European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing:	SYSPER
Created on	28/08/2020
Last update	10/09/2020
Reference number	054
Year	2020
1. Controller:	European Economic and Social Committee
2.a) Service responsible	Directorate E
2b) contact details	sysper2-cese@eesc.europa.eu
3. Joint controller	
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	Processed by: European Commission, DG DIGIT
6. Purpose(s) of the data processing	

Sysper is the integrated information system for managing human resources at the European Economic and Social Committee (EESC). It was developed by the Commission and deployed within the EESC by DG DIGIT. The system consists of different modules dedicated to the different aspects of human resources management, each of which is managed, consulted on and completed by the relevant specific managers. Managers have the right to consult, enter and validate information according to the position they occupy in the organisation chart.

The application is constantly evolving in order to adapt to the needs of users and to amendments to the rules governing the institution's relations with its staff, in particular the Staff Regulations, the Conditions of Employment of Other Servants of the European Communities, the general implementing provisions for these regulations and the internal management rules followed by the institution.
At the EESC, the following data are accessible through this system: EESC organisation chart according to staff assignments and posts, description of these posts, job quotas (i.e. maximum number of officials and other staff per entity), and personal data: career, administrative status, family rights and conditions, private data (surname, first name, birth details, address, family composition, languages spoken), management of individual rights, management of working time and payslips.

Additionally, Sysper as a portal allows for the visualisation of personal files through the NDP application (digitalisation of personal files) as well as payslips. The NDP application and the part related to payslips are subject to an additional notification).

Sysper is the application for managing the EESC's human resources through the following actions:

- Providing support for all procedures relating to the "classical" management of staff: recruitment, career development, definition of relations under the Staff Regulations and individual rights, administrative status (Article 35 of the Staff Regulations), assignment to posts, working arrangements and working time.
- Enabling management of staff rights and statutory obligations, in particular with a view to ensuring ad hoc financial processing and monitoring the professional and administrative career.
- Serving as an interface for the user to make requests for certificates or specific declarations (declaration of marriage, spouse's professional activity, children's school, etc.), these requests will subsequently be reflected in the user's rights and then in the pay.
- Sending the data to NAP (New Payroll System) for the calculation of salaries;
- Enabling extraction of statistics and reports related to personnel management;
- Enabling management of the EESC's organisation chart and allocations;
- Setting up and maintaining the directory of all EESC staff.

7. Description of the categories of persons whose data are processed	All natural persons who have or have had a statutory link or an employment contract with the institution, successful candidates in competitions or candidates for an employment contract, including officials, temporary agents, contract agents, special advisers, seconded national experts, trainees as well as former staff. Persons working for or having worked in the premises of the institution without a statutory link or employment contract with it (interim staff, staff from external service providers, etc.) are also concerned. Where this category of persons is concerned, basic management information is collected. Dependants of officials and other servants covered by the Staff Regulations or the CEOS are also included.
8. Description of data categories processed	This system consists of a series of modules, each of which covers precise and specific functions. The modules processing the personal data are: Organisation chart module dealing with the management of posts and the organisational structure of the Committee. With sub-modules: • JobHolder management: this module covers the assignment of staff and the description of their duties. It therefore provides support for "traditional" staff management procedures, including recruitment, probation period, internal mobility, assignments to posts, secondments, career breaks and the end of a career. Type of data collected: post number, surname, first name, job title, location, status, occupation, head of unit, management post, grades, job description). • job quotas management: anonymous inventory of posts allocated to each entity in the organisation chart. This module does not collect personal data as such, but it has links to other modules (personal data, career) which contain personal data. Career module containing career-related data. With sub-modules: • career summary: this module contains all the data related to an official or agent's career. Type of data collected for each staff member: administrative status, type of post of person, administrative position, working arrangement, classification (function group, grade, step), seniority (function group, grade, step), multiplying factor, postings, date of entry into service at first institution, date of entry at the EESC, summary of career history since entry into service or since implementation of Sysper at the EESC. • career history: sub-module for career managers; this module presents the timeline of career management by status and function

group as regards classification, assignments, management, contract and probation period, employment type and career events. Type of data collected for each staff member: statutory link, administrative status (starting and finishing dates, activity rate, rate of remuneration, event), grade and step since the beginning of the career in the institutions, postings, job number, job title, function, grant of the management allowance, dates of contracts and details of the probation period, all events affecting the career. The HR departments of each institution may only consult these data for the period when the person worked in that institution.

