Central register of records of processing activities (ROPA) of personal data carried out by the European Committee of the Regions (CoR) in compliance with Article 31 of Regulation (EU) No 2018/1725

Referen	Name of the data processi	Directorate	Unit	Controller	Joint contr	Joint contr	Processor(s	Purpose(s) of the data processing	Categories of persons whose personal data are processed	Categories of personal data processed	Recipients of the personal data	Transfers of personal data to a third country or an interna	Retention period of the personal data	General description of security measures, where possible
RA1-1	Access to documents	Directorate A	A.1 Services to members	European Committee of the Regions	N/A	N/A	N/A	The purpose is to handle requests for access to documents lodged under Regulation	- Every individual who submits a request for access to documents held by the CoR	a) Personal data of the individual who submits a request for access to documents held	The application is transferred by the Access to documents and Transparency Unit to	The CoR may reply to an applicant requesting access to	The retention period is maximum five (5) years after the	- Regarding paper files:
RA1-2	AGORA	Directorate A	A.1 Services to members	European Committee of the Regions	N/A	N/A	N/A	The collected data enable the administration to manage members' data related to the	Members (full members and alternates), members' assistants, coordinators of national	Basic data processed for transparency purposes:	Internal:	No, personal data are not transferred to non-EU member	Data are kept in Agora for the time necessary to carry out the	- Regarding paper files: N/A
RES-1	KIKLOS	Directorate D	D.3 Digital communication a	European Committee of the Regions	N/A	N/A	Innocraft providing matomo tool for web analytics: https://matomo.org/matomo-cloud-dpa/	The KIKLOS application is an internal working tool to create, edit, plan, follow up and optimize the legislative work of the CoR. It is addressed to accredited users, staff and Members, from CoR, EESC and Joint Services. Data subjects personal data are collected and further processed for the purposes of measurement, usage monitoring and performance evaluation. It does not entail any kind of staff evaluation or personal preferences data usage. . In this regard, personal data may be processed by the web analytics tool "Matomo".	CoR and EESC staff members (authenticated users).	The name, first name and the function of persons involved in the legislative work of the CoR. User traffic is recorded anonymously with the Matomo web analytics tool and used solely for the KIKLOS data collection regarding measurement purposes, usage monitoring and performance evaluation and analysis. Examples of data collected are: page views, visits, unique visitors, site search, countries, members and devices used.	Access to data is defined by KIKLOS permission groups: -KIKLOS Owners are staff members dealing specifically with KIKLOS and have full control rights. -KIKLOS Contributors are responsible for editing content on their respective sections of the KIKLOS (texts, documents) and have read- and contribute-rights. -KIKLOS Visitors are all EESC-CoR users identified with a user name and password. They have read-only rights. -Matomo web analytics superuser are authorised staff of the EESC-CoR IT unit have super user access to the Matomo web analytics tool. They have the possibility to enable or disable anonymisation of personal data, such as the IP addresses and user id. By default the user traffic is anonymised. -Innocraft staff get to access anonymised data only to create analytics reports, used solely for the KIKLOS data collection regarding measurement purposes, usage monitoring and performance evaluation and analysis. Examples of data collected are: page views, visits, unique visitors, site search, countries, members and devices used. -Access to anonymised data is disclosed to staff and members of the CoR via the regular reports done by KIKLOS.	No transfer of personal data to a third country takes place. The anonymized user traffic data are stored in a database in Matomo Cloud, on servers located in Frankfurt and Dublin Matomo web analytics: All raw data are deleted after 24 months and 24 days.	The dynamic text, documents, videos, references, that may contain personal data, is accessible until the staff responsible for KIKLOS removes it.	See DPA of Innocraft www.innocraft.cloud/dpa. Only a very limited number of authorised staff (Matomo web analytics superuser in the IT Unit) have the possibility to disable the anonymization of personal data processed.
RA1-3	Laissez-passer	Directorate A	A.1 Services to members	European Committee of the Regions	European Commission	SLA	N/A	The data is collected and processed with the purpose to issue a laissez-passer, which is a secure travel document to be used by the applicants, when travelling and having been authorized to attend CoR meetings and events.	CoR Members (full members and alternates) CoR staff	Category of the applicant in the CoR (member or staff) Biographical data requested for the issuance of a laissez-passer: - surname; - first name; - nationality; - date of birth; - gender; - place of birth. In addition, a copy of the applicant's passport is made and an application form must be signed.	Access to data has to be granted to: - The staff in Unit A1 (Services to members) (email: OneStopShop@cor.europa.eu) in order to process the requests for issuing a laissez-passer and to respond to possible enquiries from the European Commission (EC) and from police/security authorities in EU countries and in third countries. - CoR legal services and internal audit unit, in case needed. - The staff of the EC central service in charge of issuing a laissez-passer (during the second phase. Enrolment) shall have access to the personal data collected, as the CoR transmits the biometrical data to the EC, so the latter can continue the process of issuing an EU laissez-passer. Such staff abide by statutory, and when required, additional confidentiality agreements.	No, personal data are not transferred to non-EU member states or to international organisations.	The retention period is limited to the period of validity of the issued laissez-passer (maximum 6 years for staff members and maximum for the duration of the mandate plus six (6) months for members). The biographical data are kept in Agora by the delegated controller for the time necessary to carry out the tasks of the CoR service in charge of LP during the mandate of the person concerned. The retention period for the further processing by the EC is detailed in the EC Data protection record (DPR-EC-02010.1) on Issuance of the laissez-passer of the European Union (EU LP). In general according to Article 4 of Council Regulation 1417/2013, a laissez-passer shall be issued for a maximum period of six years and for no less than twelve months. a) For biographical personal data: The retention period should be limited to the duration of validity of the issued EU LP. Personal biographical data are deleted upon expiration of a maximum of 6 years validity period running as from the date of issuance of the laissez-passer. This retention period is without prejudice of longer storage time of the same data for other purposes, for instance of cases of audit or control activities, in other systems of the institution of origin. At the end of those retention periods, the biographical personal data will be erased from the EC laissez-passer central service databases. b) For biometrical data, the retention should be limited to the need as defined by the state of the art, for all holders (normal and/or special applicants as well as ad hoc holders) as defined in the EC relevant privacy statement. At the expiration of the validity of the laissez-passer, any data	Only colleagues working in the service in charge have access to edit data encoded for issuing a laissez-passer. The limited access rights are given by IT on a "need to know" basis. Storage of word/pdf documents in electronic format in the unit's shared drive, with access granted only to colleagues working at One Stop Shop service.
