Categories of personal data processed

The collected data enable the administration to manage members' data related to the
EU organic award

The purpose of collecting GSM numbers and private email addresses of relevant staff

No, your personal data are not transferred to a non-EU Member

Preparing and authorizing salaries for payment in accordance with the Financial

Each Joint Controller is responsible for specific activities as follows:

1.
2.
3.
4.
5.

Personal data shall be processed by the Joint Controllers for the following purposes:

− Best organic farmer (male & female): Copa and Cogeca and IFOAM Organics
− Best organic region, city & bio-district: the CoR;

− Staff members

− gender;
− date of birth;

−	Access to anonymised data is disclosed to staff and members of the CoR via the
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	European Parliament may receive the personal data as member of the jury;
−	CoR legal services and internal audit unit, in case needed.
−	Access to anonymised data is disclosed to staff and members of the CoR via the
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
−	KIKLOS Visitors are all EESC-CoR users identified with a user name and password.
−	ECAS passwords (the European Commission’s authentication service), for Centurio
−	In case of absence of passwords in the abovementioned systems, passwords are
−	Preparation and implementation of the personal data protection policy and
−	Enquiries from the European Commission (EC) and from police/security authorities in EU
to process the requests for issuing a laissez-passer and to respond to possible
−
−	By default the user traffic is anonymised.
Declaration of assurance

The present data protection notice focusses on the steps of the QeS certificate

Directorate E

Staff Mobility

The legislative footprint shall be included into the file related to

Staff Missions

N/A

N/A

EU Sign

N/A

N/A

Register of Charters of

Surname, first name, address, CoR staff number, professional telephone number,

European Committee of the Regions

British

E.4 Financial management

RE4-4

REI-3

Authorising Officers

Directorate E

511 74 -

Regions

and

European

International

Travels

the CoR's 2024 Report on the State of Regions and Cities.  

reflection on the proposals of the European Commission in this area, as well as possibly

or report in the CoR archives.

rapporteur has received input in drawing up the opinion or report.

collecting a non-exhaustive list of organisations and individuals from whom the

voluntary basis, and under their exclusive responsibility, draw up a 'legislative footprint',

IIA.

2021 between the European Parliament, the Council of the European Union and the

members on the state of play of the implementation of article 11 of the Governance of

Personal data will be collected from the persons participating to the online EU survey

whenever the creation of a QeS profile is requested, the delegated controller

QeS profiles are created on a service needs basis only, for CoR staff members and

A) Assessment of eligibility for the creation of a QeS profile

Internal to the organisation: CoR President; CoR First Vice President; statutory staff

CoR and EESC Staff members appointed as financial actors, as foreseen in CoR decision n° 14/2018 on the Internal financial rules

electronic signature service at DG DIGIT [identification data and contact data only].

Regarding digital data

Internal to the organisation: CoR Staff members appointed AOD or AOS.

Discharge authority (European Parliament)

Out of the CoR:

No

Maximum one year after the delivery of the final report, except

To be noted that, pursuant to the provisions of Council

provisions of Regulation 1049/2001 on the public's right of

EU legislative process, all documents included in the file of an

documents, the legislative footprint accompanying CoR opinions or reports are

As the file related to CoR opinions and reports includes public documents in the sense

coordination of the process on behalf of the controller).

As a result, all personal data included in such files are processed on the basis of an

Furthermore, the CoR Officers, both elected and appointed, engage in coordination

herself or himself and the CoR in the event of any conflict of interest.

The CoR Officers will be subject to the Code of Conduct for Members and Officers of the CoR, as

http://www.conselorregions.eu, CoR registers of declarations of conflict of interest

including the registry of declaration of assurance of the CoR Officers.
Microsoft is Innocraft, the EU intelligence in the form of daily newsletters, articles, alerts and legislative data across streaming operator (Dir D, A and Streamovations) and becomes available on the CoR's web-streaming is covered by a specific DPN for the event being webstreamed. For streaming of public activities of CoR following a request from any organiser within CoR (with participants’ consent only).

