

## Data Protection Notice

### Staff Administration

(17 December 2018)

This Data Protection Notice is provided to you in order to explain the policy of the Agency for the Cooperation of Energy Regulators (the “**Agency**”) regarding your privacy, as well as how your personal information is handled in the context of the administration of the Agency’s Temporary and Contract Staff Members (“**Staff Members**”), as well as temporary agency workers, trainees and Seconded National Experts (“**SNEs**”), including the processing of personal data deriving from the use of the Agency’s internal IT tools. This Data Protection Notice also covers the handling of personal information related to individuals who are members or alternates of the Agency’s Boards.

### Who is responsible for my personal information?

The Agency is the data controller regarding all Personal Data processing carried out in the context of the administration of Staff Members, temporary agency workers, trainees and SNEs engaged by the Agency, as well as members / alternates of the Agency’s senior management and the Boards.

To get in touch with the Agency’s Data Protection Officer, please contact: [dpo@acer.europa.eu](mailto:dpo@acer.europa.eu).

### What personal information of mine is being collected?

When managing your relationship with the Agency, the Agency collects and processes information related to you (as an individual), which, either by itself or together with other information to which the Agency has access, allows you to be identified. This is also the case where, in connection with the performance of the tasks and duties you have at the Agency, you make use of the Agency’s IT tools – such as the Agency’s intranet and corporate equipment (as explained further in the Agency’s Policy on IT Tools).

The Agency may also be able to collect and process information regarding other persons in this same manner, if you choose to provide it to the Agency.

This information may be classified as “**Personal Data**”.

Personal Data which may be processed by the Agency in the context of the administration of Staff Members (and of temporary agency workers, trainees and SNEs, as well as members / alternates of the Agency’s senior management and Boards, where applicable) are as follows:

(a) **Administration data**

The Agency collects Personal Data as needed to manage your working relationship with the Agency. These may include, but are not limited to, the following categories:

- name and surname;
- gender;
- scans of your ID card or similar documents;
- Slovenian Unique Master Citizen Number (EMSO number);
- Slovenian tax number;
- personal e-mail address;
- digital business portraits / photographs;
- information related to your family situation (e.g., marriage and birth certificates);
- information contained within your CV, Declaration of Interests and Compliance Commitment, where required (e.g., related to your professional experience, education, training, publications, interests held which may be considered as potentially affecting your independence);
- certificates related to your proficiency in a third language, in order to verify compliance with the Staff Regulations of Officials of the European Union ("**Staff Regulations**") and Conditions of Employment of Other Servants ("**CEOS**"), in case of participation in annual reclassification procedures;
- professional details, such as your professional contact details, personnel number, category, grade, working status, contract type and job title;
- recorded working hours, accumulated time credits / debits and relevant comments related to hours worked (for Staff Members working under Flexitime arrangements – hours worked by temporary agency workers are also recorded);
- user credentials and start / end of remote working periods (for Staff Members working remotely);
- information relating to your skills, career progression and competences (e.g., language proficiency), training requests you submit and all attended and completed training courses;
- financial data, such as your salary, IBAN and related bank account details, amounts paid and received related to "petty cash requests" you submit, allowances paid to you (e.g., education allowances), as well as information related to corporate credit cards issued to you (and the expenses charged to those cards);
- expenses you incur in the performance of tasks and duties on behalf of the Agency (e.g., related to the use of professional phones);
- overall assessment of your working performance and individual qualitative reports from past annual appraisal exercises; for Staff Members to whom the point system applies, the Agency also processes the number of reclassification / reclassification points awarded in past reclassification exercises;
- information related to your participation in events, workshops, missions on behalf of the Agency (e.g., locations, expenses incurred and claimed);
- your car plate number, VIN number and brand (if your car is registered in Slovenia and/or you wish to benefit from reserved parking spaces at the Agency's premises);
- any additional information, which may concern you, gathered in connection with complaints, requests, administrative inquiries, disciplinary proceedings or reports submitted to or initiated at the Agency (including, e.g., complaints / requests filed under Article 24, Article 22c, Article 90(1) and/or Article 90(2) of the Staff Regulations), informal anti-harassment procedures (involving external confidential counsellors), as well as formal anti-harassment procedures, under Decision AB No. 6/2017 of the Agency's Administrative Board of 16 March 2017, and reports filed via internal whistleblowing channels, under Decision AB No. 9/2018 of the Agency's Administrative Board of 7 June 2018, in relation to the prevention of fraud, corruption and any illegal activity detrimental to EU interests, where this

information is adequate, relevant and necessary for the purposes for which it was gathered;

- any additional information, which may concern you, submitted to the Agency in connection with requests related to the work and absence management, including requests for leave (holidays, sick or unpaid leave – including for temporary agency workers), teleworking arrangements or the carrying out of outside activities, sensitive functions, where this information is adequate, relevant and necessary for the purposes for which it was gathered.

**(b) IT Tools monitoring**

Whenever, in performing your duties and tasks on behalf of the Agency, you use any work-related IT tool provided by the Agency, including when connecting to the Agency's intranet (by VPN or directly), using the Agency's e-mail / webmail systems or using Skype for Business for instant messaging and/or conference calls, the Agency collects a limited amount of Personal Data on you, in the form of your name, as well as the IP and MAC addresses of the device you are using. This happens due to the standards and protocols the network devices are conforming to, and is necessary to allow them to operate properly.