RB1-1	EU organic award	Directorate B	B.1 NAT	European Committee of the Regions	The European Commission , Directorate-General for Agriculture and Rural Developme nt, the European Economic and Social Committee, the European Committee of the Regions, COPA-COGECA and IFOAM Organics Europe,joint ly process personal data in the context of the organisation of the	JCA	N/A	On 25 March 2021, the Commission adopted the "Action Plan for the Development of Organic Production" (COM(2021) 141). It did so in support of the achievement of the target of 25% of EU agricultural land under organic farming and a significant increase in organic aquaculture by 2030 included in both the Farm to Fork and Biodiversity Strategies. This Action Plan includes a number of actions related to "Promoting organic farming and the EU logo". These actions include an action to "stimulate the sector's visibility through awards recognising excellence in the organic food chain in the EU". It has been agreed between the Parties to collaborate for the organisation of these Awards. Personal data shall be processed by the Joint Controllers for the following purposes: 1.Assessing the forms submitted by applicants. 2.Shortlisting three applicants per award. 3.Selecting one winner per award. 4.Notifying the winners. 5.Presenting each winner with their award. 6.Inviting winners to an award ceremony. 7.Communicating externally about the outcome of the contest. 8.Raising awareness among the general public about the next edition of the Awards. Each Joint Controller is responsible for specific activities as follows: (a) Assessment of the forms submitted by applicants: − Best organic region, city & bio-district: the CoR; − Best organic SME, food retailer & organic restaurant: the EESC; − Best organic farmer (male & female): Copa and Cogeca and IFOAM Organics Europe. (b) Shortlisting of three applicants per award: − Best organic region, city & bio-district: the CoR; − Best organic SME, food retailer & organic restaurant: the EESC; − Best organic farmer (male & female): Copa and Cogeca and IFOAM Organics Europe. (c) Selection of one winner per award: − all the Joint Controllers	For the awards under the responsabilities of the COR, Regions, Cities and Biodistricts may apply.	The European Commission tool EU Survey will be used by the applicants for submitting their applications. The Joint Controllers jointly process the following categories of personal data: 1)Identification data: Surname and name; Gender. 2)Contact data: Postal address; Email address; Phone number. 3)Professional data: Position; Business' VAT; Employer's identity. 4)Audio-visual data: Facial image (photos and videos); Voice (audio and video). 5)Unrequested data voluntarily provided by data subjects. In case, you participate to the award ceremony, we will also collect and further process the following categories of personal data: 1) Identification data to access the Commission building: Nationality; Registration number(s) included in identity documentation. 2) Financial data for travel reimbursements purposes: Payment card number; Bank account number. 3) Sensitive data (if any) based on consent that may be considered as health data: Dietary restrictions or requirements; Disabilities or access requirements.	(1) Within each of the Joint Controllers: 1.Staff members who are involved in the organisation of the contest; 2.Natural persons appointed to the seven-member jury responsible for selecting the winners. (2) Outside the Joint Controllers: 1.The European Parliament may receive the personal data as member of the jury; 2.The Council of the European Union may receive the personal data as member of the jury. 3.Other processors of the Joint Controllers 4. Access to some of your personal data may also be provided to the general public if you consented to such purposes	Personal data, collected for the purpose of the processing operation, shall only be processed within the territory of the EU/EEA and shall not leave that territory. Each Party shall inform all other Parties about any transfer of personal data to the recipients in third countries or international organisations.	The Parties shall store the personal data for a maximum of 2 years after the nomination of the awardees to handle potential complaints unless the personal data need to be kept for a longer period given an ongoing complaint, apart from financial data of data subjects who have participated in the ceremony, which will be kept for five years after the ceremony. Contact details of data subjects who have agreed to be contacted for next awards will also be kept until the organisation of the next round of awards (a maximum of 18 months). Sensitive personal data relating to dietary and/or access requirements will be deleted as soon as they are no longer necessary for the purpose for which they have been collected in the framework of the meeting or event, but no later than within 1 month after the end of the ceremony. Parties shall not retain or process personal data longer than necessary to carry out the agreed purposes and obligations as set out in the Arrangement. In case of termination of this Arrangement (by one or more Parties) or in case of expiration of this Arrangement, all personal data shall be deleted.	The processing activities undergoing joint processing are stored on servers based in a Member State of the European Union.
RE1-1	Payment execution and recovery of revenues	Directorate E	E.1 Annual budget and finar	European Committee of the Regions	N/A	N/A	N/A	- Execution of all payments of the CoR, validated by the responsible Authorising Officers, in accordance with the Financial Regulation and Internal Financial rules. - Validation of recovery orders and recovery of the amounts.	- CoR's members -Staff members - Suppliers - Customers	Name, address, bank account number. This information already exists in ABAC or is encoded in ABAC by the responsible financial actors	Financial Institutions	No, your personal data are not transferred to non-EU Member states or to international organisations.	All paper files are kept within the service for a period of 5 years after Parliament's discharge. Afterwards, they are sent to the historical archives of the CoR. Electronic files are kept in ABAC/SAP by DG BUDG pursuant to their data protection rules.	Regarding paper files To prevent unauthorised access to the paper files, the storage room is closed and locked by salary staff every evening. Regarding electronic files Access to the IT systems: ABAC and SAP is protected by an ECAS passwords (the European Commision's authentication service).
RE1-2	Processing salaries and benefits	Directorate E	E.1 Annual budget and finar	European Committee of the Regions	N/A	N/A	N/A	Preparing and authorizing salaries for payment in accordance with the Financial Regulation, the Staff Regulations and the CoR's Internal Financial Rules as materialised in procedures and checklists but relying on the quality of the supervisory and control systems of the HR Units for the data provided.	CoR staff	-Grade, step and personal number (or name), individual rights and time management of officials and agents (Human Resources units input these data in Sysper2 and Payroll application). - When preparing salaries the Salary Service uses an IT-application provided for by the Pay Master's Office (PMO), NAP, that includes inter alia monetary data. The NAP automatically uses the data in Sysper 2 and in Payroll application when making calculations. -However, data covering exceptional payments and recuperations, percentage of pension contribution for part time, transfers abroad are input directly into NAP by the Payroll Service. The data covering the recuperation of childcare facilities and nursery expenses are transferred from a program managed by OIB -The NAP outputs salary data and it is transferred into the IT-workflow/accounting application ABAC/SAP used for inter alia initiation, verification, authorization, payments of salaries and accounting. The actual payments and accounting are done by the Accounting Sector of Unit E1 Annual Budget and Finance. -The Payroll Service input bank account data into ABAC. The IT-application ABAC/SAP is provided for by DG Budget of the European Commission.	Data subjects themselves. The payslips are uploaded in Sysper2 (in the module Rights & Privileges, in 'Latest Payslip' and 'Payslips' (starting 2014/04). Staff of Unit E2 (Recruitment and career) and E3 (Working conditions and talent management) for encoding in Sysper2 (see DPN managed by the EC) Staff of Unit E1 (Internal control and LAM office, and deputy Head of Unit) in the frame of ex-post exercises. NAP Support, the helpdesk of the PMO (the Pay Master Office), in case there is a specific problem about someone's salary. The CoR's Internal Audit Service can access everything at any point in time.	No, your personal data are not transferred to non-EU member states or to international organisations.	The data concerning the career and rights are preserved by the HR Units, especially for determining the rights at pension (a complete career represents about 35 years in service). These data have to be kept as well in order to be able to recalculate any retroactivity for which there is no limit imposed by statutory regulation. These data are kept for 5 years in case of decisions of seizures on salaries after the extinction of the procedure.	Regarding paper files To prevent unauthorised access to the paper files, the offices are closed and locked by salary staff when unattended. Regarding digital data -preventing unauthorised access to the IT systems: for Sysper2, ABAC and NAP we use ECAS passwords (the European Commission's authentication service), for Centurio passwords are in place, managed by the GAU (segregation of duties) with a written procedure and forms requiring proper authorisation. -preventing unauthorised reading, copying, alteration or removal of the storage media: NAP + ABAC: see the IT procedures in the Luxemburg data centre of the PMO -preventing unauthorised memory inputs […]: through the use of passwords in Sysper2, Centurio, NAP and ABAC -preventing unauthorised persons: we access NAP through ECAS passwords (the European Commision's authentication service) and ABAC through TESTA (the network used to communicate among EU institutions) -access to personal data other than those which we have access rights: NAP and ABAC prevent access to non-CoR data. Sysper2 and Centurio prevent access to confidential data. -recording which personal data have been communicated: N/A (personal data are not communicated) -[log] Sysper2, Centurio and ABAC contain a log. -ensuring that during communication the data cannot be read: n.a. (personal data are not communicated) -designing the organisational structure: strict segregation of duties
RE1-1	Business Continuity Plan	Directorate E	E.I - Strategic use of resou	European Committee of the Regions	N/A	N/A	N/A	The purpose of collecting GSM numbers and private email addresses of relevant staff members is to ensure effective management of and communication within the CoR in times of any threat. GSM numbers and private email addresses of Crisis Management Team members and the staff responsible for priority activities are collected and stored as defined in the Business Continuity Plan. GSM number sand private email addresses of staff members in general are encoded by the staff member in question in Sysper.	All CoR staff members, and those exercising priority activities in the frame of the BCP in particular.	GSM numbers and private email addresses of staff members of the CoR responsible for priority activities and GSM numbers of staff members of the CoR.	Pursuant to the Business Continuity Plan framework, following persons are recipient of the data: - Directors and Deputy Directors - Crisis Management Team members - Business Continuity Department - Business Continuity Correspondents - Security officer	No, your personal data are not transferred to a non-EU country or international organisation.	For members of the Crisis Management Team and for staff responsible for priority activities, data are stored for as long as the staff member has this quality according to the BCP. For staff members in general, the general data storage modalities for personal contact data in Sysper apply.	Regarding paper files: Private data is only to be kept in: 1) the "memory card" listing the contact details for the members of the Crisis Management Team (CMT) that is given to the members of this CMT. It has the size of a credit card and is to be carried by the member. 2) before distributing the cards, Unit EI will store them in a locked drawer, the CMT members as well as the BCP Duty Officer (holders of the "memory cards") will sign a confidentiality agreement before receiving the card. 3) a copy of the contact details of the staff in charge of the priority activities in the office and home of the BC Duty Officer and of the Local BC Plans in the offices of the respective Directors. Regarding electronic files: 1) Communication with Crisis Management Team (CMT) members is organised as a rule only via telephone or via the functional BCP mailbox. A specific CoR CMT Signal Group has been created upon unanimous decision by the members of CMT. 2) The data will be stored on the SharePoint-based Convergence Platform. 3) The data printed on "memory cards" will be transmitted to the publication department for its publication. The publication department will consult the data when processing the cards, however they will be asked to destroy all copies afterwards). Communication with staff members in times of crisis is organised as a rule via (professional) e-mail and/or sms texting to private GSM numbers encoded by staff in Sysper.