As distribution of a weekly info flash and a monthly newsletter;

- the operation and management of the network;
- view images, interviews and videos from events or for internal communication;
- CoR Members and Alternates;
- representatives of regional and local bodies who either hold a regional or local mandate or participate in the CoR’s network group (link provided) and benefit from the range of services available to them, depending on the purposes of the data processing, the following categories of persons, whose data are processed, could be listed:
- role in the organisation,
- NUTS classification,
- country represented,
- EU Member States.

Access to the personal data collected for the processing operation in question is available to:

- CoR and EESC staff members (authenticated users).
- representatives of regional and local bodies who either hold a regional or local mandate or participate in the CoR’s network group (link provided) and benefit from the range of services available to them, depending on the purposes of the data processing, the following categories of persons, whose data are processed, could be listed:
- role in the organisation,
- NUTS classification,
- country represented,
- EU Member States.

Access to the personal data collected for the processing operation in question is available to:

- CoR and EESC staff members (authenticated users).
- representatives of regional and local bodies who either hold a regional or local mandate or participate in the CoR’s network group (link provided) and benefit from the range of services available to them, depending on the purposes of the data processing, the following categories of persons, whose data are processed, could be listed:
- role in the organisation,
- NUTS classification,
- country represented,
- EU Member States.

The controller and the processor only keep personal data for the duration of the purpose for which they are processed or is agreed with the publication [Specific Privacy Statement SysPer, March 2017 version].

No transfer of personal data is foreseen. The controller and the processor do not transfer personal data to any third country or international organisation.

Innocraft and its subcontractors, Microsoft, have established standard contractual provisions and technical and organisational measures for the protection of personal data.

The controller and the processor are bound to use the following personal data protection measures:

- the processor takes necessary technical and organisational security measures in order to ensure that the data are not lost, destroyed, damaged or accessed by unauthorised persons.
- the controller and the processor have implemented the necessary measures to ensure that the data are not lost, destroyed, damaged or accessed by unauthorised persons.
- the controller and the processor have implemented the necessary measures to ensure that the data are not lost, destroyed, damaged or accessed by unauthorised persons.
- the controller and the processor have implemented the necessary measures to ensure that the data are not lost, destroyed, damaged or accessed by unauthorised persons.
- The controller and the processor take appropriate technical and organisational measures to ensure security levels, taking into consideration the state of the art, the costs for implementing these measures, the risks of the processing of the personal data and the degree of protection necessary to protect the rights and freedom of individuals. The measures include, as a minimum, the encryption of personal data stored or transmitted in an electronic format and the use of strong passwords. The controller and the processor shall take reasonable steps to ensure that third parties to whom personal data are transferred or who are given access to it, are bound by similar obligations. If the controller or the processor transfers personal data to third parties in a country or international organisation where there is no adequate level of protection, the controller or the processor shall provide an adequate level of protection to those data (Art. 49 GDPR).
The data are processed for publication in the Whoiswho.

Not applicable

Measuring the capacity used and estimating the required capacity in the future, surveillance.

The Committees do not use covert detection and investigate theft of equipment or assets owned by the Committees, visitors access, including unauthorised access to secure premises and protected rooms, IT service providers and their time sheets.

Committees and the registration of them when arriving. The new visitors management visitors​.eVisitors is a software, designed to automatize the invitation of visitors to the work of employees or to monitor attendance. The Committees do not use covert detection and investigate theft of equipment or assets owned by the Committees, visitors access, including unauthorised access to secure premises and protected rooms, IT service providers and their time sheets.

A fifth group of data is composed of telephone directories containing all staff.

The first set of data is composed of records known as "call data records". These technical data (IP address, MAC address, etc.) permit direct identification of the data subject. The financial operators are included in the financial files.

Anonymous data is kept indefinitely. The financial operators are included in the financial files.

• Telephone numbers(s),
• Surname
• Internal address
• gender
• last name, first name

- committee
- first name,
- body and
- message header (traffic information),

in order to bring the workstation into line with the applicable technical standards of the EU institution.

