<table>
<thead>
<tr>
<th></th>
<th>Title of the processing activity</th>
<th>Administrative inquiries and disciplinary procedures in the European External Action Service (EEAS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Update of the record (last modification date)</td>
<td>04/12/2020</td>
</tr>
<tr>
<td>3</td>
<td>Register reference number</td>
<td>1701</td>
</tr>
</tbody>
</table>
| 4 | Identity and contact details of the Data Controller | European External Action Service (EEAS)  
Controller  

European External Action Service (EEAS)  

Directorate/Division responsible for managing the personal data processing operation:  

Secretariat General EEAS. SG  

Directorate General for Budget and Administration EEAS.BA  

Delegated Contact Entities:  

Directorate for Human Resources EEAS.BA.HR  

Advisors to the Directors of BA.HR  

Data Protection Officer:  

Emese Savoia-Keleti, SG.AFFGEN.DPO  

DATA-PROTECTION@EEAS.EUROPA.EU |
The processing of personal data in the framework of general administrative inquiries and disciplinary proceedings is a task performed in the public interest as provided for in the Staff Regulations as well as for the obligation to comply with the Staff Regulations.

Information is gathered and processed to allow the Appointing Authority (AA) or Authority Authorised to Conclude Contracts (AACC) of the EEAS, further referred to as AA to determine if a staff member has failed to comply with his/her obligations under the Staff Regulations and to proceed to disciplinary measures, if necessary. In that framework, processing of personal data is considered lawful.

In this context, the EEAS has concluded a Service Level Agreement (SLA) With DG HR/IDOC. Annex 6 to this SLA describes the services provided by IDOC.

It is further specified that the notification of IDOC DPO-63.9 mentions in point 9 that:

En vertu d’accords interservices (SLAs), l’IDOC peut être mandaté pour conduire des enquêtes, des procédures pré-disciplinaires et disciplinaires pour le compte d’autres institutions et organismes communautaires. Les procédures faisant l’objet de la présente notification s’appliquent dans ce cas aux membres du personnel de ces institutions et organismes en l’absence de procédures spécifiques adoptées par les institutions et organismes communautaires concernés.

Data are gathered and collected both by the EEAS and by IDOC, depending on the stage of the process.

The SLA describes the cases where IDOC does a prior check with OLAF. The EEAS also has an agreement with OLAF for cases directly referred to the Anti-fraud Office.

I. Administrative inquiries within the meaning of article 86 of the Staff Regulations and Annex IX to the staff regulations

The aim of administrative inquiries under Annex IX of the Staff Regulations is to explore a situation likely to concern a data subject's personal responsibility.

In the context of the SLA with DG HR/IDOC, the AA, informed of a situation with a possible disciplinary dimension, may also ask IDOC to proceed to an assessment of the case. IDOC issues recommendations:

- either not to follow up (non-case)
- or to open an administrative inquiry,
- or to organise a preliminary hearing directly.

Other sources of information can be OLAF or DG HR.E.2 in cases of article 24 SR requests for assistance.

II. Disciplinary proceedings, without prejudice to the responsibilities of the Disciplinary Board of the EEAS as organisational entity as regards processing of data

On the basis of the investigation report a pre-disciplinary hearing can be held at the request of the AA and further disciplinary proceedings may be launched by the AA against the data subject to determine whether and which disciplinary penalty should be imposed or not on the data subject.

The processing of personal data will intend:

By DG HR/IDOC : to conduct the hearing of the data subject addressing the possible breaches of the Staff Regulations and

By the Disciplinary Board of the EEAS: to issue a reasoned opinion to the AA of the EEAS on the appropriate penalty.

The processing of personal data will end with the data subject's final hearing and the decision by the AA.
**EEAS Personal Data Processing Record**

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

### Purpose of the processing activity

The processing of personal data in the framework of general administrative inquiries and disciplinary proceedings is a task performed in the public interest as provided for in the Staff Regulations as well as for the obligation to comply with the Staff Regulations.