REI-2	Declaration of assurance of Authorising Officers	Directorate E	E.I - Strategic use of resou	European Committee of the Regions	N/A	N/A	N/A	The Authorising Officer by Delegation (AOD) is responsible for providing reasonable assurance that the resources assigned to the activities described in the Annual Activity Report have been used for the purposes intended in accordance with the principle of sound financial management and that the control procedures put in place provide satisfactory guarantees concerning the legality and regularity of the underlying transactions. The AOD signs the DoAS to this end. In addition, each AOS (Authorising Officer by Sub-delegation) signs a DoAS for the budget lines under his/her responsibility, which feeds into the AOD DoAS, providing assurance to the AOD that the resources allocated to the activities financed from the concerned budget headings were used for the purposes intended and in accordance with the principle of sound financial management and that the monitoring procedures established provide the necessary guarantees of the legality and regularity of the underlying transactions. Name, signature and position of the AOS are collected and archived in Unit EI, in accordance with the requirements of the Financial Regulation	CoR Staff members appointed AOD or AOS.	Name, signature and position in the CoR organigram.	Pursuant CoR Annual Activity Report procedure: Head of Unit EI-Strategic use of resources, smart house General Administration and Public Procurement Administrator Planning and Reporting within unit E4 (Deputy-) Director for Human Resources and Finance Head or advisors of the Private Office of the Secretary General Secretary General Out of the CoR: Discharge authority (European Parliament)	No, your personal data are not transferred to non-EU Member States or to international organisations.	Following art 75 of the FR, 5 years minimun from the date on which the EP grants discharge for the budgetary year to which the document relates.	Regarding paper files Original hard copies of the Declaration of assurance is kept as part of the Annual Activity Report by unit EI in the archives, in a locked cabinet. Regarding digital data The data (scans of the DoAs) are stored on a shared drive accessible to Unit EI only.
REI-3	Register of Charters of financial actors	Directorate E	E.I - Strategic use of resou	European Committee of the Regions	N/A	N/A	N/A	When a new financial actor is appointed, it is required he/she signs the charter of financial actors, as foreseen in CoR decision n° 14/2018 on the internal financial rules for implementing the Committee of the Regions section of the general budget of the EU. The purpose of the processing is to ensure every financial actor knows his/her duties and obligations under general and CoR financial regulations. To this aim they are to sign the charter of financial actors in order to officially confirm this knowledge. Name, signature and position of the AOS are collected and archived in Unit EI, in accordance with the requirements of the Financial Regulations.	CoR and EESC Staff members appointed as financial actors for the CoR.	Name, signature and position in the CoR organigram.	CoR Local Authorisations Managers within Directorate E-Human resources and finances and any financial actor can consult the signed charters, as well as the Court of Auditors.	No, your personal data are not transferred to non-EU Member States or to international organisations.	Following art 75 of the FR, 5 years minimun from the date on which the EP grants discharge for the budgetary year during which appointment of the financial actor was terminated.	Regarding paper files Signed charters as well as the registry are kept as part by unit EI in the archives, in a locked cabinet. Regarding digital data The data (register and scans) are stored on a shared drive accessible only to appointed Local Authorisations Managers and the Head of Unit EI.
RE4-1	EU Sign	Directorate E	E.4 Financial management	European Committee of the Regions	N/A	N/A	N/A	The present data protection notice focusses on the steps of the QeS certificate issuance process for which the delegated CoR controller is directly responsible. This implies processing of your personal data for the following three internal processing purposes: A) Assessment of eligibility for the creation of a QeS profile QeS profiles are created on a service needs basis only, for CoR staff members and other relevant beneficiaries whose functions requires them to regularly sign documents in electronic form which, for reasons of legal validity, must bear a qualified electronic signature. This notably includes the CoR President, the CoR First Vice-President, CoR authorising officers and possibly other relevant CoR staff members. Whenever the creation of a QeS profile is requested, the delegated controller processes personal data in order to assess the eligibility of the CoR requester for a QeS, notably considering the justification they provided in their request (such as, for instance, type and number of legal documents/commitments to be signed). Requests for the creation of a QeS profile are submitted on a voluntary basis by CoR staff members and other relevant beneficiaries. The delegated controller processes personal data also when monitoring the eligibility of CoR requesters on the long run and when requesting the deletion of invalid QeS profiles. B) Transfer of relevant personal data to the European Commission When a request for the creation of a QeS profile is deemed eligible, the delegated controller transfers relevant personal data (identification and contact data) to the European Commission's Directorate-General for Informatics (DG DIGIT). Pursuant to a service-level agreement (n° DIGIT-058-2020 – 08/12/2020) and an EU Sign-related addendum (n° 1 – 10/09/2021), DG DIGIT (Unit D.3 - DIGITAL IDENTITY AND SIGNATURE SERVICE – DIGIT-DATA-PROTECTION-COORDINATOR@ec.europa.eu) is solely responsible for the creation and deletion of QeS profiles, and thus for contacting the CoR requester directly in order to collect the personal data necessary for the creation of their QeS profile. DG DIGIT acts as a controller when processing the personal data it collects from the CoR requester (see information about such processing here: https://ec.europa.eu/dpo-register/detail/DPR-EC-03187). DG DIGIT uses an external contractor for delivery	Internal to the organisation: CoR President; CoR First Vice President; statutory staff members of the CoR.	•Identification data: forename, surname •Contact data: corporate email address, corporate phone number •Professional data: function(s)/assignment, career, QeS profile •Electronic communications: emails	Within the institution: Statutory staff members of the CoR assigned to the delegated controller, on a need-to-know basis [all data categories] Outside the institution: Staff members of the European Commission assigned to the electronic signature service at DG DIGIT [identification data and contact data only].	No, your pesonal data will not be transferred to a third country or international organisation.	The following personal data related to a CoR requester, as well as data regarding the justification provided, are kept for the entire period during which that CoR requester holds a QeS profile: •Identification data: forename, surname •Contact data: corporate email address, corporate phone number •Professional data: function(s)/assignment, career, QeS profile. Electronic communications (emails) between the delegated controller and a CoR requester related to the latter's QeS profile are kept for a period of two (2) years. The following data are kept for a period of seven (7) years after the date of termination of the QeS certificate issued to a CoR requester, for sound financial management purposes in compliance with the provisions of article 75 FR (requiring essential supporting documents to be kept at least five years from the date on which the European Parliament gives discharge for the financial year to which the documents relate): •Identification data: forename, surname •Professional data: QeS profile (date of issuance and date of termination of the QeS certificate)	Personal data processed by the delegated controller are exchanged via a dedicated functional mailbox and stored on a dedicated shared drive, with limited need-to-know-based access rights.