The Agency also collects information on any attempts to log onto Agency devices and IT tools – including online portals maintained by the Agency – and keeps logs of any access and activities carried out (including any pages and/or files read, modified or deleted). Additionally, aggregated logs (meaning, logs which do not identify particular users) are generated regarding access and use of certain Agency IT Tools, such as (but not limited to) the Agency's intranet, operating systems, exchange server (used for the operation of e-mail and webmail accounts) and Active Directory system.

Please refer to the Agency's Policy on IT Tools for more information on why and how this information may be collected and used by the Agency.

**(c) Special categories of Personal Data**

Special categories of Personal Data include information revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data related to you or data concerning your health, sex life or sexual orientation. Additionally, for the purposes of this Data Protection Notice, Personal Data relating to offences, criminal convictions or security measures will also be considered as special categories of Personal Data.

Staff Members may be required to perform pre-employment medical checks prior to beginning their functions at the Agency; however, these checks are carried out by the Medical Service of the European Commission's Directorate-General for Human Resources and Security ("**DG HR**"), and the Agency is informed only whether the check has been satisfactorily passed, without having access to any Personal Data related to your health.

Furthermore, when you submit a request for sick leave, any processing of Personal Data related to your health which may be needed to process that request (e.g., medical certificates) is carried out by DG HR; the Agency is only informed whether the request for sick leave is confirmed, and what the expected duration of the leave is.

Additionally, in the context of the management and investigation of complaints, informal and formal harassment proceedings, administrative inquiries, disciplinary proceedings and reports related to whistleblowing, other special categories of personal data may be collected regarding persons involved in the investigation (including Personal Data related to suspected criminal offences) – depending, naturally, on the nature of the complaint or acts investigated.

The Agency only processes any special categories of Personal Data where your explicit consent is given, or where another legal basis for processing can be relied on (such as the need to process these data in order to comply with the Agency's specific rights and obligations in the field of employment law), and in any case only where this is deemed adequate, relevant and necessary in the context of the processing purposes provided in this Data Protection Notice. In particular, any Personal Data gathered during internal investigations carried out as a result of complaints, informal and formal harassment proceedings, administrative inquiries or disciplinary proceedings which are of no interest or relevance to those investigations will be promptly erased and not further processed.

**(d) Other persons' Personal Data**

As a Staff Member or individual otherwise engaged by the Agency, information on your family situation, as well as documentation evidencing this (such as marriage and birth certificates), is collected by the Agency. This information and documentation contains Personal Data related to your family members.

Additionally, in some instances, Staff Members and other individuals engaged by the Agency may be able to disclose to the Agency (inadvertently or not) Personal Data related to other persons. This is true, e.g., regarding requests made by Staff Members for the Agency to enter into tuition agreements with education institutions for their children, or to contribute towards education fees for their children (as Personal Data related to those children will be requested by the Agency, such as their name and date of birth). The Agency may also collect information on your family members where necessary to support the payment of certain allowances to you (e.g., household allowances, child allowances).

Please note that, in any situation where you decide to share Personal Data related to other persons, you will be considered as an independent controller regarding those Personal Data – meaning you will be held responsible for that decision. In turn, this means, among other things, that you may be held liable for any complaints, claims or demands for compensation which are brought against the Agency, due to the fact that you decided to share Personal Data related to other persons with the Agency.

As such, you must make sure that you are legally entitled to provide the Agency with this information (e.g., because you have the consent of the other persons to whom the Personal Data relate, or are able to provide consent for them, because a legal obligation to inform the Agency exists, because this information is provided in the performance of a task in the public interest, etc.).

## Why is the Agency using these Personal Data?

The Agency uses these Personal Data for the following purposes:

**(a) Human Resource Management**

To manage your working relationship with the Agency, under the terms of the agreement signed with the Agency.

This includes onboarding you as a Staff Member, temporary agency worker, trainee or SNE. It also includes handling requests you make (e.g., training requests, leave requests, support requests / help tickets, petty cash requests, VAT refund requests, requests for legal advice), assigning tasks and duties to you (including the completion of training courses), managing your work schedules and absences (particularly for Staff Members working under Flexitime arrangements or remotely) and, in general, performing administrative functions tied to your work and use of the Agency's facilities and benefits (e.g., managing events and missions in which you take part, keeping track of books you borrow from the Agency's library, ordering business cards and Urbana Cards for Staff Members, issuing and managing the use of corporate credit cards), as well as other related activities.

Specifically regarding Flexitime arrangements, the Agency processes Personal Data in order to record hours worked by Staff Members, including by automated means, while allowing them to vary the time at which they start and finish their work, as well as to recover accumulated excess hours.

- Having signed an agreement with the Agency, it is contractually mandatory for Personal Data to be shared with the Agency for this purpose; failure to do so will prevent the agreement from being properly performed, which may hinder or prevent your working relationship with the Agency, or prevent the Agency from adequately responding to any requests you make.