Information is gathered and processed to allow the Appointing Authority (AA) or Authority Authorised to Conclude Contracts (AACC) of the EEAS, further referred to as AA, to determine if a staff member has failed to comply with his/her obligations under the Staff Regulations and to proceed to disciplinary measures, if necessary. In that framework, processing of personal data is considered lawful.

In this context, the EEAS has concluded a Service Level Agreement (SLA) with DG HR/IDOC. Annex 6 to this SLA describes the services provided by IDOC.

It is further specified that the notification of IDOC DPO-63.9 mentions in point 9 that:

> En vertu d'accords interservices (SLAs), l'IDOC peut être mandaté pour conduire des enquêtes, des procédures pré-disciplinaires et disciplinaires pour le compte d'autres institutions et organismes communautaires. Les procédures faisant l'objet de la présente notification s'appliquent dans ce cas aux membres du personnel de ces institutions et organismes en l'absence de procédures spécifiques adoptées par les institutions et organismes communautaires concernés.

Data are gathered and collected both by the EEAS and by IDOC, depending on the stage of the process.

The SLA describes the cases where IDOC does a prior check with OLAF.

The EEAS also has an agreement with OLAF for cases directly referred to the Anti-fraud Office.

### I. Administrative inquiries within the meaning of article 86 of the Staff Regulations and Annex IX to the Staff Regulations

The aim of administrative inquiries under Annex IX of the Staff Regulations is to explore a situation likely to concern a data subject's personal responsibility.

In the context of the SLA with DG HR/IDOC, the AA, informed of a situation with a possible disciplinary dimension, may also ask IDOC to proceed to an assessment of the case. IDOC issues recommendations:

- either not to follow up (non-case)
- or to open an administrative inquiry,
- or to organise a preliminary hearing directly.

Other sources of information can be OLAF or DG HR/E.2 in cases of article 24 SR requests for assistance.

### II. Disciplinary proceedings, without prejudice to the responsibilities of the Disciplinary Board of the EEAS as organisational entity as regards processing of data

On the basis of the investigation report a pre-disciplinary hearing can be held at the request of the AA and further disciplinary proceedings may be launched by the AA against the data subject to determine whether and which disciplinary penalty should be imposed or not on the data subject.

The processing of personal data will intend:

- By DG HR/IDOC: to conduct the hearing of the data subject addressing the possible breaches of the Staff Regulations and issue a report to the AA accompanied by a recommendation to close the case without a follow-up, or to issue a warning or to open a disciplinary procedure with or without referral to the Disciplinary Board
- By the EEAS Disciplinary Board: to issue a reasoned opinion to the AA of the EEAS on the appropriate penalty
- By the AA of the EEAS: to determine, following the preliminary phase, the necessity to initiate disciplinary proceedings or not, and upon completion of the disciplinary procedure, to hold the final hearing of the data subject with the assistance of DG HR/IDOC before deciding on the disciplinary penalty to be imposed to the data subject, following or not the involvement of the Disciplinary Board.

### Legal basis and lawfulness

**Legal bases at stake are as follows:**

- Article 86 and Annex IX of the Staff regulations, Articles 47,49,50,50a and 119 of the CEOS
- Service-Level Agreement concerning the collaboration between the EEAS and the EC, DG HR signed on 12/12/2012

Further reference

A Practical Guide on procedures and inquiries, pre-disciplinary and disciplinary proceedings adopted by IDOC is also at the disposal of the individuals concerned.

N.B. It is a not a legal basis as such, however it provides the individuals concerned information on the different stages of procedures and describes the rights and obligations of staff in these procedures. Part 6 of the guide has a reference to data protection.