RE4-3	Staff Missions	Directorate E	E.4 Financial management	European Committee of the Regions	N/A	N/A	Carlson Wagons-lits Travels	The purpose of the processing operation is to allow staff to go on mission for professional reasons.	CoR staff leaving on mission for professional reasons.	Surname, first name, address, CoR staff number, professional telephone number, professional email.	Members of the CoR Missions Service, authorising officers from the budget line for missions expences, verification cell, accounts, and members of the travel agency company linked to the CoR by a contract relating to staff missions. Hierarchical superiors and OIA in the assignment services (operational initiate staff) have access to it for the missions of members of their service/unit/directorate.	No, your personal data are not transferred to non-EU member states or to international organisations.	5 years after the date of discharge by the EP for the budget year in which the mission is carried out.	Electronic storage – functional mailbox of the Missions Service (svc-missions-cdr@cor.europa.eu). Staff missions are encoded in the MIMA application managed by the Missions Service. Only the members of that department, the authorising officers responsible for the budget heading for missions and the verification service have access to it in full. The line managers and OIA in the department to which they are assigned (operational initiating agents) have access to it for missions by members of their department/unit/directorate. The rest of the staff have access only for their own tasks. A Windows password is needed to access MIMA. The data are also transmitted to the travel agency via its online travel management tool. Finally, for budgetary and statistical monitoring reasons, BO reports are taken from MIMA and stored in Excel spreadsheets in the Missions department alone. These spreadsheets are password-protected.
RE4-4	Staff Mobility	Directorate E	E.4 Financial management	European Committee of the Regions	N/A	N/A	N/A	The purpose of the processing is to allow the reimbursement of certain costs related to staff mobility from and to the place of work, namely public transport season tickets.	CoR staff members wishing to be reimbursed for public transport season tickets.	Surname, first name, address, CoR staff number, professional telephone number, professional email.	Members of the CoR Mobility Service, authorising officers for the mobility budget line, verification unit, accounting.	No, your personal data are not transferred to non-EU member states or to international organisations	5 years after the date of discharge by the EP in respect of the budget year in which the reimbursement is made.	Concerning physical files Applications for reimbursement of public transport season tickets shall be submitted in paper format. They are filled in by the staff member and then reach the relevant service. These requests are also seen by the authorising officer by the verification and accounting services. They are then archived under key to the Mobility Service. Electronic files For budgetary and statistical monitoring reasons, Excel spreadsheets are compiled within the Mobility Service alone. These spreadsheets are password-protected.
RB2-1	Study on energy governance	Directorate B	B.2 ENVE	European Committee of the Regions	European Committee of the Regions (CoR) and Council of European Municipalities and Regions (CEMR) - 1 Square de Meeûs B - 1000 Brussels Tel : + 32 2 511 74 - email : info@ccre-	JCA	Milieu Consulting srl	Personal data will be collected from the persons participating to the online EU survey and the interviews. In addition, the established report on 'Local and regional authorities in the governance of the energy union', based on the collected data, may include personal data if consent has been provided to refer to concrete examples. This report will feed into any CoR's consultative work on the governance of the Energy Union, the CoR's reflection on the Future of the Green Deal, as well as possibly the CoR's 2023 Report on the State of Regions and Cities. CEMR will use the data for its own publication on NECPs, which aims to study the Local and regional government relevant competences and the subnational governments involvement in the revision of the different national plans, provide them with comparative case studies and inform CEMR members on the state of play of the implementation of article 11 of the Governance of the Energy Union and Climate Action Regulation.	Respondents to the survey questionnaire.	First name, last name, email address, function/position in the organisation.	-European Committee of the Regions (CoR) Directorate for Legislative Work I – Unit B2 (ENVE commission), -CEMR, -Milieu srl	No, your personal data are not transferred to non-EU Member States or to international organisations.	Maximum one year after the delivery of the final report.	Data are kept in EU Survey and in shared drives with limited access to the recipients of the data.
RA1-5	Publication of meetings	Directorate A	A.1 Services to members	European Committee of the Regions	N/A	N/A	N/A	On 4 July 2023, The CoR Bureau adopted Regulation n° 6/2023 on transparency measures at the CoR in accordance with the Interinstitutional Agreement of 20 May 2021 between the European Parliament, the Council of the European Union and the European Commission on a mandatory transparency register (IIA). Pursuant to this Regulation, starting 1 January 2024, office-holding CoR members and rapporteurs shall make public information on all meetings held by them in their official capacity as CoR member with interest representatives falling under the scope of the IIA. More specifically, at the latest two months following the meeting, the following information shall be made public on the CoR website: date of the meeting, location of the meeting, subject of the meeting, name of the CoR office holding member or rapporteur and name of the interest representative.	The categories of persons whose data are processed are interest representatives falling under the scope of the IIA, that is to say: any natural or legal person, or formal or informal group, association or network that interact with CoR office holding members or rapporteurs to engage in 'covered activities' with the objective of influencing the formulation or implementation of policy or legislation, or the decision-making processes of the institutions in the sense of article 3 IIA. Interest representatives' data shall not be processed: * when they perform 'not-covered activities' pursuant to article 4§1 IIA (such as experts making submissions to direct and specific requests from the institution or its representatives for factual information, data or expertise or when they make submissions to a stakeholder consultation in the framework of a legal administrative procedure established by Union law); * when they are excluded from the scope of IIA in accordance to article 4§2 IIA (such as public authorities on national or subnational level and their associations or networks, political parties and members or staff of EU institutions); * when they meet with CoR office holding members or rapporteurs outside the latter's official quality as CoR member (for instance when they meet them in private or in the context of the local or regional mandate on the basis of which they have been appointed to the CoR).	In addition to information regarding the date, location and subject of the meeting as well as on the CoR member with whom they meet, the personal data processed is the name of the interest representative (be it a natural or legal person, or formal or informal group, association or network).	a) Within the organisation CoR staff members assigned to the secretariats working with the designated office-holding members and rapporteurs as indicated under point 2 (for publication purposes) as well as, potentially, CoR staff members of the OneStopShop within unit A1 (as service responsible for the horizontal coordination of the process on behalf of the controller). b) Outside the organisation The general public (the meeting lists with interest representatives' personal data are made accessible to any person consulting the related pages of the CoR website).	No, personal data are not transferred to non-EU Members States or to international organisations.	For meetings with office-holding members, the meeting lists with interest representatives' personal data shall be available on the concerned member's pages for the duration of their mandate as an office-holding member. If the member's mandate is renewed in the same office-holding position or in a different office-holding position, the list shall remain and will keep being updated. In the event of successive mandates in an office-holding position, data shall noth be kept for more than 10 years. For meetings with rapporteurs, the meeting lists with interest representatives' personal data shall be available for a period of ten years following the adoption of the opinion or report in question. If a member is appointed rapporteur for consecutive opinions or reports, the previous list shall remain and will keep being updated without prejudice to the deletion of data after a period of ten years following the adoption of a previous opinion or report. When an office-holding member or rapporteur ceases to be member of the CoR, the information shall no longer be available on-line but may still be accessed pursuant to the provisions of Regulation 1049/2001 on the public's right of access to documents of Community institutions and bodies, without prejudice to the deletion of data after a period of ten years.	Personal data are stored on shared folders with limited access to CoR staff members on a need to-know basis in function of the member having a meeting with interest representatives (as indicated under "Recipients").
RA1-6	Legislative footprint	Directorate A	A.1 Services to members	European Committee of the Regions	N/A	N/A	N/A	On 4 July 2023, The CoR Bureau adopted Regulation n° 6/2023 on transparency measures at the CoR in accordance with the Interinstitutional Agreement of 20 May 2021 between the European Parliament, the Council of the European Union and the European Commission on a mandatory transparency register (IIA). Pursuant to this Regulation, starting 1 January 2024, CoR rapporteurs may, on a voluntary basis, and under their exclusive responsibility, draw up a 'legislative footprint', collecting a non-exhaustive list of organisations and individuals from whom the rapporteur has received input in drawing up the opinion or report. The case being, the legislative footprint shall be included to the file related to the opinion or report in the CoR archives.	The name of natural persons interacting with the concerned rapporteur for the purposes of drafting a CoR opinion or report.	The "legislative footprint" processes personal data of person of individuals acting in their name and in a self-employed capacity or together with the name of a legal person (organisation, group, association or network).	a) Within the organisation Within the CoR, the personal data on interest representatives having provided input to the elaboration of an opinion or report are shared with the CoR staff members assigned to the Commission secretariats working with the designated rapporteurs, with the staff of the CoR Archives department in unit A1 as well as, potentially, with the CoR staff members of the OneStopShop within unit A1 (as service responsible for the horizontal coordination of the process on behalf of the controller). b) Outside the organisation As the file related to CoR opinions and reports includes public documents in the sense of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, the legislative footprint accompanying CoR opinions or reports are accessible to the general public, on request, along with the other documents of the file.	No	The legislative footprint shall be included into the file related to the opinion or report in the CoR archives. As they relate to the EU legislative process, all documents included in the file of an opinion or report – including the legislative footprint – are as a rule kept for an indefinite period or time. Such open ended transparency allows the citizen, including scientific researchers (be it for contemporary or historic analytical purposes), to follow the activities and be aware of the potential influence of interest representatives on a given CoR opinion or report. To be noted that, pursuant to the provisions of Council Regulation (EEC, Euratom) 354/83 (last amended by Regulation 496/2015), after 30 years, the CoR transfers its 'historical archives' to the Historical Archives of the European Union (HAEU), located in Florence.	Regarding paper files: The paper archives are kept and processed in secure areas which are accessible only to authorised personel. Regarding digital data: The digital archives are stored and processed on dedicated drives with limited access rights, on a strict need-to-know basis.
