Processing Record

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

| | | |
|---|---|---|
| 7 | Legal basis and lawfulness | - Note 17948 of 14 December 1995 and its upcoming successor legal basis, the Joint Decision C(2019) 5684 – for LA-Medical. This information is available in the EU Delegations' Guide or the EEAS Intranet.<br>- Good administrative practices in the framework of the Treaty of Lisbon and the Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU) available on:<br>https://eeas.europa.eu/sites/eeas/files/eeas_decision_en.pdf |
| 8 | Categories of individuals whose data is processed<br>- Data subjects | Data, including personal data, are processed from the following individuals or groups of people:<br>- Affiliated members (local agents and former local agents)<br>- Beneficiaries (dependents of affiliated members)<br>- Medical practitioners<br>- Third party involved in an accident in case of accident at work<br>- Actual insurance policy holder concerning the third party in case of accident at work. |
| 9 | Categories of data - Data processed | The data, including personal data, processed may be the following:<br>For affiliated members and beneficiaries : personal data (Per id, name, forename, date of birth, nationality, age, relationship type, employer, statute, gender, marital status, dependent (Y/N), relationship date, personal number of local agent); official documents (birth certificates, adoption/guardianship decision, study certificates, marriage certificates, income declarations) and medical data (reports with information about treatment, foreseen treatment and dates, complete diagnosis, health conditions, medical results, plaster models; X-rays, pictures, medical practitioners' prescriptions and invoices, accident reports, reimbursements by the primary insurance, reimbursable amounts).<br>For electronic prior authorisations: in addition to the above, workflow status, request date, request number, last change date, last modified by, medical advisor's opinion, diagnosis and decision of the request.<br>For medical practitioners : personal data (credentials, name, forename and contact details).<br>For third parties involved in an accident : personal data (name, forename and contact details).<br>For insurance policy holders : personal data (name, forename, contact details, name of the insurance company and number of the insurance policy).<br>For electronic claims (dealt by the Delegation and / or RCE): in addition to the above, LA Analytical code, ABAC Bank Account Id, Bank Account number. |
| 10 | Recipients of data – Access to data | - In EU Delegations:<br>assigned and authorised staff, the Head of Administration, the Head of Delegation;<br>- In the Regional Centre Europe:<br>case handlers, team leader, Head of the RCE<br>- In HQ:<br>- Division Local Agents' case handlers, Head of Sector, Deputy Head of Division, Head of Division<br>- Other authorised EEAS staff such as legal officers or advisors (e.g. of Legal Affairs, Horizontal Coordination, Internal audit)<br>- Medical or dental advisers contracted by the Division |