Lawfulness of the processing:

- Article 5.1 (a) and (b) of the Regulation (EU) 2018/1725
- This processing was subject to article 27 of Reg. (EC) 45/2001.
Categories of individuals whose data is processed

- Data subjects

I. Administrative Inquiries
   - Officials
   - Temporary Agents
   - Contractual Staff
   - National experts and trainees
   - Local Agents
   - Staff posted in Delegations by the Commission subject to an investigation
   - Former officials or agents
   - Other individuals (e.g.: victim, witness, …) whose data may be processed in the frame of an administrative inquiry.

II. Disciplinary procedures
   - Officials
   - Temporary Agents
   - Contractual Staff
   - National experts and trainees
   - Local Agents
   - Staff posted in Delegations by the Commission subject to an investigation
   - Former officials or agents
   - Other individuals (e.g.: victim, witness, …) whose data may be processed in the frame of an administrative inquiry.

N.B. Disciplinary procedures involving Commission staff as concerned individuals will be dealt with by the European Commission. Local agents in the Delegations follow a different process and the process is notified by the Division for Local Agents (BA.HR.5, Record eDPO 1043: Disciplinary Measures for Local Agents in EU Delegations)

Categories of data - Data processed

- Names and personal information relating to facts, action or inaction of individuals under inquiry or concerned individuals in the pre-disciplinary or disciplinary procedures
- Legal assessment of facts, action or inaction according to the Staff Regulations and other obligations of the concerned individuals
- Data related to the personal responsibility of the individuals concerned including their financial responsibility (article 22 SR)
- Information including personal data of concerned individuals relating to offences, criminal convictions or security measures which are likely to be qualified as breach pursuant to SR obligations
- Information relating to sanctions taken
- Data mentioned in article 10(1) of Regulation (EU) 2018/1725 are in principle not collected nor processed unless, in exceptional cases, the data are relevant for the overall understanding of the facts and necessary for the assessment of the individual responsibility of the individual concerned.

N.B.
Information that is of no interest or relevance shall be promptly erased and not further processed.
### Recipients of data – Access to data

Recipients of the data include:

- The Appointing Authority
- Support staff of the AA
- Director General (EEAS DG BA)
- Director Human Resources (EEAS BA.HR)
- Director IBS (EEAS BA.IBS)
- Designated and relevant Heads of Divisions and Heads of Sectors within Directorate General Budget and Administration
- Investigations and Disciplinary Office (IDOC)
- EC Directorate-General Human Resources and Security (EC DG HR)
- Chairman, members and secretary of the EEAS Disciplinary Board
- Dedicated data operators in SYSPEAR
- EEAS Internal services (Legal Affairs Division, Internal Audit)
- Office for the Administration and Payment of individual Entitlements (PMO)
- EEAS and Commission Services in charge of access to the buildings
- ISIF
- European Ombudsman
- European Anti-Fraud Office (OLAF)
- European Data Protection Supervisor (EDPS)
- European Court of Justice and General Court
- Competent national authorities such as a national court

The type of recipient may vary according to the type of administrative inquiries, disciplinary proceedings, and the need to know basis for implementation purposes.

Any recipient of the data shall be reminded of their obligation not to use the data received for other purposes than the one for which they were transmitted.

### Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)

N/A

### Time limit for keeping the data - Retention period

Contrary to the initial provision as referred in EEAS/DGHR IDOC SLA, processing and storage of data is entirely entrusted to IDOC for reasons of homogenous and secured handling. This also applies to the retention of the files.

In particular, as described in point 13 of the notification DPO-63.9:

Les décisions de mise en garde adoptées par l'AIPN/AHCC aprs l'audition pr-disciplinaire sont versées au dossier individuel de la personne concernée pour une priede de 18 mois, les sanctions d'avertissement crit ou de blme adoptées l'issue de la procédure disciplinaire sont versées au dossier individuel pour une priede de 3 ans, les autres sanctions pour une priede de 6 ans. À l'issue de ces priedes, la personne concernée peut demander l'AIPN/AHCC que toute mention de la décision soit retirée de son dossier individuel. Le pouvoir disciplinaire appartient l'AIPN/AHCC. Tout refus ventuel doit tre motiv.