- management files: the sub-module used by recruitment, career and mobility managers to deal with any file related to recruitment, internal mobility, promotion, transfer or the end of a contract or career, career break or reinstatement, for each function group. Type of data collected for each staff member: depending on the type of file, the relevant details for each request are: start and end dates, details of names, details of birth, nationality, languages, contact information, recruitment details (vacancy notice, Sysper post number, place, budget, range of grades), details of classification (Staff Regulations, function group, grade, step with seniority granted), date of entry into first institution, date of entry into the EESC.

Time Management (TIM) module: this module makes it possible to manage the time aspects of a given jobholder's benefits. Type of data collected: presence/absences, leave, working arrangements, working time, teleworking, timesheets for standby duty and overtime (Article 56 of the Staff Regulations). The sub-modules are:

- absences/presence (including timesheets for standby duty and overtime)/teleworking
- work patterns: For this module, additional data are collected for working arrangements involving special conditions (parental leave – the name of the child and the situation of the parent: single or not, family leave – details of the relationship with the person for whom the leave is taken).

Personal data module: this module collects all the personal information of the person. The information in this module is either introduced by the managers during recruitment (gender, surname, first name, provisional address, phone number, e-mail address, date and place of birth) or entered and managed by the staff members (addresses, contact information). Sub-Modules:

- identity (name data, birth data, user names in the various applications, languages used, photo, contact details at the office, place of origin, place of recruitment)
- languages
- address: private address, contact person and contact details
- personal file: access portal to the NDP application

	Rights module: this module collects all information related to management of people's individual rights and financial rights. It includes information related to the family composition of staff members (relationship, surnames, names, nationality, addresses, date and place of birth) and are either managed exclusively by authorised rights managers or managed by the rights managers following the submission of an ad hoc declaration via the system by each member of staff concerned. Data collected: for each sub-module, the relevant information is collected. The details of this are too numerous to be listed in this privacy statement but are included in the Sysper manual. The sub-modules of the rights module are: • financial rights related to the person and their family members • family composition • declarations: schooling, marriage/partnership, professional activity of spouse, removal, change of private address, birth • certific ates (certificate generation module, managed by HR) None of the Sysper modules entails any processing of data which could reveal racial or ethnic origins, political opinions, religious or philosophical beliefs, membership of trade unions or sexual orientation. Neither medical records nor disciplinary records are included in Sysper at present.
9. Time limit for retaining the data	In general, personal data is stored until the end of a staff member's work with the institution. Certain data are retained beyond the period employment if they are related to subsisting rights and obligations. The data of officials who have taken up their duties at the EESC are retained throughout their career and for a period of 10 years from the date of termination of service or the last payment of a pension by the administrative documentation and information/staff communication service.
10. Recipients of the data	

the data concerning each person are accessible to various actors in the institution:
each member of staff, for themselves
each staff member only with regard to the organisational entity and assignment of tasks.

hierarchical superiors: head of unit, Deputy Director, Director, Secretary-General: (time management data, organisation chart, grade and job description)
authorised human resources services (access limited according to management work or stage of workflow)
by delegation, any other person designated by the above-mentioned persons.

the Sysper Business Manager to enable them to solve problems or transfer bugs that cannot be solved internally
HR staff responsible for the administration of Sysper in DG HR as well as developers and DG DIGIT's helpdesk who need this data to solve bugs, test new developments or to search for users and conduct usability tests.
The recipients outside the Commission are:

OLAF, the European Court of Auditors (for limited data)
Individual people (limited information via EU WhoIsWho)
The access rights granted to the above-mentioned persons are different in nature (reading/writing) and scope (data and accessible populations) depending on the profile of the recipient. This profile (the job, i.e. function and responsibilities) reflects the need to access certain data or a certain population.