RB3-2	Study on attracting Global Skills and Talents	Directorate B	B.3 CIVEX	European Committee of the Regions	N/A	N/A	British Institute of International and Comparative Law	Personal data will be collected from the persons participating to the online EU survey and the interviews. In addition, the established report on 'Attracting Global Skills and Talents to EU's cities and regions', based on the collected data, may include personal data if consent has been provided to refer to concrete examples. This report will feed into any CoR's consultative work on migration and integration policies, the CoR's reflection on the proposals of the European Commission in this area, as well as possibly the CoR's 2024 Report on the State of Regions and Cities.	Respondents to the survey questionnaire.	First name, last name, email address, function/position in the organisation.	European Committee of the Regions (CoR) Directorate for Legislative Work I – Unit B3 (CIVEX commision), British Institute of International and Comparative Law.	The personal data are transferred to United Kingdom by the processor based in United Kingdom, who ensures the same level of personal data protection pursuant to the Commission implementing Decision (EU)2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.	Maximum one year after the delivery of the final report, except for personal data included in the established report on 'Attracting Global Skills and Talents to EU's cities and regions' if consent has been provided to refer to concrete examples.	Data are kept in EU Survey and in shared drives with limited access to the recipients of the data.

RD3-2	Dynamics 365	Directorate D	D.3 Digital communication a	European Committee of the Regions	N/A	N/A	Microsoft Ireland	The CoR makes use of Microsoft Dynamics 365 Marketing, an email marketing tool that allows emails to be created and sent, as well as statistics to be generated. Dynamics 365 is a cloud-based platform that allows us to orchestrate personalized emails/journeys to increase the engagement of our audience and have more impact with all our communications. - Stakeholder relationship management: 360° contact view with one central point of all contact data and history - Email marketing: Keeping the target audience informed about the work of the CoR through newsletters, press releases and similar mailings - Event management via event registration platform: Management of session registrations, automation of confirmation emails, generating e-tickets, reducing manual effort and ensuring a smooth registration experience for attendees - Internal communication (newsletter for members, cultural events etc.) - Analytics/reporting: Via Dynamics Insights we can measure the impact of our mailing based on the open rate, click-through rate and heat map.	Depending on the purposes of the data processing, the following categories of persons, whose data are processed, could be listed: - individual subscribers to our emailings; - recognised experts and other stakeholders in subjects about which CoR is preparing a consultation; - representatives of regional and local bodies who either hold a regional or local authority electoral mandate or are politically accountable to an elected assembly; - past event/survey participants who have expressed interest in staying informed either about our consultations or about all CoR communications; - CoR Members and Alternates; - CoR staff; CoR retirees; Members and staff of other European Institutions; Contacts from "Accredited associations"; - "CoR Regional offices", "Europe Direct", "National EU associations" and Permanent Representations; - other external contacts not falling into previous categories and who have subscribed to receive emailings from EventsCoR is preparing a consultation.	Some or all of: - Email address, - last name, - first name, - gender, - organisation, - country represented, - region represented, - NUTS classification, - department, office, job title, mandate start and end date, salutation, languages, - phone number, - X, Facebook, LinkedIn, Instagram account, - street and number, postal code, city, country, - role in the organisation, - areas of interest, and - for CoR Members – political affiliation.	CoR and CoR/EESC Joint Services staff (officials, temporary agents, contract agents, seconded national experts, trainees), who request it for the purposes of their work , and who are granted access based on the needs of their job , and after having completed the relevant training.	The CoR does not transfer personal data to third countries directly. The data exporter for the transfers which take place under the ILA is the processor (Microsoft Ireland Operations Ltd.) and the data importer the sub-processor (Microsoft Corp.) All personal data in electronic format (emails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the CoR's data centre or in Microsoft data centres in the EU (linked to the EESC-COR M365 tenant). To protect data subjects personal data, the CoR has put in place several strong contractual safeguards, complemented by technical and organisational measures. In addition to the general policy of Microsoft to secure personal data by means of pseudonymisation and encryption (at rest and in transit), the risk of disclosure of personal data to third country authorities by Microsoft Ireland and its affiliates is mitigated by customised contractual provisions and technical and organisational measures. Contractual provisions address the way Microsoft responds to access requests, limiting risks to personal data of the customer. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation. Data is not transferred to international organisation(s).	By default, personal data in Dynamics 365 are kept for an indefinite period, either in an active or inactive status. There is always the "unsubscription" option available for the users and/or the option to be deleted from the database upon request. Data is no longer used after the data subject opts out of all CoR content. Data is deleted without undue delay and in any event within one month upon receipt of the request to do so. Note that CoR and other EU institutional contacts are updated automatically in Dynamics 365 by other IT services and deactivated when they stop working. If they have no subscriptions then these too are deleted in a certain period of time otherwise they are retained indefinitely or until they unsubscribe globally.	Standard Dynamics 365 security is applied.
RD3-3	CoR Intranet (MYCOR)	Directorate D	D.3 Digital communication a	European Committee of the Regions	N/A	N/A	For the Sharepoint application, the processor is Microsoft (see further the DPN Microsoft 365). For web analytics, the processor is Innocraft, who provides a web analytics tool, Matomo, in Microsoft Sharepoint Environnement (see further the Matomo Data Processing Agreement link below).	The CoR intranet is the internal working tool and information channel for the staff and members of the CoR and the EESC/Joint services. It's a SharePoint-based collaborative web application, meaning that contributors or owners can share information, articles and documents directly with all colleagues. For the efficient function of the CoR's intranet, your personal data may also be processed. It is meant to facilitate communication between colleagues in various buildings and members in the member states. The intranet allows staff inter alia to: - find out who colleagues are and on what they work; - find administrative information and forms; - view images, interviews and videos from events or for internal communication; - access various applications needed for the daily work or for administrative matters;.	CoR and EESC staff members (authenticated users).	- Processing of content (texts, documents, images, videos) on the intranet pages is manual – each Intranet contributor has responsibility for the content they upload on their respective sections of the intranet, having obtained the consent from the persons appearing in them. - On the Who is who pages and/or parts on the CoR intranet, name, official work title, office number, phone number, e-mail are collected from the staff database (ECAS/Sysper data protection notice), structured according to Directorates/units. Photos are automatically imported from the Sysper database, in case the person agreed with the publication [Specific Privacy Statement SysPer, March 2017 version]. - User traffic is recorded anonymously within the SharePoint Analytics tool and the Matomo web analytics tool. Information collected is anonymised and used solely for CoR intranet data collection regarding measurement purposes, usage monitoring and performance evaluation and analysis. It does not entail any kind of staff evaluation or personal preferences data usage. Examples of data collected are: top pages, average number of daily unique visitors, page views, busiest day and time, search words.	- All authenticated users (CoR staff and members and EESC staff and members and Joint services staff) have access to the intranet; - Webmaster team's staff (who manages the MyCoR page); - Matomo web analytis superuser: authorised staff of the IT unit have super user access to the Matomo web analytics tool. They have the possibility to enable or disable anonymisation of personal data, such as the IP addresses and user ID. By default the user traffic is anonymised; - Innocraft staff get access to anonymised data only to create analytics reports, used solely for the intranet data collection regarding measurement purposes, usage monitoring and performance evaluation and analysis. Examples of data collected are: page views, visits, unique visitors, site search, countries, members and devices used.	No transfer of personal data to to a third country or international organisation takes place. The CoR intranet data is stored in a database in the Innocraft/Matomo Analytics Cloud, on servers located in in Frankfurt and Dublin.	- The data on the Who is who pages and/or parts are derived from the Sysper staff database and will be available on the Intranet for as long as the person is active. - Intranet content (texts, documents, calendars, images, videos, references): accessible until the Intranet contributors or Intranet owners remove it. - User traffic: The CoR intranet data (anonymised) in the Sharepoint environment is stored for 15 calendar days on the CoR/EESC IT unit's servers on the CoR premises (with backups on tapes, kept for a period of 3 months). - Matomo web analytics: All visits and actions raw data are deleted after 24 months and 24 days.	See DPA of Innocraft https://www.innocraft.cloud/dpa. Only a very limited number of authorised staff (Matomo web analytics superuser in the IT Unit) have the possibility to disable the anonymization of personal data processed.