Les décisions de l'AIPN citant sans suite une procédure disciplinaire ne sont pas versées au dossier individuel de la personne concernée, sauf, exceptionnellement, si celui-ci en fait la demande.

Les dossiers considrs comme des 'non cas' l'issue de la phase d'valuation sont dtruits par l'IDOC.
Les dossiers constitus par l'IDOC dans l'exercice de ses fonctions d'enquête et de discipline sont conservs dans les archives de l'IDOC pendant les dures suivantes:
EEAS Personal Data Processing Record

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

Time limit for keeping the data

Contrary to the initial provision as referred in EEAS/DGHR IDOC SLA, processing and storage of data is entirely entrusted to IDOC for reasons of homogenous and secured handling. This also applies to the retention of the files.

In particular, as described in point 13 of the notification DPO-63.9:

Les décisions de mise en garde adoptées par l'AIPN/AHCC après l'audition pré-disciplinaire sont versées au dossier individuel de la personne concernée pour une période de 18 mois, les sanctions d'avertissement ou de blâme adoptées à l'issue de la procédure disciplinaire sont versées au dossier individuel pour une période de 3 ans, les autres sanctions pour une période de 6 ans. À l'issue de ces périodes, la personne concernée peut demander à l'AIPN/AHCC que toute mention de la décision soit retirée de son dossier individuel. Le pouvoir décisionnel appartient à l'AIPN/AHCC. Tout refus ventuel doit être motivé.

Les décisions de l'AIPN clôturant sans suite une procédure disciplinaire ne sont versées au dossier individuel de la personne concernée, sauf, exceptionnellement, si celui-ci en fait la demande.

Les dossiers considérés comme des 'non cas' à l'issue de la phase d'évaluation sont détruits par l'IDOC.

Les dossiers constitués par l'IDOC dans l'exercice de ses fonctions d'enquête et de discipline sont conservés dans les archives de l'IDOC pendant les durées suivantes:

- Les dossiers ayant donné lieu à une enquête administrative close sans suite sont conservés pendant 5 ans, de même que les dossiers ayant donné lieu à une procédure au titre de l'article 3 de l'annexe IX du statut dès lors que cette procédure n'a pas suivi d'une procédure disciplinaire. Il en va de même des dossiers constitués en vue de la rupture ventuelle du contrat d'un agent contractuel.

- Les dossiers ayant donné lieu à l'ouverture d'une procédure disciplinaire sont conservés pendant une période de 20 ans compté de la décision finale de l'AIPN/AHCC. Cette durée de conservation est justifiée au regard de l'obligation de tenir compte, en cas de sanction disciplinaire, d'une possible récidive comme de la conduite du fonctionnaire tout au long de sa carrière (article 10, lettres h et i de l'annexe IX du statut).

Les personnes concernées sont informées de ce que, même au cas où la sanction figurant dans son dossier personnel devrait en être retirée par application de l'article 27 de l'Annexe IX du Statut, celle-ci continuerait de figurer dans les dossiers de l'IDOC pendant les durées indiquées ci-dessus.

Les dossiers de l'IDOC ne peuvent être consultés que par le fonctionnaire concerné ou par l'autorité disciplinaire

It is specified that personal files of EEAS Staff (according to article 26 SR) are managed by the Commission on the basis of the SLA between the EEAS and DG HR. IDOC will communicate the decision directly to the service concerned to be included in the personal file.

In view of the revised EDPS Guidelines of 18 November 2016, the EEAS confirms the differentiation of inquiry and disciplinary files.

1. Pre-inquiry files that constitute a preliminary assessment of the collected information. As the case is dismissed, the maximum retention period of 2 years is not in contradiction of what has been described as EEAS practice.

2. Inquiry files are prepared, when an inquiry is launched and evidence is collected and interviews are conducted. In case the inquiry is closed without a follow up or a caution is issued, the file can be kept for 5 years after the closure of the investigation. The inquiry file needs to be transferred to the disciplinary file, if the disciplinary proceeding is launched on the basis of the evidence collected. For cases of the EEAS IDOC does so.