The data of an official or other agent are communicated to other institutions and to the Member States only in so far as a legal basis so provides or where it has been established as necessary. The Staff Regulations and the implementing texts cover all the purposes of managing staff and the institutions. For example, information is transferred to another institution in case of transfer of a person in order to allow the new institution to manage the data. Some data may be transferred for auditing purposes to duly authorised institutions (such as the Court of Auditors or OLAF) or forwarded to the European Court of Justice or the European Data Protection Supervisor.

To enable internal communication, certain data (name, administrative address, telephone number and job description) may be made accessible to all staff of the institution. Some of these data (name, assignment, office number, office telephone) are published in the institution's "Who's who".

As part of the Committee's crisis management and business continuity plan (BCP), staff members are required to enter their private and mobile phone numbers.

11. Transfers of personal data to a third country or an international organisation	The data will not be transferred to a third country or international organisation.
12. General description of security measures, where possible	These data are safeguarded in the Commission's Data Centre in Luxembourg, and are therefore covered by the numerous defensive measures implemented by DG DIGIT to protect the integrity and confidentiality of the electronic assets of the institution. Access to personal data is protected by a login and access rights which are strictly limited according to the "need to know" principle depending on the tasks assigned to access holders. Access rights are linked to the posts (i.e. functions) of individuals so they are constantly updated as staff are assigned or reassigned to posts. User names (login) and passwords are managed by the ad hoc human resources departments of the institution. Every year a data access monitoring exercise is run for HR managers. Every holder of an access right may delegate their rights to a trusted representative in the interests of the smooth operation of the departments. Heads of Units may, for example, delegate the right to approve leave to their secretaries. This delegation is transparent and reversible. The responsibility lies with the person who delegates the access right. The delegation is linked to a person's job, therefore the person loses all access rights upon leaving the job. Of course, a person can only see, print save, etc. data that they have received a delegation for. Audit trail techniques monitor any access to and manipulation of data in Sysper and can be used in case of investigation. The overall responsibility for implementing the rules for granting access rights and ensuring compliance with data protection rules lies with the Director of Human Resources and Finance.
13. Privacy statement	SYSPER

Part 2
Compliance check and risk screening

1.a) Legal basis and reason for processing	☑ (a) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body ☑ (b necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)

	☐ (c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ☑ (d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes ☐ (e) necessary in order to protect the vital interests of the data subject or of another natural person [Tick (at least) one of the boxes]
1b) Legal basis	The Staff Regulations of Officials of the EC and Conditions of employment of other servants of the EC The Financial Regulation of the institutions.
2. Are the purposes specified, explicit and legitimate?	Yes
3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?	The data may be used for statistical purposes, in order to trace any development of one or more aspects related to recruitment, rights, nationalities, etc. However, these data will be used anonymously.
4. Do you really need all the data items you plan to collect?	Yes, all the data are necessary for processing
5. How do you ensure that the information you process is accurate?	...
6. How do you rectify inaccurate information?	...
7. Are they limited according to the maxim "as long as necessary, as short as possible"?	Yes
8. If you need to store certain information for longer, can you split the storage periods?	...
9 How do you inform data subjects?	By means of a privacy statement.
10. Access and other rights of persons whose data are processed	Staff members can access the data through Sysper. Data subjects may contact the controller to exercise their other rights. (sysper2-cese@eesc.europa.eu)

11. Does this process involve any of the following?	☐ (a) data relating to health, (suspected) criminal offences or other special categories of personal data ☐ (b) evaluation, automated decision-making or profiling ☐ (c) monitoring data subjects ☐ (d) new technologies that may be considered intrusive
Part 3 Linked documentation	
1. Links to threshold assessment and DPIA (where applicable)	 No hyperlink inserted
2. Where are your information security measures documented?	 No hyperlink inserted
3. Links to other documentation	 No hyperlink inserted
4. Other relevant documents	