| | | |
|---|---|---|
| 11 | Transfer to Third Countries<br>or International Organizations (IOs)<br>and suitable safeguards (if applicable) | Potential transfer to:<br>-the primary insurance system or company with whom the affiliated member has the primary insurance coverage;<br>-insurance companies of the EU Delegations;<br>-in case of accident, the third party's insurance company.<br>The insurance company and the medical or dental advisors, as contractors, will be bound by a service provider contract signed between the EU Delegation and the insurance company or the EEAS and the medical or dental advisor. The service contract shall include contractual clauses on data protection defining the subject matter, duration, nature of the processing, the retention period, that the processor acts only on behalf of the data controller and that technical and organisational security measures are to be implemented by the contractor, the obligations of the contractor in terms of data protection and the possibility for the EEAS to verify compliance by audits/inspections.<br>If there is no adequacy decision on the basis of article 45 of<br>Regulation (EU) 2016/679 for that country by the EC, more information to be filled under 'High risk identification' |
| 12 | Time limit for keeping the data<br>- Retention period | The personal data of local agents are kept for 10 years after the end of their affiliation to the health insurance.<br>Description:<br>Files are organised by local agent (nominative files). Due to the fact that it is technically impossible to delete specific parts of the file, all documents related to the health insurance for local agents are to be kept for 10 years after the end of the affiliation. This respects the purpose of avoiding insurance fraud as well as the rules on the budgetary discharge (as foreseen under the Financial Regulation).<br>Files are kept for 18 months for making the last claims, plus a specific period for the administrative handling of claims and 7 years due to the requirements of the Financial Regulation. This adds up to the 10 years overall retention period. |
| 13 | Data Storage | Storage<br>Electronic archives:<br>Outlook folders: documents related to the health insurance of local agents are only accessible to staff members involved in the management thereof;<br>Group drive (Y): documents related to the health insurance of local agents are only accessible to staff members involved in the management thereof (protected folder);<br>e-Del-HRM: personal data stored and accessible to staff members involved in the management of local agents files;<br>HR-Delegation: personal data stored and accessible to staff members involved in the management of local agents files;<br>ARES (document management system): documents related to the health insurance of local agents are only accessible to staff members involved in the management thereof (stamp medical secret).<br><br>Paper archives:<br>In EU Delegations and in the RCE, the files are kept in the Administration Section (usually Head of Administration Office), in a locked room. Only the assigned staff dealing with medical reimbursements has access to the files.<br>At Headquarters, the files are kept in a locked room in a locked cupboard of the premises of the EEAS HQ (Local Agents Division), only the staff dealing with the health insurance of local agents has access to this room.<br>A confidentiality declaration has to be signed by all staff in Delegations, at the Regional Centre and at Headquarters.<br>Reimbursement requests have to be submitted in a sealed envelope addressed to the Head of Administration and marked 'Medical Matter'.<br>Requests requiring headquarters' authorisation are submitted as above and transferred to Headquarters by email via the functional mailbox. The use of SECEM is recommended. Medical reports can be submitted directly to Headquarters by the affiliated member or his/her medical practitioner.<br>It is foreseen that all requests may be submitted electronically via HR-Delegation. |
| 14 | General description of security measures | Based on assessing risks related to potential access to data with regard to health insurance for Local Agents in EU Delegations, the EEAS ensures that adequate organisational and technical measures are in place in order to safeguard personal data of data |

subjects.

I. Physical files

Physical files are locked in cupboards in EEAS HQ (Local Agents Division) and in EU Delegations premises.

II. Electronic files:

-All data in electronic format are stored either on the servers of the EEAS, the operations of which abide by the Decision of The High Representative of the Union For Foreign Affairs And Security Policy of 19 April 2013 on the security rules for the European External Action Service (2013/C 190/01) concerning the security of information systems used by the EEAS.

-Access to the data is provided to authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

-Access to electronic files is granted to assigned staff.

-Outlook folders are only accessible to assigned staff members of EEAS HQ and EU Delegations.

-Drive Group Share (drive 'Y'): health insurance related files are only accessible to assigned staff members of EEAS HQ and EU Delegations / RCE.

-ARES: only accessible to staff members involved in the processing operation.

-Security is also ensured by the safety measures built in the various IT applications.

-Measures are provided to prevent non-responsible entities from accessing data.

III. Transmission of data:

For the time being, requests are forwarded through the Delegation’s administration. The cover note must not contain any reference of a medical nature.

Exceptionally, and in order to safeguard the confidentiality of the medical data, the local staff member may, if they so wish, forward directly the documents containing medical data to the functional mailbox. In such case, the local agent will have to inform the Delegation's administration section.

Communications on ongoing requests for authorisation are normally sent only to the Head of Administration and the assigned administrative staff member so as to limit their circulation within the Delegation. They do not contain references of a medical nature.

Furthermore, requests for reimbursement have to be submitted in a sealed envelope addressed to the Head of Administration and marked ‘Medical Matter’.

In order to guarantee confidentiality at Headquarters by limiting circulation of the files to the Health Insurance, requests requiring Headquarters’ authorisation must only be sent to the functional mailbox. The use of SECEM is recommended.