3. Disciplinary files are managed by IDOC, who is in charge of the disciplinary proceeding, as the EAS concluded an SLA with IDOC to carry out the disciplinary proceeding, and therefore evidence collected is transferred to IDOC. IDOC provides conclusions and the Appointing Authority adopts the decision. In certain cases the EEAS is obliged to keep OLAF reports and recommendations in order to inform OLAF of the actions taken following their recommendations.
13 Data Storage

As soon as the EEAS decides to refer a case to IDOC, contrary to the initial provision as referred in EEAS/DGHR IDOC SLA, processing and storage of data is entirely entrusted to IDOC for reason of homogenous and secured handling.

As mentioned in the privacy statement of IDOC:
Toutes les données en format électronique (courriels, documents, données télesignées, etc.) sont stockées sur un drive encrypt dont l’accès est limité aux membres de l’IDOC. Elles sont conservées sur les serveurs de la Commission : la décision de la Commission C (2006) 3602 du 16 oct 2006 relative la scurité des systèmes d’information utilisés par les services de la Commission leur est applicable.

Toutes les données en format papier sont conservées dans des locaux sécurisés accessibles aux seuls membres de l’IDOC.

Main guiding provisions

In particular THE FILE, which may become the disciplinary file is kept by IDOC.
Communication with the EEAS designated recipients is done via ARES under the marking inquiries and disciplinary procedure.

The EEAS does not keep printed versions of the file. There is a limited archiving in ARES of the communications with IDOC at the AA’s level only accessible to a restricted number of recipients.

14 General description of security measures

Appropriate security measures of personal data are ensured both by organisational and technical measures, in particular by limited access to data through restrictions and (only restrictions apply – no encryption of data) guaranteed for authorised members of EEAS management staff as well as through safety measures for paper files.

Outline on security measures

Physical files during the process of the administrative inquiries and disciplinary procedures are locked in cupboards on BA.HR premises.
Complete physical files are kept by IDOC.
Use of investigations and disciplinary matters marking in Ares*. In case of email exchanges, the transmission of such documents is encrypted by using SECEM email.
Upon instruction of EEAS.BA.HR, the DMO manages the list of staff needing to read documents marked with the security marking Investigations and disciplinary matters.
Related ARES files are attached to the EEAS the filing plan heading 12.007.100.200 Human Resources /Legal Advice, Statutory Issues. Access to ARES files is restricted to staff having the need to know. EEAS.BA.HR identifies who has the right to access the files and asks the DMO to implement such access in Ares. The management of marking lists and restrictions of access to Ares files is therefore a double security applied to such cases.
Access to Ares files under heading 12.007.100.200 is granted for the period until the user has the assigned position/function, even if s/he continues to have access to staff matter / inquiries and disciplinary procedures.
Access needs to be requested and authorised for new staff members, and access needs to be withdrawn by a notification to the DMO.
Security is also ensured by the safety measures built in the various IT applications.
Electronic files are password-protected and the access is an EU LOGIN/EU Login-authenticated process**.
Measures are provided by DIGIT to prevent non-responsible entities from accessing data.

Description on organisational measures

Organisational measures include appropriate access rights and access control precautions. More specific, access to the data ARES file is granted according to the level of responsibility of the user, from DMO to the AA's level only accessible to a restricted number of recipients.