The database can only be accessed by means of an individual

The data, indicated as basic data for each group, are sent to the OP (to be published in the Whoiswho).

The data are accessible in a form permitting the data subject to be identified only by the sequence in question concerns a member of an Institution of the Union.

Concerning members, your personal data is archived in a

Concerning members, your personal data will appear as long

The data are only collected if the person gives their consent. If special arrangements appear thereto, relates to:

Security incident handling includes machine-based, automated processing of personal data. The personal data that is collected is in connection with security incident handling, the identification of the data subject is possible by means of the technical data (IP address, MAC address, etc.)

The DIIT and its hierarchy for anonymous reports relating to the infrastructure.

The persons responsible for recovery orders are informed of the amounts to be disclosed must be reasoned, submitted in writing to the Security Service and must images may be transmitted to the Belgian Federal or Local Police. Such requests for Local police may be given access if needed to investigate or prosecute criminal

In-house security staff and outsourced security-guards. Recorded video is accessible to

- e-mail services of other institutions

Address book (data fields as indicated in this notification):

Internal e-mail system users: Committee Members & staff.

For more details concerning the processing of personal data by the OP, the respective privacy statement of the OP can be consulted.

For more details concerning the processing of personal data by the OP, the respective privacy statement of the OP can be consulted.

The data are processed for publication in the Whoiswho.

The data are processed for publication in the Whoiswho.
The EESC and CoR have four Intranets: EESC Intranet, MYCOR, DT Intranet and DL Intranet. Infrastructure Unit — Directorate for Interinstitutional exchanges - translation of EESC and CoR. Processing is necessary to follow up requests and ensure good quality service in line with the mission and objectives of the environmental management system. The data collected are necessary for the organisation, management and follow-up of problem related to environmental management or to obtain information and advice. It gives the option of indicating the name of the person professionally responsible for the inventory of assets (except consumable goods and buildings) in line with Article 157 of the Financial Regulation (FR) and Article 247 of the Rules of Application (RAP), ABAC Committee and the Committee of the Regions, conditions relating to the preservation of documents and destruction. The data included will be kept and made anonymous for the purposes for which the materials were slightly altered, so that they can be used for the purposes for which the materials were altered. The processing operation will done manually and/or by external agents. For the purposes detailed above, access to your personal data is given or may be limited to the following persons or categories of persons: the data controller, the officer and Head of unit. Access is requested from the CIS by the head of unit and is forwarded to the Local Data Protection Officer. The horizontal or language units and services seeking or requested by the Translation Directorate (notably the heads of unit concerned and the coordinator in charge of translation) will also get access to your personal data to fulfill their mission and objectives. Information can relate to the following data: personal details: First name, family name, Committee, office number, Unit, end of the date of the recruitment, reason for recruitment, in case of trainee or contract agent: the name of the person professionally responsible for the inventory of assets, the specific workplace (unit). Financial Regulation (FR) and Article 247 of the Rules of Application (RAP), ABAC Committee and the Committee of the Regions, conditions relating to the preservation of documents and destruction. The data included will be kept and made anonymous for the purposes for which the materials were slightly altered, so that they can be used for the purposes for which the materials were slightly altered. The processing operation will done manually and/or by external agents. For the purposes detailed above, access to your personal data is given or may be limited to the following persons or categories of persons: the data controller, the officer and Head of unit. Access is requested from the CIS by the head of unit and is forwarded to the Local Data Protection Officer. The horizontal or language units and services seeking or requested by the Translation Directorate (notably the heads of unit concerned and the coordinator in charge of translation) will also get access to your personal data to fulfill their mission and objectives. Information can relate to the following data: personal details: First name, family name, Committee, office number, Unit, end of the date of the recruitment, reason for recruitment, in case of trainee or contract agent: the name of the person professionally responsible for the inventory of assets, the specific workplace (unit).
Microsoft 365

We collect the following personal information: surname, first name, email address.