**(b) IT Management**

To allow you to use the Agency's IT infrastructure, tools and online portals, and to ensure the security, availability, integrity and confidentiality of that infrastructure, as well as those tools and portals, as well as to allow internal auditing of their access and use;

**(c) Payroll / Expense Reimbursement**

To pay salaries and other sums due to you (e.g., allowances), as well as to process any other associated payments (e.g., social security contributions, pensions) and reimburse expenses validly claimed (e.g., removal expenses, etc.);

- Having signed an agreement with the Agency, it is contractually mandatory for these Personal Data to be shared with the Agency; failure to do so will prevent the agreement from being properly implemented – in particular, this will prevent the Agency from making any payments to you.

**(d) Evaluation of Probationary Period Reports, Yearly Performance Appraisal and Reclassification Exercises**

To allow the Agency to assess the performance of Staff Members, to evaluate probationary reports regarding Staff Members subjected to probation periods and to create reports in order to provide regular and structured feedback to Staff Members, with the aim to improve performance, contribute to future career development and identify training needs.

In particular, appraisal exercises seek to create reports to assess the fulfilment of the objectives and performance indicators previously set, providing a qualitative appraisal of Staff Members' individual performance for the reporting period from 1 January to 31 December of the previous year, and including a conclusion as to whether that performance has been deemed satisfactory or not.

Reclassification exercises, which are carried out once the appraisal exercise organised in the same year has been finalised, aim to determine whether a Staff Member may be classified in the next higher grade within his/her function group, based on factors such as their time of permanence in their current grade, the comparative merits of Staff Members eligible for advancement to a higher grade and previous reports produced on those Staff Members.

- It is mandatory for you to share Personal Data for this purpose, as failure to do so would prevent the correct performance of the work relationship and functioning of the Agency.

**(e) Management of Contracts and Internal Documents**

To register and manage the documents stored by the Agency, by keeping track of Staff Members and other individuals which make entries in the Agency's electronic repository for contracts and other documents, e.g., when using the Agency's document management tools or SharePoint applications.

- It is mandatory for you to share Personal Data for this purpose, as failure to do so would prevent the correct performance of the work relationship and functioning of the Agency.

**(f) Management of Requests and Complaints**

To handle requests and complaints you submit to the Agency, including:

- Complaints regarding the way in which you, or the person(s) identified in a report you submitted, were treated after, or in consequence of fulfilment of obligations to report any facts leading to a presumption of the existence of possible illegal activities detrimental to the interests of the Union, or of conduct relating to the discharge of professional duties which may constitute a serious failure to comply with the obligations imposed upon civil servants of the Union;
- Requests for assistance, in proceedings against any persons perpetrating threats, insults, defamatory acts / utterances or any attacks to you or your family, or you or your family's property, caused by reason of your position within the Agency;
- Applications for the Agency to take any relevant decisions related to you;
- Complaints regarding acts which affect you adversely, as a result of a decision taken by the Agency or any perceived failure by the Agency to adopt measures prescribed by the Staff Regulations and the CEOS.

- It is mandatory for you to share Personal Data for this purpose, as failure to do so would prevent the correct performance of the work relationship and functioning of the Agency.

**(g) Informal and Formal Anti-Harassment Procedures**

To manage internal anti-harassment measures.

This includes the use of Personal Data, in line with the principle of confidentiality, in order to e.g.:

- Implement any preventive measures which may be deemed appropriate;
- Provide information and provide general advice and training to Staff Members;
- Appoint confidential counsellors and assist them in carrying out their operations within the context of an informal procedure;
- In the context of informal procedure, direct alleged victims towards confidential counsellors;
- Monitor the Agency's policy on these procedures, so as to assess its impact and effectiveness;
- Take appropriate steps with regards to initiating/conducting a formal procedure on the basis of a request for assistance under Article 24 of the Staff Regulations, concerning the Agency's obligation to provide assistance in order to determine the facts of the case/apportionment of any responsibility.
  - It is mandatory for these Personal Data to be shared with the Agency for this purpose, as failure to do so would impede or prevent the Agency from correctly managing these complaints, inquiries and proceedings, as mandated by law.

**(h) Administrative Inquiries and Disciplinary Proceedings**

To manage internal proceedings triggered in order to establish whether Staff Members/SNEs breached their statutory and/or contractual obligations, which may result in sanctions when deemed appropriate (e.g., warnings or penalties). Personal Data collected are compiled into a file which will serve as the documental basis for these inquiries and proceedings.

- It is mandatory for these Personal Data to be shared with the Agency for this purpose, as failure to do so would impede or prevent the Agency from correctly managing these complaints, inquiries and proceedings, as mandated by law.

**(i) Whistleblowing**

To manage any reports received from Staff Members, or other individuals engaged by the Agency, regarding facts discovered in the course of, or in connection with, their duties and which point to the existence of serious irregularities – i.e., illegal activities, including fraud and corruption, as well as serious professional wrongdoings – via internal channels within the Agency.

Personal Data concerning you may be processed for this purpose, e.g., where you make such a report, where you are quoted in a report, where you are indicated as a witness to the facts reported or accused of wrongdoings within a report.

Note that, as set out in Decision AB No. 9/2018 of the Administrative Board of the Agency of 7 June 2018, any individuals which make such reports in bad faith – particularly where basing a report on knowingly false or misleading information – will not be entitled to the protection afforded to good faith reporters (e.g., confidentiality of whistle-blowers' identity) and may be subjected to disciplinary measures.