Security is also ensured through organisational measures such as:

- Use of strong authentication systems.
- Encryption of data during transmission.
- Access control mechanisms.
- Regular periodic reviews of access rights.
- Training of staff on data protection.
- Audit trails of data access and use.
- Limited access to sensitive data.
- Regular data backups and disaster recovery plans.
- Restricting access to data to only those with a need to know.
- Use of secure IT equipment and networks.
- Regular assessments of the security of IT systems.
- Use of secure communication channels.
- Use of secure file transfer protocols.
- Use of secure document management systems.
- Use of secure printing and scanning devices.
- Use of secure disposal methods for sensitive data.
- Use of secure data destruction methods.
- Use of secure access control mechanisms.
- Use of secure data backup and recovery procedures.
- Use of secure data encryption and decryption methods.
- Use of secure data storage and retrieval methods.
- Use of secure data transfer and transmission methods.
- Use of secure data indexing and searching methods.
- Use of secure data monitoring and logging methods.
- Use of secure data aggregation and reporting methods.
- Use of secure data analysis and visualization methods.
- Use of secure data visualization and reporting methods.
- Use of secure data dissemination and distribution methods.
- Use of secure data sharing and collaboration methods.
- Use of secure data management and governance methods.
- Use of secure data governance and compliance methods.
- Use of secure data quality and assurance methods.
- Use of secure data integrity and authentication methods.
- Use of secure data confidentiality and non-repudiation methods.
- Use of secure data availability and backup methods.
- Use of secure data redundancy and failover methods.
- Use of secure data scalability and performance methods.
- Use of secure data security and risk management methods.
- Use of secure data compliance and regulatory methods.
- Use of secure data storage and archiving methods.
- Use of secure data storage and retrieval methods.
- Use of secure data transfer and transmission methods.
- Use of secure data indexing and searching methods.
- Use of secure data monitoring and logging methods.
- Use of secure data aggregation and reporting methods.
- Use of secure data analysis and visualization methods.
- Use of secure data visualization and reporting methods.
- Use of secure data dissemination and distribution methods.
- Use of secure data sharing and collaboration methods.
- Use of secure data management and governance methods.
- Use of secure data governance and compliance methods.
- Use of secure data quality and assurance methods.
- Use of secure data integrity and authentication methods.
- Use of secure data confidentiality and non-repudiation methods.
- Use of secure data availability and backup methods.
- Use of secure data redundancy and failover methods.
- Use of secure data scalability and performance methods.
- Use of secure data security and risk management methods.
- Use of secure data compliance and regulatory methods.
- Use of secure data storage and archiving methods.
- Use of secure data storage and retrieval methods.
- Use of secure data transfer and transmission methods.
- Use of secure data indexing and searching methods.
- Use of secure data monitoring and logging methods.
- Use of secure data aggregation and reporting methods.
- Use of secure data analysis and visualization methods.
- Use of secure data visualization and reporting methods.
- Use of secure data dissemination and distribution methods.
- Use of secure data sharing and collaboration methods.
- Use of secure data management and governance methods.
- Use of secure data governance and compliance methods.
- Use of secure data quality and assurance methods.
- Use of secure data integrity and authentication methods.
- Use of secure data confidentiality and non-repudiation methods.
- Use of secure data availability and backup methods.
- Use of secure data redundancy and failover methods.
- Use of secure data scalability and performance methods.
- Use of secure data security and risk management methods.
- Use of secure data compliance and regulatory methods.
General description of security measures

Appropriate security measures of personal data are ensured both by organisational and technical measures, in particular by limited making it available for use.

EU LOGIN includes supports for stronger types of authentication, but organisational and other measures are required before credentials can take many forms, but initially EU LOGIN will only use passwords. Password authentication relies on authentication, but if the rules for the password usage and composition are good enough, it can be sufficient for most applications of credentials is minimised or eliminated.

EU LOGIN provides a set of mechanisms, procedures and rules that endeavour to ensure that the chances of fraudulent use of credentials is minimised or eliminated. Successful authentication is not a 100% guarantee that the user is the individual to whom the credentials belong, only that the user was able to present correct credentials for the claimed identity.

The access for electronic files is secured through DIGIT security measures and the authentication system of EU LOGIN. Only people having received both the right to read the marking and to have access to the file will be allowed to consult the document. The marking used is Staff matters. The digitised document can be attached to the corresponding ARES record.