Directorate D
Security Service, Directorate L, Joint
Directorate E
EESC and CoR

We will collect only the following personal data from the event participants necessary
for financial purposes for the organisation and management of the event, in case of registration via EU-Learn, the personal data
will be processed in accordance with the consent given, but can also be processed
in accordance with Article 6.1(c) of the GDPR.

We will retain the personal data for 5 years from the end of the financial year
in which the personal data were collected, except if the data is of a type
that may be retained in accordance with legal and regulatory requirements.

The Interinstitutional Relations
Directorate D – Communication and
Interinstitutional Relations
department.

openday@eesc.europa.eu

DTmanagement@eesc.europa.eu

mgmt-IIT-sc@eesc.europa.eu

Interinstitutional Relations

Directorate D – Communication and
Interinstitutional Relations

Ex Libris
Provider of
BDO LLP
BUDG/19/P
processor
applicable
for financial purposes
for the organisation and management of the event

The SECABC platform, developed, operated and administered by DIGIT, enables the
participants to follow the session at a later stage, and to generate cost and time efficiency
benefits. Such meetings may take place online, in a hybrid format or in-person. The
Platform allows for the following:

•	 Staff interviews (concerning staff with management responsibilities):
  - Entity of employment (directorate, unit, service, etc.)
  - Category
  - Entry into service (at the EESC)
  - Email messages
  - Telephone calls
  - Video calls
  - Names
  - Function
  - Department
  - Workgroup
  - Category
  - Department
  - Team
  - Name
  - Position

•	 ID or passport number,
•	 Date and place of birth;
•	 Telephone number,
•	 Address
•	 Company and

- Key contacts from the organisation

Special lanyards are available at the information desk in JDE reception hall so identify
the participants. In case of registration via EU-Learn, the personal data
will be processed in accordance with the consent given, but can also be processed
in accordance with Article 6.1(c) of the GDPR.

Rectangular Office

For key contacts, the personal data will be processed in accordance with consent
given, but can also be processed in accordance with Article 6.1(c) of the GDPR.

Microsoft 365

For key contacts, the personal data will be processed in accordance with consent
given, but can also be processed in accordance with Article 6.1(c) of the GDPR.

The location of the processing is fixed in these standard contracts
and in the compliance program of Microsoft 365. Service generated
data remains under the control of Microsoft and is used to
service provisioning of Microsoft 365, Microsoft copies
subscription
- Up to six months

- Identification data
- Contact data
- Data on the use of services
- Billing data
- Financial information
- Data for security management
- Data on security, risk of data loss, alteration or unauthorised access,
- Data for the prevention of computer misuse
- Data on the billing and financial administration
- Data on the management of the technical and organisational measures
- Data on the identification of the users and their access rights
- Data for the maintenance and repair of hardware and software
- Data on the support services provided
- Data on the monitoring and evaluation of the functioning of the IT systems
- Data on the control of the personal data protection policies

There are appropriate measures in place to restore access
to the personal data and to ensure its portability.

The security and confidentiality requirements are
presented by the processing and the nature of the personal
data. The standard security requirements are presented in the standard
contracts of Microsoft 365. There are appropriate measures in place to restore access
to the personal data and to ensure its portability.

MSA22

The CloudCenter application is subject to the Cloudficient, Cognisys, and Securide
security, risk of data loss, alteration or unauthorised access,
- Data on the billing and financial administration
- Data on the management of the technical and organisational measures
- Data on the identification of the users and their access rights
- Data for the maintenance and repair of hardware and software
- Data on the support services provided
- Data on the monitoring and evaluation of the functioning of the IT systems
- Data on the control of the personal data protection policies

There are appropriate measures in place to restore access
to the personal data and to ensure its portability.

The CloudCenter application is subject to the Cloudficient, Cognisys, and Securide
security, risk of data loss, alteration or unauthorised access,
- Data on the billing and financial administration
- Data on the management of the technical and organisational measures
- Data on the identification of the users and their access rights
- Data for the maintenance and repair of hardware and software
- Data on the support services provided
- Data on the monitoring and evaluation of the functioning of the IT systems
- Data on the control of the personal data protection policies

There are appropriate measures in place to restore access
to the personal data and to ensure its portability.