- It is mandatory for these Personal Data to be shared with the Agency for this purpose, as failure to do so would impede or prevent the Agency from correctly managing these complaints, inquiries and proceedings, as mandated by law.

**(j) Internal Newsletter**

To allow the Agency to distribute its internal newsletter to Staff Members and other individuals engaged by the Agency, containing updated and reliable information on news and developments related to the Agency, and which includes Personal Data on joiners or leavers to the Agency, or on individuals appointed as Agency Board members.

**(k) Publication of Photographs**

To increase transparency and to ensure identification of the members of the Agency's Senior Management and Boards (on the Agency's website) and of other Staff Members (on the Agency's intranet).

- It is not mandatory for Personal Data to be shared with the Agency for this purpose, and no adverse consequence will arise for you if you choose not to.

**(l) Registration and Publication of CVs, Declarations and Commitments**

To establish and operate a register of declarations of interests for the Agency's Senior Management and for members and alternates of the Boards (including the Administrative Board, the Board of Regulators and the Board of Appeal), as well as for certain other categories of Staff Members, in order to detect potential or actual conflicts of interest and, regarding Senior Management, members and alternates of Boards and certain categories of Staff Members, to publish these declarations (along with CVs and Compliance Commitments, where necessary) on the Agency's website, for transparency purposes.

- It is mandatory for these Personal Data to be shared with the Agency for this purpose, as failure to do so would be contrary to legal obligations imposed upon the Agency and the individuals in question.

**(m) Selection Committee Disclosure**

To disclose information related to Staff Members which are members of the Agency's Selection Committee on the Agency's website, as well as to individual candidates and applicants to positions within the Agency.

- While it is not strictly mandatory to provide your Personal Data to the Agency for publication on the Agency's website as a member of the Selection Committee (as you may be entitled to object to this, on compelling legitimate grounds relating to your situation), it is mandatory to provide those Personal Data for disclosure to candidates which are invited to a written test and oral interview; where you choose not to, you may not take part in the Selection Committee.

(n) **Information Exchange**

To disclose information related to Staff Members, and other individuals engaged by the Agency, to requesting permanent representations, embassies and consulates of the EU.

- It is only mandatory to provide your Personal Data to the Agency for this purpose where the request made falls under Article 15, second subparagraph, of Protocol no. 7 of the TFEU ("*The names, grades and addresses of officials and other servants [included in categories defined by the EU Parliament and Council] shall be communicated periodically to the governments of the Member States*"). Any requests falling outside of this scope will be responded to only with your prior consent.

(o) **Compliance**

To comply with Union or Member State laws which impose upon the Agency the collection and/or further processing of certain kinds of Personal Data.

- It is mandatory for individuals to share Personal Data for this purpose, as failure to do so would be contrary to a legal obligation imposed upon the Agency and/or those individuals.

All Personal Data processed by the Agency may further be included in periodic backups carried out to ensure the availability of information stored on the Agency's IT systems, and may further be processed to ensure the appropriate handling of security incidents related to those systems, as well as the Agency's compliance with its legal obligations regarding the processing of Personal Data (e.g., related to management of personal data breaches).

## Why can the Agency use these Personal Data?

The legal bases which the Agency relies on to process these Personal Data, according to the purposes identified above, are as follows:

(a) **Human Resource Management**

Processing for this purpose is necessary for the Agency to perform the employment agreements entered into with its Staff Members and other agreements entered with the representatives/employers of temporary agency workers, and directly with trainees and SNEs, or otherwise for the Agency to respond to work-related requests

made by those individuals; furthermore, this processing is also necessary to allow the Agency to comply with the rules laid down in EU Civil Service Law – in particular, in the Staff Regulations and CEOS – as well as for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest.

In particular, processing carried out related to Flexitime arrangements is necessary in order to comply with the rules laid down in the Staff Regulations and CEOS, but also in EU Commission Decision C(2014) 2502, of 15 April 2014, on working time, applicable to the Agency by analogy in accordance with Article 110(2) of the Staff Regulations.

Any processing of special categories of Personal Data by the Agency is carried out only to the extent that it is necessary for the purposes of complying with the Agency's specific rights and obligations in the field of employment law (as established in Union law or otherwise authorised by the European Data Protection Supervisor).

**(b) IT Management**

Processing for this purpose is necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest.

**(c) Payroll / Expense Reimbursement**

Processing for this purpose is necessary for the Agency to perform the employment (or similar) agreements entered into with its Staff Members, or otherwise for the Agency to respond to requests made by its Staff Members.

**(d) Evaluation of Probationary Period Reports, Yearly Performance Appraisal and Reclassification Exercises**

Processing for this purpose is necessary for the Agency to perform the employment (or similar) agreements entered into with Staff Members (where applicable, given the terms of the agreement).

Furthermore, this processing is also necessary to allow the Agency to comply with the rules laid down in:

- The Staff Regulations and CEOS;
- Decision AB No. 22/2015 (17 December 2015), of the Administrative Board of the Agency;
- Decision AB No. 23/2015 (17 December 2015), of the Administrative Board of the Agency;
- Decision AB No. 06/2016 (4 April 2016), of the Administrative Board of the Agency;
- Decision AB No. 07/2016 (4 April 2016), of the Administrative Board of the Agency;
- Director Decision No. 2016-3, of the Director of the Agency on Team Leaders as reporting officers.