RDI-1	Futurium	Directorate D	D.I - Coordination, planning,	European Committee of the Regions	N/A	N/A	European Commission (Directorate General for Communication Networks, Content and Technology (DG CONNECT)	The purpose of the processing is to facilitate the operation and management of the European Network of Regional and Local Councillors, that is an initiative run by the CoR for local or regional politicians having a political mandate at regional or local level in one of the EU Member States. Personal data received from the EU-Councillors is necessary to ensure that the network operates and carries out its functions. Specifically, the processing of personal data is necessary for: •the operation and management of the network; •the approval of the membership for being part of the EU-Councillors group on the Futurium platform and of the EU-Councillors' Facebook group; •the communication activities such as webinars, meetings and networking sessions with CoR members and EU experts, exchange of correspondence, sending invitations to flagship events, political debates and meetings at EU, national and local level, as well as distribution of a weekly info flash and a monthly newsletter; •the organisation of training on social media tools and channels, as well as digital masterclasses and coaching; •the conducting of surveys to gather members ideas and proposals on how to develop the network further.	Regional and local politicians who are elected representatives in a government, parliament or assembly of a region, city, town, province, municipality or village and hold an active mandate.	- Name (first and last name); - Email; - Gender (How one identifies oneself); - Languages; - Country; - Name of the locality represented; - Postcode of the locality; - Region (or equivalent); - Political mandate or function; - National political party; - Political affiliation at European Level; - Mandate End date (upload proof/link of the mandate); - Name of other(s) member(s) of the CoR from the applicants' city or region.	Access to the personal data collected for the processing operation in question is provided to the authorised personnel of the CoR and its processor responsible for carrying out this processing operation according to the "need to know" principle. - Moderators and administrators from Directorate D of CoR collect personal data via the applications in EU Survey filled in by the candidate to become part of the EU Councillors network. Once confirmed that the candidate fulfils the condition of having a current political mandate at regional or local level in one of the EU Member States, the members are invited to create an account via EU-Login in order to have access to the network group (link provided) and benefit from the range of services available to them, as well as are integrated in the CoR's Data management database (Dynamics 365). - Staff members of the processor at DG Connect have access, under the Data Processing Agreement, to the necessary personal data of the network members for the purposes of adding members to the group; giving management role to some members; sending notifications (depending on members's preference); taking care of the platform maintenance and development. - The members of the European Network of Regional and Local Councillors have access to the name of the other members, as well as to the information the members provided themselves in the EU Councillors group in Futurium or in the EU Councillors Facebook group.	No	Personal data necessary for the management of the network (including the management of contact lists for correspondence) is stored in the CoR's Data management database (Dynamics 365) and in the service providers' (processor) database for as long as the data subject participates in the group and for a maximum period of 3 (three) years afterwards. Once the mandate has expired and if an individual member ceases to be a member of the network, unit D.I will remove the person from the EU-Councillors member's list and informs the processor to do alike in due time.	The security measures are those of the tools used, so notably: - EU Survey - Dynamics 365 - Futurium platform - Facebook
RD2-4	Summit of Regions and Cities	Directorate D	D.2 Events and local dialog	European Committee of the Regions	Walloon Region	JCA (EN) JCA(FR)	Pracsis	- Register participants to the 10th European Summit of Regions and Cities; - Provide access to the venue; - Link participants to the corresponding category for specific organisational and administrative reasons; - Respond to participants' personal special requirements (mobility, food preferences, etc.); - Maintain the possibility to update registration data; - Provide useful guidelines/instructions on this particular event (with participants' consent only); - Fulfil the communication objectives of the 10th European Summit of Regions and Cities (with participants' consent only); - Share participants' name with the other participants (with participants' consent only); - Send invitations to participants for future events the CoR and/or WR may organise (with participants' consent only).	- Participants to the event (e.g. MEPs, CoR members, YEPs); - VIP guests; - Speakers; - Journalists; - Citizens; - Invited persons (e.g. pupils and their teachers/parents after their consent).	- information necessary for registration: title, first name, surname, country of residence/occupation, e-mail, phone number, name of organisation; - information necessary for access to the conference venues: number of ID card/passport, date of birth, date of birth, nationality and in the case of a VIP guest the following personal data will be processed: first name, surname, role (such as minister, ambassador, etc) and vehicle registration number; - Information necessary for specific organizational, administrative and financial (reimbursement) purposes: participant's category (Young Elected Politicians, EU Councilors, speakers, journalists); - Photos, audio and video recordings and web streaming related to the 10th European Summit of Regions and Cities; Additionally, based on consent of the data subject (provided via the event registration form or oniste at the registration desk during the event): - information necessary for commuting services: hotel reservations, arrival/departure details; - information necessary for special requirements: disabilities, food preferences;	- CoR's and WR's staff in charge of coordinating, organising, managing and following-up the event; - CoR's and WR's contractors related to the event, only to the point and extent needed to perform their duties, acting only under instructions from CoR and WR and in compliance with the agreed purposes of processing and Article 29 of Regulation (EU) 2018/1725 and Article 28 of Regulation (EU) 2016/679, respectively. Photographs and/or audio and video recordings could be published in the context of the 10th European Summit of Regions and Cities and in the framework of CoR and WR activities on the web, including via social media. If need be, the files containing the video materials may be slightly altered (for example, brightness and contrast) so that they can be used for the purposes for which they were taken. Some live web streaming, video recording and images of the speakers and the participants, as well as photographs of groups of participants and organisers are taken and published in the context of the event activities (during and afterwards).	No (apart the communication by Internet and social media).	12 months after the end of the event, unless the data subjects explicitly agreed to their contact details being kept in order to receive invitations to future similar events organised by the data Joint Controllers (CoR and/or WR). In accordance with Article 75 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, financial data is kept for at least five years from the date on which the European Parliament gives discharge for the financial year to which the documents relate. Concerning accreditation, ID card or passport number is kept for 12 months. Photos, audio and video recordings may have been published (for example on the web or in publications) will remain in that format indefinitely.	Data is secured on: - Commission servers and on contractors' premises; a security convention is established between the contractors and the Commission. - Walloon Region servers and on contractors' premises; - Standard Dynamics security is enforced for communication actions.