In line with HQ instructions and in order to safeguard the confidentiality of medical data, the number of people handling the reimbursement of local staff members' medical expenses is limited to the strict minimum. A confidentiality declaration has to be signed by all staff members involved in the process (Declaration On Handling And Processing Of Personal Data And Information Of Confidential And Sensitive Nature).

It is foreseen that prior authorisations and reimbursement requests may be submitted via HR-Delegation. In order to submit or treat a request, users sign an electronic confidentiality declaration.

1/ To be noted: any disclosure or unauthorised use of the data by an official or contractual agent constitutes a failure to comply with the obligations laid down in Article 17 of the Staff Regulations and is liable to lead to disciplinary proceedings under Title VI of the Staff Regulations. Such an act by a local staff member constitutes serious misconduct within the meaning of Article 20 of the Framework Rules and Chapter IX of the Specific Conditions of Employment, without prejudice to the relevant provisions of national legislation.

In order to safeguard the confidentiality of medical data, it is necessary to limit to the strict minimum the number of people required to handle the reimbursement of local staff members' medical expenses in accordance with article 66 of the FR and article 49 of the RAP.

2/ Having received the EDPS opinion of 3 July 2018 on reimbursement of medical expenses, the EEAS is taking into consideration their recommendations related to mitigation of risks by re-evaluating the procedures and tools to avoid unfairness of processing, discrimination, further use for different purposes of the data collected, unauthorised disclosure of data and other security risks which may be higher when sensitive data is processed by Delegation staff who are not medical professionals or health insurance specialists. A threshold assessment is also to be prepared to verify if a data protection impact assessment (DPIA) is to be conducted subsequently.

| | | |
|---|---|---|
| | | In order to comply with Art 5.1(a) and 10(3) of Regulation (EU) 2018/1725, at Delegation level, only the initiating agent, the Head of Administration (verifying agent) and the Head of Delegation (authorising officer) have access to the medical files. These Delegation staff members must sign a specific confidentiality declaration which contains the staff member's undertaking not to reveal such medical data or his/her interpretation thereof and not to use it in an unauthorised manner. It is also an acknowledgement that she/he will be liable to penalties if she/he does not fulfil the obligation to maintain confidentiality.<br>The EEAS launched a pilot project which aims, among other things, at concentrating the reimbursement of medical expenses and thus minimising the access to sensitive information at Delegation level. The RCE (a department set up within the EEAS) was therefore established to function as a regional service. It handles and administers reimbursements for 27 Delegations, thus mitigating the risks of unauthorised use of personal data.<br>4/ To be noted that the present data protection record is a model record. Model records are used when there are similar processing operations in several divisions, directorates, or in this case, in EU Delegations. It means that there will be only one record covering the same process for all EU Delegations. There is a central management of the present procedure and data processing determined by the relevant division of the EEAS. Therefore, with regard to the personal data processing operation, the controller is the division in HQ, which is responsible for determining the purpose and the means of the procedure. Although the Data Controller for the Model record is the organisational entity specified, each Delegation under the supervision of the Head of Delegation will be the joint o-controller responsible for processing personal data in compliance with the provisions of Regulation (EU) 2018/1725. |
| **15** | Rights of individuals | Individuals 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, individuals 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. The EEAS will consider the request, take a decision and communicate it to the individuals 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. For more detailed legal references, information can be found in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply.<br>If individuals have questions concerning the processing of their personal data, they may address them to the Data Controller via the following functional mailbox: LOCAL-AGENTS@eeas.europa.eu<br>Beyond correcting administrative errors, local agents are also entitled to supplement their file by adding opinions of other doctors to ensure the completeness of their file. |
| **16** | Information to data subjects | Information is provided to the Data Subjects<br>related to this Record in the Privacy Statement. The Privacy Statement or Data Protection Notice is accessible on the intranet of the EEAS. |