This processing is also necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest.

**(e) Management of Contracts and Internal Documents**

Processing for this purpose is necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest.

**(f) Management of Requests and Complaints**

Processing for this purpose is necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest; furthermore, this processing is also necessary for the Agency to comply with its legal obligations under Articles 22(c), 24, 90(1) and 90(2) of the Staff Regulations.

Any processing of special categories of Personal Data by the Agency is carried out only to the extent that it is necessary for the purposes of complying with the Agency's specific rights and obligations in the field of employment law (as established in Union law or otherwise authorised by the European Data Protection Supervisor); specifically concerning Personal Data relating to (suspected or actual) criminal offences, the Agency processes these Personal Data only to the extent established in Union law or otherwise authorised by the European Data Protection Supervisor.

**(g) Informal and Formal Anti-Harassment Procedures**

Processing for this purpose is necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest; furthermore, this processing is also necessary for the Agency to comply with its legal obligations under Articles 1(d), 12(a), 24, 86 and 90 of the Staff Regulations, as well as under EU Commission Decision C(2006) 1624/3 of 26 April 2006, applicable to the Agency by analogy in accordance with Article 110(2) of the Staff Regulations.

Any processing of special categories of Personal Data by the Agency is carried out only to the extent that it is necessary for the purposes of complying with the Agency's specific rights and obligations in the field of employment law (as established in Union law or otherwise authorised by the European Data Protection Supervisor); specifically concerning Personal Data relating to (suspected or actual) criminal offences, the Agency processes these Personal Data only to the extent established in Union law or otherwise authorised by the European Data Protection Supervisor.

**(h) Administrative Inquiries and Disciplinary Proceedings**

Processing for this purpose is necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest; furthermore, this processing is also necessary for the Agency to comply with its legal obligations under:

- Articles 86 and Annex IX of the Staff Regulations;
- Articles 47, 49, 50, 50a and 119 of the CEOS; and
- Decision AB no. 2/2013 (10 January 2013), of the Administrative Board of the Agency.

Any processing of special categories of Personal Data by the Agency is carried out only to the extent that it is necessary for the purposes of complying with the Agency's specific rights and obligations in the field of employment law (as established in Union

law or otherwise authorised by the European Data Protection Supervisor); specifically concerning Personal Data relating to (suspected or actual) criminal offences, the Agency processes these Personal Data only to the extent established in Union law or otherwise authorised by the European Data Protection Supervisor.

**(i) Whistleblowing**

Processing for this purpose is necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest; furthermore, this processing is also necessary for the Agency (and Staff Members) to comply with the rules laid down in the Staff Regulations and CEOS.

Any processing of special categories of Personal Data by the Agency will be carried out only to the extent that it is necessary for the purposes of complying with the Agency's specific rights and obligations in the field of civil service law (as established in Union law or otherwise authorised by the European Data Protection Supervisor); specifically concerning Personal Data relating to (suspected or actual) criminal offences, the Agency processes these Personal Data only to the extent established in Union law or otherwise authorised by the European Data Protection Supervisor.

**(j) Internal Newsletter**

Processing for this purpose is necessary in order to allow the Agency to provide updated and reliable information on its news and developments to Staff Members and other individuals engaged by the Agency. This is deemed necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest.

**(k) Publication of Photographs**

Processing for this purpose is based on your consent. Any consent given may also be withdrawn at a later stage (see below – [What are my rights? How can I exercise them?](#))

**(l) Registration and Publication of CVs, Declarations and Commitments**

Processing for this purpose is necessary for the Agency to comply with its legal obligations, including under Articles 1, 2 and 16(1) of Regulation (EC) no. 713/2009 and the Decision of the European Parliament of 3 April 2014 on discharge in respect of the implementation of the budget of the Agency for the financial year 2012 (C7-0328/2013 – 2013/2240(DEC), as well as Decision of the Administrative Board of the Agency AB No. 2/2015 of 31 January 2015 laying down the policy for the prevention and management of conflict of interest); furthermore, this processing is also necessary for the management and functioning of the Agency and, as such, is necessary to carry out a task in the public interest.

**(m) Selection Committee Disclosure**

Processing for this purpose is necessary for the management and functioning of the Agency and comply with the EU Ombudsman's Good Practice Guidelines regarding disclosure of the names of Selection Committee members; as such, this processing is necessary to carry out a task in the public interest.

(n) **Information Exchange**

Processing for this purpose is necessary for the Agency to comply with its legal obligations, including under Article 15, second subparagraph, of Protocol no. 7 of the TFEU; otherwise (where there is no legal obligation to process for this purpose), any such processing will be based on your consent.

(o) **Compliance**

Processing for this purpose is necessary for the Agency to comply with its legal obligations.

The inclusion of all Personal Data stored by the Agency in its IT systems in periodic backups, as well as all processing carried out to ensure the appropriate handling of security incidents related to those systems, is deemed necessary in order to ensure the proper management and functioning of the Agency and, as such, necessary to carry out a task in the public interest.