Administrative inquiry and disciplinary files will be stored in locked cupboard managed by EEAS.BA.HR and located in their premises. Access is granted only to authorised staff.

* Advanced Records System (ARES)
The HERMES–ARES–NOMCOM (HAN) is an IT system of the European Commission. ARES is a document management system, linked to HERMES, used by the European Commission and Executive Agencies. ARES is hosted on secure servers of the Commission.

Electronic documents containing personal data will be transferred and archived via ARES which provides security for sensitive documents in two simultaneous ways: the marking and the filing.

The marking: A special marking is to be applied when personal data is processed in the context of administrative inquiry and disciplinary investigations. The marking used is Staff matters. The digitised document can be attached to the corresponding ARES record.

Filing: In order to ensure limited access to a file, a predefined group of users identified by the controller shall be created. The file will only be visible to the predefined group identified by the controller.

Only people having received both the right to read the marking and to have access to the file will be allowed to consult the documents.

The Audit trails for data processing and communication will be done via ARES workflow. Considering the use of ARES for each transmission and storage of personal data according to the above mentioned measures, no undue removal or undue transmission will be possible.

** EU LOGIN/EU-Login system (EU LOGIN is the system replacing ECAS as of October 2016)
The access for electronic files is secured through DIGIT security measures and the authentication system of EU LOGIN.

EU LOGIN is the European Commission Authentication Service that enables web applications to authenticate centrally with a common strong password, offering more security than the current LDAP password. It offers also single sign-on between applications using it.

Authentication means verifying the credentials of a user. Credentials usually consist of some kind of identifier (e.g. a username) and an element such as a password that has been linked to the identifier.

Successful authentication is not a 100% guarantee that the user is the individual to whom the credentials belong, only that the user was able to present correct credentials for the claimed identity.

EU LOGIN provides a set of mechanisms, procedures and rules that endeavour to ensure that the chances of fraudulent use of credentials is minimised or eliminated.

Strong authentication is one of these mechanisms. Passwords are considered to be one of the weakest kinds of authentication, but if the rules for the password usage and composition are good enough, it can be sufficient for most applications that deal with 'sensitive', but not classified information.
### Rights of individuals

Data subjects have the right to access their personal data and the right to correct any inaccurate or incomplete personal data, as well as to request the removal of their personal data if unlawfully processed according to pre-defined provisions aligned with IDOC activity, which will be implemented within 10 working days once the request has been deemed legitimate.

The aforementioned access rights are granted as follows to the person under investigation, pre-disciplinary or disciplinary procedure as defined in point 12 of the notification of IDOC DPO-63.9.

**Au titre des articles 1 et 2 de l’Annexe IX du Statut et de l’article 4(4) de la décision IDOC, la personne concerne a le droit d’exprimer ses commentaires sur les conclusions d’un rapport d’enquête administrative, dans la mesure où celles-ci font état de faits la concernant avant que le rapport d’enquête ne soit finalisé et transmis à l’AIPN/AHCC pour suite appropriée. Le rapport d’enquête fait état de ces commentaires, qui y sont annexés.**

Lorsque la procédure pr-disciplinaire est ouverte, la suite d’une enquête simplifiée, conduite sous la forme d’un examen des documents portant la connaissance de l’IDOC, la personne concerne est informée des faits la concernant avant son audition au titre de l’article 3 de l’annexe IX du statut et peut les commenter, les compter ou les rectifier avant la décision ventuelle de l’AIPN/AHCC d’ouvrir une procédure disciplinaire son encontre.

Lorsque l’AIPN/AHCC décide de l’ouverture d’une procédure pr-disciplinaire (article 3 de l’annexe IX), la personne concerne reçoit un exemplaire de toutes les pièces du dossier la concernant, sous réserve, le cas chant, de la protection du droit des tiers. Elle peut alors commenter et rectifier, le cas chant, les données qui seraient inexactes. Elle peut également au cours de la procédure pr-disciplinaire compiler ces données par l’ajout de tout document qu’elle estime utile.