RD3-4	Webstreaming	Directorate D	D.3 Digital communication a	European Committee of the Regions	N/A	N/A	Processor: Streamovations offers the centralized stream management system (CMS) in the cloud (Sub-processor: Google datacenter)	Web-streaming is a technology to deliver live images and sound on the web (Internet or Intranet) to a designated public. Web streaming contributes to the transparency enabling citizens to follow the CoRs activities (meetings, events, plenary sessions etc.) by allowing the dissemination of the CoRs proceedings and therefore extending CoRs reach. This is a generic record of processing acivity, covering information relating to web-streaming of public activities of CoR following a request from any organiser within CoR and covered by the external contractor of CoR (processor: Streamovations). As each event/meeting or conference may be different in terms of the intended audience, the web-streaming is covered by a specific DPN for the event being webstreamed. For example, the management of audiovisual recordings of the CoRs statutory meetings are covered by a specific ROPA and DPN (Dir A: RA2-7). DESCRIPTION OF THE PROCESSING The delegated controller and the processor collect and process your personal information to provide the web-streaming and audio-visual recording of an event, as well as to deliver live images and sound on the web (internet or intranet) to a designated public. At the request of the organising CoR department, live web-streaming and audio-visual recording of the speakers, organisers and participants will be carried out and published in the context of the event on the specific website or place indicated in the specific data protection notice (DPN) linked to the event. The audience or non-speaker participants may appear in the web-streaming and audio-visual recording of the whole event. The meeting/event organiser requests the web-streaming and audio-visual recording of an event via the booking form (Ticketing system) in the CoR's internal booking system. The web-streaming (and possible audio-visual recording) of the event is validated by the streaming operator (Dir D, A and Streamovations) and becomes available on the CoR's relevant cloud (https://frontend.cor.sirnv.cloud/). Its type of access is specified by the organiser of the event, and it can be internal or public (=Intranet or Internet). In this context the processor (Streamovations) is responsible for the processing of personal data (info@streamovations.be) when one submits a request to download	- Internal to the CoR: Potentially any person working in the CoR and participating in a web-streamed event (CoR members, staff etc). - External to the organisation: Any participant or group of participants to a meeting, event, conference which is being web-streamed.	- Participants of the meeting/event: The web-streaming processes the voice and image of participants of the meeting/event, as well as possibly the name, organisation and role or function identifying the participants/speakers. - Meeting/Event Organiser: person who introduces the web-streaming request in the ticketing system, which is the entry point of the creation of a web-streaming request. - Interpreters: voice and interpretation performance/service during the meeting/event and possible image. - If a request to download specific parts of a video-on-demand after web-streaming was made, the requesting email address is processed.	It is the responsibility of the Meeting/Event Organiser of CoR to inform participants in the specific Data Protection Notice (DPN) of the event about the type of access that it has selected to apply on the web-streaming (possibly on Internet or only available to staff in the CoR and/or EESC using a password). The Meeting/Event Organiser should also inform participants (in the DPN) if there is further processing of the personal data (e.g.: processing the streaming or video-on-demand through other platforms including other European institutions' web-players and social media). Access to the personal email, in the case a request to download specific parts of a video-on-demand is made, is provided to the CoR's staff responsible for carrying out this processing operation and to authorised staff of the processor according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.	Personal data will not be transferred to a non-EU country or international organisation. The recording of the web-streamed event is available on the web-streaming e.g. portal or on the website of the CoR, Streamovation's platform and can be embedded on other websites. The recording can be directly downloaded by citizens or organisations. In case, such recording should be reposted on other (social media) platforms, the administrator of the social media account or the website and/or the individual posting the recording becomes responsible and therefore the controller of the personal data.	Videos are stored as video-on-demand according to the duration defined by the Meeting/Event organiser in the specific Data Protection Notice (DPN) of the meeting or event, for a maximum of five years. When a request is submitted to download specific parts of a video-on-demand, the email address used by the Processor is kept for a maximum of one year.	- Access to emails provided for the service is restricted to the processor's system administrators and communicated to the CoR by secure email to a predefined contact point. Data is treated in accordance with the internal confidentiality policy. - Servers where data is stored are located in the EU (Saint-Ghislain, Belgium). - The impact of potential leak of personal identification information (PII) is limited as the email addresses are not linked to any other personal identification information. - Statistics are gathered unonymized for connection IPs and geopositioning. No other personal data are gathered via other means from the platform (e.g no cookies)
RD3-5	Newsroom	Directorate D	D.3 Digital communication a	European Committee of the Regions	N/A	N/A	The European Commission Directorate-General for Communication Networks, Content and Technology (DG CONNECT) (CNECT-MEWSRO OM-SUPPORT @ec.europa.eu)	Personal data may be collected and processed for the use of Newsroom, which is a tool that allows CoR to send newsletters or notifications in the areas of CoRs activities and political groups activities upon data subjects request. The controller and the processor collect and further process personal data, upon one's subscription to the respective newsletter depending on the topic of interests and the frequency of notifications. This allows the subscribers to receive information that they have requested on important developments, activities, events, initiatives or thematic issues in the area of the CoRs activities, consultations of the CoRs commissions (COVEX, COTER, ECON, ENVE, NAT, SEDEC) and news, in particular through events, news, opinions, publications, regional news, studies.	- Internal to the organisation: Staff working for the CoR; - External to the organisation: General public, Members of CoR, staff of Member States' authorities, journalists, the academic/scientific/research community, law firms, etc.	Categories of personal data: - Name, surname; - Email address; - Organisation; Additional personal data is needed for providing the subscribers with a more personalised information and for generating anonymised statistics: - Frequency of the newsletter (daily/weekly); - Type of information preferred (events, news, opinions, publications, regional news, studies); - Preferred language(s); - Topics of interest.	- Within the CoR: CoR staff responsible for carrying out this processing operation and other authorised CoR staff according to the "need to know" principle. - Outside the CoR: European Commission's staff, who is the processor for managing the subscriptions of the subcribers to the respective newsletter/notification system. In particular the processor (DG CONNECT) collects the e-mail address of each subscriber, their topic of interests and the frequency of the notifications. Personal data needs to be processed by the processor in order for the service to be provided to the controller. Such staff abide by statutory, and when required, additional confidentiality agreements. The processor is bound by the signed Data Protection Agreement (DPA) between the parties and by the confidentiality obligations deriving from the EUDPR Regulation (EU) 1725/2018. Pursuant to Article 3(1) of Regulation (EU) 2018/1725 public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. The personal data collected will not be given to any third party, except to the extent and for the purpose required by law.	No, personal data are not transferred to non-EU member states or to international organisations.	The controller and the processor only keep personal data for the time necessary to fulfil the purpose of collection, namely until the data subjects unsubscribe from the mailing list. Depending on the technical solutions available, subscribers can either write to the dedicated functional mailbox and ask to be unsubscribed from the mailing list or follow the unsubscribe link in the information email they have received. Appropriate action shall be taken within one month of receiving the request. In case where data is kept for statistical purposes, subscriber's additional data (frequency, type of information, preferred language(s), topics of interest) may be kept for five years after a subscriber erases his/her account or unsubscribes from the mailing list.	All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the processor (EC). All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46, of 10 January 2017, on the security of communication and information systems in the European Commission. In order to protect personal data, the processor has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.
RAL-7	Subscriptions to external news service platforms	Directorate A	A.1 Services to members	European Committee of the Regions	N/A		N/A	Personal data are collected and processed in order to provide subscription for staff members to specific platforms for which the CoR is bearing the costs. These platforms offer (premium) news services through real-time news and data intelligence in the form of daily newsletters, articles, alerts and legislative data across the EU.	Staff members who may be interested in subscripting to specific platforms for which the CoR is bearing the costs.	The following personal data are processed: - Surname; - First name; - E-mail address, in order to provide them to the respective platforms for the subscription, that will be further processed pursuant to the specific privacy policy of the respective contractor (service provider).	Only authorised persons of the CoR Documentation Centre staff and the respective contractor.	The personal data are not transferred to non-EU Member States or to international organisations, except if the contractor is seated in a non-EU country or indicates so in their privacy statement to a non-EU country.	Personal data are kept for maximum 12 months after the end of the specific subscription.	N/A

RE2-18	EU Whoiswho	Directorate E	E.2 Recruitment and career	European Committee of the Regions	N/A	N/A	N/A	The data are processed for publication in the Whoiswho.	Members and management staff members.	For Members - Basic data (which will be shared publicly): • Title • Surname • First name • Represented country • Mandate/function as per Council decision • Telephone numbers(s) • Professional address • E-mail address(es) • Website(s), if available • Photo, if provided • National delegation at the CoR • Political group and commissions at the CoR • Membership of other CoR bodies For management staff members (Heads of units and above levels) - Basic data: • Job title • Surname • First name • Telephone numbers(s),	The data, indicated as basic data for each group, are sent to the OP (to be published in the EU Whoiswho), which is available in the following formats: online version, e-book and paper version. If available, photo will be published in the electronic EU Whoiswho. The postal address and e-mail address for correspondence are sent to the OP to be entered into the automated address and publications management system (SAGAP), in order to enable products of the European institutions to be distributed. For more details concerning the processing of personal data by the OP, the respective privacy statement of the OP can be consulted :	No, personal data will not be transferred to a non-EU Member State or international organisation.	For more details concerning the retention period of your personal data by the OP portal you can consult the respective privacy statement of the OP. In principle, OP portal of the Publications Office keeps your personal data for the time necessary to fulfil the purpose of the collection or further processing, namely for maintaining an up-to-date directory of EU staff in the EU Whoiswho. Concerning members, your personal data will appear as long as your mandate last at an EU institution. Concerning staff members, if you change your position within the EU services, this will be reflected after a short delay in the EU Whoiswho. If you leave the EU services, your personal data will disappear from the EU Whoiswho after a short delay. Concerning members, your personal data is archived in a public data base Concerning staff members, your personal data is archived in a non-public database, from which it will be deleted after 5 years for non-political important persons (PIP) (e.g. EU staff not in a management position).	