## Who can see your Personal Data, and who will they be shared with?

Your Personal Data may be shared with the following list of persons / entities ("**Recipients**"):

- Companies, consultants or professional associations engaged by the Agency, as well as other Union institutions and/or bodies, in order to provide services related to the management of Staff Members and other individuals engaged by the Agency (e.g., training providers, travel agents, hotels, payroll processors, insurance providers, transport services, law firms and legal consultants) and technical maintenance / assistance, as well as operational security of systems used to store, transmit or otherwise process Personal Data in connection with the management and functioning of the Agency. These entities typically act as data processors on behalf of the Agency, and have access to Personal Data only to the extent strictly required for them to provide those services;
- Persons authorised by the Agency to process Personal Data needed to carry out activities strictly related to the purposes described above, who have undertaken an obligation of confidentiality or are subject to an appropriate legal obligation of confidentiality (e.g., staff members of the Agency). Other Staff Members or persons engaged by the Agency may also have access to your Personal Data to the extent that it is included in the Agency's internal organisational chart, internal directories and other internal documents used for the management of absence of Staff Members, temporary agency workers, trainees and SNEs;
- Candidates and applicants to positions within the Agency, where you are a member of the Selection Committee;
- External confidential counsellors, consultants and experts, regarding **Informal and Formal Anti-Harassment Procedures**;

- Public entities, bodies or authorities, including other Union institutions or bodies, to which your Personal Data may be disclosed, in accordance with Union or Member State law, or on the basis of binding orders from those entities, bodies or authorities, or otherwise to facilitate transfers of Staff Members to those institutions or bodies, allow the Agency to assess employment / training requirements (such as third language proficiency), to perform its obligations as employer or to assist you in handling required administrative procedures (e.g., the Slovenian Administration Office and Ministry of Foreign Affairs).

Some documents containing Personal Data, such as Declarations of Interests, CVs and Compliance Commitments for the Agency's senior management and for members and alternates of Boards, may be published on the Agency's website, thereby becoming accessible to the general public.

Generally, the Agency will not transfer your Personal Data outside of the EU. However, under specific and limited circumstances, your Personal Data may be transferred to non-EU entities.

### **(Read more)**

In order to allow you to go on missions, events or workshops on behalf of the Agency which take place outside of the EU, your Personal Data may be transferred to event hosts, accommodation and travel providers located outside of the EU (whenever strictly necessary).

- The legal grounds relied on for this depends on the country where the mission, event or workshop will take place (e.g., due to that country having been subjected to an adequacy decision from the European Commission) and the external providers to which your Personal Data is transferred (e.g., due to their self-certification under the EU-US Privacy Shield, or due to contracts entered into with those providers containing standard data protection clauses as approved by the European Commission).
- Where none of the above applies, given the limited and non-repetitive nature of these transfers, and the fact that participation in these missions, events or workshops is carried out for reasons of public interest, the Agency may rely on legally applicable derogations, subject to informing the European Data Protection Supervisory where this occurs.

For more information on transfers of Personal Data carried out by the Agency for these purposes, or on the specific recipients which may have access to your Personal Data, please contact the Agency's DPO, at: [dpo@acer.europa.eu](mailto:dpo@acer.europa.eu).

## How long do we keep your data?

The retention periods applicable to Personal Data handled by the Agency, for the purposes described in this Data Protection Notice, are as follows:

### **(a) Human Resource Management**

Personal Data processed for **Human Resource Management** are, generally, retained until the end of the working relationship with the Agency, and are stored in the personal files for each Staff Member, or other individuals engaged by the Agency (where applicable), for a further period of 8 years following extinction of all rights of the individual concerned and of any dependents and archived for at least 10 years following the termination of employment or the last pension payment (to address any subsisting rights and obligations, such as pension rights).

However, there are more specific retention periods which apply in certain cases.

**(Read more)**

- Personal Data relating to Staff Members which make a request to receive legal advice on Slovenian law from the Agency contractor engaged by the Agency are kept for 1 year, in order to ensure that Staff Members do not exceed the number of requests allowed yearly (2);
- Personal Data relating to books borrowed from the Agency's library are retained until the books in question are returned;
- Personal Data relating to parking spaces or public transport cards (e.g., Urbana cards) allocated to individuals are kept for the duration of their engagement with the Agency, or for the duration during which the parking space or public transport card is allocated (if lesser);
- Personal Data relating to car plate numbers for vehicles are retained for as long as the vehicle in question is registered to a Staff Member or other individual engaged by the Agency;
- Financial documentation containing Personal Data, such as receipts and bills collected in connection with requests for reimbursement of expenses, petty cash requests, VAT refund requests, bank statements related to the issuance and use of corporate credit cards and lists of attendance to external training courses (as supporting documentation for invoices paid to the training provider) are retained for 7 years;
- Personal Data processed in connection with support requests / help tickets are retained for at least 2 years, unless further retention is deemed necessary strictly for archival / analysis purposes (to gain general knowledge on the types of incidents more frequently occurring at the Agency and how best to respond to them), subject to appropriate safeguards (such as pseudonymisation or anonymisation of the requests / tickets, where feasible);
- Personal Data relating to training requests and courses are kept for the duration of the working relationship with the Agency and for 10 years thereafter. Where these Personal Data relate to ongoing rights and obligations (e.g., certificates of participation in a training course), these may be retained for longer. Additionally, any feedback provided on training is kept for the duration of the Agency's contract with external training providers;