The CloudCenter application is subject to the Cloudficient, Cognisys, and Securide
security, risk of data loss, alteration or unauthorised access,
- Data on the billing and financial administration
- Data on the management of the technical and organisational measures
- Data on the identification of the users and their access rights
- Data for the maintenance and repair of hardware and software
- Data on the support services provided
- Data on the monitoring and evaluation of the functioning of the IT systems
- Data on the control of the personal data protection policies

There are appropriate measures in place to restore access
to the personal data and to ensure its portability.

The CloudCenter application is subject to the Cloudficient, Cognisys, and Securide
security, risk of data loss, alteration or unauthorised access,
- Data on the billing and financial administration
- Data on the management of the technical and organisational measures
- Data on the identification of the users and their access rights
- Data for the maintenance and repair of hardware and software
- Data on the support services provided
- Data on the monitoring and evaluation of the functioning of the IT systems
- Data on the control of the personal data protection policies

There are appropriate measures in place to restore access
to the personal data and to ensure its portability.

The CloudCenter application is subject to the Cloudficient, Cognisys, and Securide
security, risk of data loss, alteration or unauthorised access,
- Data on the billing and financial administration
- Data on the management of the technical and organisational measures
- Data on the identification of the users and their access rights
- Data for the maintenance and repair of hardware and software
- Data on the support services provided
- Data on the monitoring and evaluation of the functioning of the IT systems
- Data on the control of the personal data protection policies

There are appropriate measures in place to restore access
to the personal data and to ensure its portability.
Transmission of personal data to the European Commission (DG DIGIT) for the Service Now Platform

22-04-24

Directorate IIT
niall.ohiggins@eesc.europa.eu

EESC and CoR

ServiceNow is a platform that already hosts several different applications in DIGIT (EC) for which there is an existing integration with ComRef (the reference database for inter-institutional HR applications). For the moment it includes only European Commission user data.

The ServiceNow userbase needs to be extended with colleagues from EESC-CoR, in particular from DIIT (Directorate Innovation and Information Technology) as they should be part of the current user database for the Service Catalogue.

Therefore, to allow colleagues from EESC and CoR to have unrestricted access to the new DIGIT Service Catalogue, the following user data will be loaded from ComRef onto the ServiceNow platform and processed by it:

- Person ID
- User ID
- First & Last name
- DG/department
- Email address

This record covers the corresponding processing operations of personal data to use the platform (before and after granting access to colleagues from DIIT).

EESC and CoR staff members of DIIT who need to have access to ServiceNow platform

User data in ServiceNow: Person ID, User ID, First name, Last name, DG/department (only for data loaded from ComRef), e-mail address.

Log data for the connection to the platform: Transaction log, User ID, IP address, URL, session ID, Security log, User ID, IP address, browser, privileged user, Yes/No, last URL

Data recipients are restricted to EC DIGIT C.1. corporate platform management team, ServiceNow Administrators on a need to know basis and EESC-CoR DIIT team granted access.

In principle, no data transfer outside the EU are carried out as all data remains in EU/EEA.

The only case of transfer is when a ticket needs to be forwarded for support and technical assistance purposes. This only happens in a situation of third-level support, meaning that the transfer is carried out only as a last resort measure when other support options have not been able to resolve the ticket. Generally, the ticket will only contain technical information related to the troubleshooting. In this case the agreements and contractual clauses with that vendor apply.

User data (imported from ComRef) are removed when user is no longer present in ComRef.

Log data are deleted after 2 years.

User data (through EU-login) are removed after no connection to the platform after 2 years.

The license agreements with ServiceNow includes provisions that ServiceNow is compliant with all the HR.DS cloud recommendations. On top of that all ServiceNow corporate instances are encrypted with encryption keys being stored at Commission (EC) premises. There are appropriate measures in place to ensure that personal data is kept confidential and that access is restricted to authorized users. The team from EC regularly undertakes training and awareness programs for staff, as well as audits and reviews of data protection policies and procedures.