La personne concernée par une procédure disciplinaire a le droit d’obtenir la communication intégrale du dossier qui la concerne et de prendre copie de toutes les pièces de la procédure.

Le droit d’accès aux dossiers, de vérification et de rectification ventuelle des données personnelles s’y trouvant est reconnu à toutes les personnes concernées par des enquêtes et des procédures pr-disciplinaires et disciplinaires une fois celles-ci clôturées. Ces règles sont systématiquement communiquées lors du premier entretien avec la personne concerne. Il lui est remis, cette occasion, une copie de la partie VI du guide pratique de l’IDOC qui traite de la protection des données personnelles.

En cas de refus d’accès aux données (article 25.1 b) et h) du règlement (EU) 2018/1725), la personne concerne peut saisir le Contrôleur européen pour la protection des données qui examinera si les données sont traitées correctement et, dans la négative, fera apporter toutes les corrections nécessaires.

If the data subject has any queries or request concerning the processing of his/her personal data, s/he may address them to the data controller, depending on the stage and matter of the processing at the following functional mailbox in the EEAS: `HUMAN-RESOURCES@eeas.europa.eu` or at the address of IDOC, as indicated directly to the person concerned.
I. Information to the Data Subject by the EEAS

A Privacy Statement linked to this Record contains information for the Data Subject(s).

II. Involvement of IDOC in the process of providing information to the Data Subject

According to the SLA with the European Commission, it is IDOC, who is in contact with data subjects during the inquiry and is able to provide information to the data subjects about their rights and on the details of the data processing.

Once the AA decides to open an inquiry and provides the required mandate to IDOC, IDOC takes steps to inform the individual(s) concerned as soon as appropriate.

Therefore, reference should be made to the EC DG HR notification DPO-63.9 relating to Enquêtes administratives et procédures disciplinaires internes de la Commission européenne

http://ec.europa.eu/dpo-register/details.htm?id=41787

The individual concerned is informed, at the latest on his/her first hearing by IDOC of his/her rights under regulation (EU) 2018/1725 by handing a copy of part VI of the practical guide of IDOC. The privacy statement of IDOC will apply for any activity of IDOC pursuant to the role defined in the SLA.

In particular:

L'ouverture d'une enquête administrative est notifiée la personne concerne en vertu et dans les conditions de l'article 4(4) de la décision IDOC. Celle-ci est également informée de la décision de l'AIPN de l'entendre au titre de l'article 3 de l'annexe IX du statut en vue d'apprécier le bien-fondé de l'enquête et de la procédure disciplinaire. L'ouverture d'une procédure disciplinaire est notifiée à la personne concerne en vertu et dans les conditions de l'Annexe IX du Statut. Si la personne concerne n'avait pas été informée de l'ouverture de l'enquête en raison de la nuisance potentielle que cette information aurait pu causer au déroulement de l'enquête, l'IDOC l'informerait de la disparition de cette nuisance, et ce, aussitôt après cette disparition. La rétention d'information qu'autorise l'article 1(1) de l'Annexe IX du Statut ne peut en effet durer que le temps nécessaire au bon déroulement de l'enquête. La personne concerne est informée, au plus tard lors de sa première audition par l'IDOC, de ses droits au titre du règlement (UE) 2018/1725, par la remise d'une copie de la partie VI du Guide pratique de l'IDOC qui mentionne, notamment, l'identité du responsable du traitement, la finalité et la base légale de celui-ci, l'origine des données transmises à l'IDOC et la durée de conservation de celles-ci. S'agissant d'un 'non cas', les personnes concernées sont informées de leurs droits par la déclaration de confidentialité qui figure sur la page réservée à l'IDOC du site web europa. Liste des pièces jointes : - partie VI du Guide pratique - déclaration de confidentialité

Part VI IDOC Guide FR.pdf
Privacy statement IDOC 2016.doc