- Personal Data related to requests from Staff Members for the Agency to enter into agreements with education institutions related to tuition fees, or for contributions to education expenses, are retained for 5 years after the end of the working relationship with the Agency.
- Personal Data related to missions carried out on behalf of the Agency are kept by the Agency at least for the duration of the mission, and for an additional period of time beyond that mission's conclusion as deemed necessary to comply with the Agency's obligations regarding mission management, as well as to defend the Agency's interests in the event of Staff Member complaints related to a given mission.
- Personal Data related particularly to the management of sick, special and annual leave requests, or of Flexitime or teleworking (such as records of working hours, time credits / debits and start / end dates for remote work) are kept for a period of 2 years.
- Personal Data related to temporary agency workers are kept for up to 5 years after termination of their engagement with the Agency.
- Personal Data related to SNEs are kept for up to 10 years after termination of their engagement with the Agency.

**(b) IT Management**

Personal Data processed for **IT Management** are, generally, kept for 7 days, unless further retention is required for the purpose of investigating and preventing anomalies or misuse.

However, there are more specific retention periods which apply in certain cases.

**(Read more)**

- Personal Data on individuals under remote working arrangements are kept for up to 12 months and logs are retained for at least 3 years, in order to enable detailed investigations in case of potential external attack;
- Activity logs relating to the use of the Agency's intranet are kept for up to 5 years, for auditing purposes;
- Personal Data relating to logs generated by use of the Agency's operating systems are kept for 14 days;
- Information relating to attempts to log on to the Agency's IT systems, devices and portals are kept for 6 months after the individual concerned (i.e., the individual whose authentication details were used) leaves the Agency, or is no longer assigned a role requiring authentication and authorisation via the Agency's Active Directory system, or the Agency's e-mail / webmail services.
- Personal Data relating to logs generated by use of Skype for Business are kept for 60 days for statistical reasons (e.g., to compare the use of this service

against services offered by other providers, in order to assess the value of this service for the Agency).

- Personal Data relating specifically to operational security of the Agency's REMIT Portal – i.e., on Staff Members or other individuals engaged by the Agency which perform actions through administrative channels related to the REMIT Portal – are kept for 2 years.

(c) **Payroll / Expense Reimbursement**

Personal Data processed for **Payroll / Expense Reimbursement** are kept for the standard retention period for financial documents – 7 years.

(d) **Evaluation of Probationary Period Reports, Yearly Performance Appraisal and Reclassification Exercises**

Personal Data processed for **Evaluation of Probationary Period Reports, Yearly Performance Appraisal and Reclassification Exercises** are kept for the following periods:

- Personal Data related to evaluation of probationary periods are kept for 5 years after termination of the probationary period in question.
- Personal Data related to performance appraisal for temporary and contract staff are kept for 5 years in the Agency's appraisal tool, following which they are transferred to the Staff Member's personal file, where they are further retained for 8 years following extinction of all rights of the Staff Member concerned and of any dependents and archived for at least 10 years following the termination of employment or the last pension payment.
- Personal Data related to reclassification exercises are retained for as long as the Staff Member in question is recorded as an active user (e.g., for the duration of the employment contract or retirement), and for a period of 1 year thereafter – any tables or reports produced to reach a decision on reclassification (which may contain Personal Data related to Staff Members) are kept for a total of 5 years.

(e) **Management of Contracts and Internal Documents**

Personal Data processed for **Management of Contracts and Internal Documents** are generally kept for 5 years. However, retention periods may vary according to the rules on retention for the documents in question.

(f) **Management of Requests and Complaints**

Personal Data processed for **Management of Requests and Complaints** are stored in the personal files of Staff Members (or other individuals engaged by the Agency) concerned, where they are retained for 8 years following extinction of all rights of the Staff Member concerned and of any dependents and archived for at least 10 years following the termination of employment or the last pension payment.

(g) **Informal and Formal Anti-Harassment Procedures**

Confidential counsellors do not retain Personal Data received in this context beyond the time limit necessary to perform their tasks (generally, 2 months, except in the event of an extension due to absence or leave); in any case, confidential counsellors do not keep any such Personal Data beyond 3 months after closure of a case.

**(h) Administrative Inquiries and Disciplinary Proceedings**

Personal Data processed for **Administrative Inquiries and Disciplinary Proceedings** are retained as follows:

- Where a case is dismissed after a preliminary assessment of information collected, these Personal Data are stored for a period of 2 years.
- Where, at the end of the inquiry, the Director of the Agency decides that no case can be made against the individual concerned, or where only a warning is to be issued, these Personal Data are stored for a period of 5 years.
- Where, at the end of the inquiry, a formal decision that disciplinary proceedings will be launched is adopted, those Personal Data are transferred to a disciplinary file, where they are retained for a maximum period of 20 years after adoption of the final decision within those proceedings ("**Decision**").

However, if a Staff Member submits a request, under Article 27 of Annex IX to the Staff Regulations, for the deletion of a written warning or reprimand (3 years after the Decision) or in the case of another penalty (6 years after the Decision, except where the penalty given was the person's removal from his/her post) and the Director of the Agency grants the request, the disciplinary file which led to the penalty will also be deleted.

The Director of the Agency may decide to grant the request for the deletion of disciplinary file 10 years after the adoption of the final decision, in light of the severity of the misconduct, the seriousness of the disciplinary measure imposed and possible repetition of the misconduct.

**(i) Whistleblowing**

Generally, Personal Data collected in connection with reports made under **Whistleblowing** are retained by the Agency for a period of 2 months from completion of the preliminary assessment of each report. However, there are circumstances under which this retention period may be shortened.

**(Read more)**

- Any Personal Data collected in connection with reports made under **Whistleblowing** which are not relevant to the allegations within the said reports are not further processed by the Agency.
- Reports made which, following an initial assessment, are deemed not to be referred to the European Anti-Fraud Office ("**OLAF**") or otherwise not within the scope of the Agency's whistleblowing procedure are deleted as soon as possible, or otherwise referred to the appropriate channels (e.g., where they

concern alleged harassment, reports may be redirected to functions responsible for **Informal and Formal Anti-Harassment Procedures**).

- Where a report is to be transferred to OLAF, the Agency deletes Personal Data collected in connection with the said report as soon as OLAF decides to start its own investigation; if OLAF decides not to start an investigation, these Personal Data are deleted without delay.

(j) **Internal Newsletter**

Personal Data processed for the **Internal Newsletter** (i.e., Personal Data contained within the newsletters and used to send the newsletters out) are retained for 20 years, as an historical archive.

(k) **Publication of Photographs**

Personal Data processed for **Publication of Photographs** are kept for the entire duration of your engagement with the Agency, unless you withdraw your consent for this purpose. At the end of your engagement with the Agency, any photographs of you are erased.

Please bear in mind that the withdrawal of your consent will not affect the lawfulness of processing of your Personal Data carried out beforehand.

(l) **Registration and Publication of CVs, Declarations and Commitments**

Personal Data processed for **Registration and Publication of CVs, Declarations and Commitments** are retained for 5 years after the discharge for the budgetary year to which the declaration relates.

(m) **Selection Committee Disclosure**

Personal Data processed for **Selection Committee Disclosure** remain available on the Agency's website for as long as you are a part of the Agency's Selection Committee.

Additionally, Personal Data included in documentation related to the election / appointment of Selection Committee members are retained for a period of 2 years.

(n) **Information Exchange**

Personal Data processed for **Information Exchange** are held by the Agency for a period of 5 years.

(o) **Compliance**

Personal Data processed for **Compliance** are kept by the Agency for the period required by the specific legal obligation or by the applicable Union or Member State law.

Please note that, in any case, the Agency may continue to store Personal Data for a longer period, as may be necessary for internal auditing and security purposes

(including within periodic backups carried out) and, in general, to protect the Agency's interests related to potential liability related to this processing.

For more information on these or other retention periods which may apply, please contact the Agency's DPO, at: [dpo@acer.europa.eu](mailto:dpo@acer.europa.eu).

## What are my rights? How can I exercise them?

As a data subject, you are entitled, in general, to exercise the following rights before the Agency:

- Access your Personal Data being processed by the Agency (and/or obtain a copy of those Personal Data), as well as information on the processing of your Personal Data;
- Correct or update your Personal Data being processed by the Agency, where it may be inaccurate or incomplete;
- Request the erasure of your Personal Data being processed by the Agency, where you feel that the processing is unnecessary or otherwise unlawful;
- Request the blocking of your Personal Data, where you feel that the Personal Data processed is inaccurate, unnecessary or unlawfully processed, or where you have objected to the processing;
- Withdraw your consent to the processing of your Personal Data (for **Publication of Photographs**);
- Exercise your right to portability: the right to obtain a copy of your Personal Data provided to the Agency, in a structured, commonly-used and machine-readable format, as well as the transmission of that Personal Data to another data controller.

You may also have a right to **object to the processing of your Personal Data**, based on relevant grounds related to your particular situation, which you believe must prevent the Agency from processing your Personal Data for a given purpose. This right may apply whenever the Agency relies on the need to perform a task in the public interest as the legal basis for a given processing purpose, e.g., **Human Resource Management, Internal Newsletter, Selection Committee Disclosure** and others (see above – [Why can the Agency use these Personal Data?](#)).

To exercise any of the abovementioned rights, you may send a written request to the Agency at: [hr-info@acer.europa.eu](mailto:hr-info@acer.europa.eu). You may also contact the following persons / departments within the Agency, for specific inquiries related to processing activities described within this Data Protection Notice:

### **General Staff Management Inquiries:**

[HR-info@acer.europa.eu](mailto:hr-info@acer.europa.eu)

### **IT-related Inquiries:**

[ithelpdesk@acer.europa.eu](mailto:ithelpdesk@acer.europa.eu)

**Facility Management related Inquiries:**

[procurement@acer.europa.eu](mailto:procurement@acer.europa.eu)

**Agency Data Protection Officer:**

[dpo@acer.europa.eu](mailto:dpo@acer.europa.eu)

Please note that the above rights may not apply, or may not apply in full, as there may be applicable legal exemptions or restrictions to those rights. This will be assessed by the Agency on a case-by-case basis; if such an exemption or restriction is found to be applicable, you will be informed of the Agency's main reasoning for this.

In any case, please note that, as a data subject, you are entitled to file a complaint with the European Data Protection Supervisor, if you believe that the processing of your Personal Data carried out by the Agency is unlawful. You will suffer no prejudice on account of any such complaints lodged.