J001	Accreditation	21-09-18	L1 SECU	SECU - Directorate L secu@eesc.europa.eu	EESC and C	EESC-CoR JCA	Proxyclick	Security of buildings and staff and facilitating access to buildings by staff and visitors.eVisitors is a software, designed to automatize the invitation of visitors to the Committees and the registration of them when arriving.The new visitors management system aims to manage all processes related to the organisation of a visit to the Committee's premises. This will structure the process, give a smooth check in process, provide more security and correct information on number of visitors inside the building and increase the safety of visitors	Officials and other staff of the European institutions, CoR and EESC members, visitors, suppliers, external security guards.	- for the system users (staff encodoing visitors): name, surname, eesc mail address, office number - for VIP guests: last name, first name, role (minister, ambassador, etc.), vehicle registration number - for external participants: last name, first name, date of birth, nationality and identity card/passport number - for internal participants (other EU institutions): last name and first name.	The two Committees' internal security service, the security guard department, the organisers of events and activities and, subject to prior authorisation from the secretaries-general, the local or federal police and the national security service. All transfers and disclosures outside the Committees are documented and subject to a rigorous assessment of the need for such a transfer.	Not applicable	Initially the basic data are retained between the invitation that is send out and the registration at the entrance. Afterwards the data will be retained for 1 year following the registration at the entrance of the buildings (or can be retained longer, when it is asked for by law enforcement agencies or Member State's security services, as well as in the realm of internal investigations. This longer period is always motivated and duly documented.) The data are only available an accessible by duly mandated security officers for this purpose).	The database can only be accessed by means of an individual access code by a limited number of people working for the Committees' security services and those duly accredited.
J002	External service providers for	18-04-23	Directorate IIT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	N/A	Registration in the Human Resource Management systems of identity of external service providers and their time sheets.	Non-statutory staff, external service providers.	Name, sex, date of birth, type of contract, fiche or show photograph, internal addresses (telephone N°, office, email address, alias), type of contract, period of contract, function description, company, time sheets.	IT Project & Financial Managers	None	The data is kept for period of 10 years after the termination of the contract.	In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.
J003	Videosurveillance	19-09-18	L1 SECU	secu@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable	The Committees use their video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to EESC-CoR buildings and helps ensure the security of buildings, the safety of staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support EESC-CoR broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment or assets owned by the Committees, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault). The system is not used for any other purpose. For example, it is not used to monitor the work of employees or to monitor attendance. The Committees do not use covert surveillance.	EESC and CoR staff - EESC and CoR members - Visitors - External Security company - Any other person likely to enter the Committees' buildings - Demonstrators passing in front of the Committees' buildings	Video images digitally recorded. Due to the location of their buildings and in order to fulfil their security needs, Committees video-surveillance system might record images of protestors that might contain special categories of data, such as political opinions, religious or philosophical beliefs, trade union membership.	In-house security staff and outsourced security-guards. Recorded video is accessible to in-house security staff only. Live video is also accessible to security guards on duty. These security guards work for an external security company. Local police may be given access if needed to investigate or prosecute criminal offences. In the course of investigating crimes or offenses or in order to prosecute, images may be transmitted to the Belgian Federal or Local Police. Such requests for disclosure must be reasoned, submitted in writing to the Security Service and must comply with the formal and content requirements imposed by the national legislation in force. Whenever possible and independently of the obligations imposed at the national level, the Committees will request a judicial warrant, a written request signed by a sufficiently high ranked police officer or a similar formal request. The request should also specify, as accurately as possible, why the video surveillance sequence is required as well the exact place, date and time of the sequence requested. If the police or another national organisation of a Member State makes a request for access under an official procedure, it must first obtain a waiver of immunity if the sequence in question concerns a member of an Institution of the Union. Under exceptional circumstances, access may also be given to: - the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF; - the Commission's Investigation and Disciplinary Office ("IDOC") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or - those carrying out a formal internal investigation or disciplinary procedure within the	Not applicable	Footage is retained for a maximum of 30 days. Thereafter, all images are automatically erased by the system which overwrites on data older than 30 days. In case of security incidents, due to administrative procedures, it might take up to a month for judicial and/or police authorities to request recordings necessary for investigating security incidents. Some images may be stored longer if they are retained as part of an investigation or as evidence of a security incident. Their retention is rigorously documented and the need for retention is periodically reviewed. Images of demonstrators are retained for 48 hours only, due to the nature of data collected (special categories of data might be collected, such as political opinions, religious or philosophical beliefs, trade union membership). This period is necessary in order to identify whether security incidents have occurred (for example, damage to buildings).	Restricted access: recorded video is accessible to the Committees in-house security staff only. Live video is accessible to security guards on duty. Premises hosting the servers storing the footage are protected by physical security measures. Network firewalls protect the perimeter of the IT infrastructure. The main computer systems holding the data are security hardened. Administrative measures include the obligation of all outsourced personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared. All staff (external and internal) signed non-disclosure and confidentiality agreements. Access rights to users are granted only to those persons who need them in order to carry out their jobs. Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul access rights of any persons. The log-in and use of the system is traceable to a particular user.
J004	Ergonomics	28-09-18	L1 SECU	secu@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable	To take stock of the ergonomic status of workstations in order to remedy any shortcomings observed and to collect data in order to identify structural measures to be undertaken as part of efforts to ensure well-being at work.	The following are data subjects: officials, temporary and contract staff, agency staff, seconded national experts, EESC members and their alternates, CCMI delegates and their alternates, and staff made available to the EESC on the basis of service contracts.	Data that may be processed under this procedure, provided the data subject consents thereto, relates to: - last name, first name - gender - date of birth - internal address - function - seniority - working arrangements - type of furniture and IT installation - date of visit - degree of satisfaction of the person with their IT equipment, office - space and office furniture - type of work carried out - number of years of on-screen work and the number of hours spent daily in front of the screen - type of work performed (encoding, data consultation, etc.) - use of spectacles or lenses (type of lenses) - person's perceived state of health (general fatigue, stress, insomnia, headaches, other - to be specified) - pain experienced in the back, neck, shoulders, elbows, wrists, forearms, tingling sensation in fingers, legs - type of ergonomic surveillance specific content with third parties)	The data are accessible in a form permitting the data subject to be identified only by the persons responsible for ergonomics within the Directorate for Logistics. Where appropriate, if specific adjustments to the workstation are required by the state of health of the person concerned, the Medical Service of the institution will be informed in order to give an opinion on the proposed adjustments. Medical data are forwarded and processed only by the institution's Medical Service. An external contractor specialising in ergonomics may also be called upon to collect and access these data in order to advise the EESC on ergonomics. As regards data relating to the data subject's self-assessment of their state of health (back pain, neck pain, general fatigue, etc.), it is noted that, as with other data, these data are only collected if the person gives their consent. If special arrangements appear necessary as a result of the self-assessment, the person will be asked to contact the institution's Medical and Social Service in order to describe in more detail the problems encountered and to provide the relevant medical documents. These medical data will not be processed as part of the present data processing operation, but will be processed exclusively by the Medical and Social Service of the institution, which will make a recommendation as to the necessary adjustments.	Not applicable	Data enabling persons to be identified are kept only for the time necessary to identify and implement the correct actions in order to bring the workstation into line with the applicable ergonomic rules. The maximum period for retaining data is one year after the visit.	The office where the Security Service files are kept is locked whenever staff are out. The cupboards are also locked. Computer data are accessible only to Security Service staff and are secured by a password.
J005	E-mail management	18-04-23	Directorate IIT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable	To enable internal and external communication of Committees' staff and members. To offer to the Committees' e-mail system user the e-mail access to addresses of all internal correspondents and of main external partners (other institutions and bodies, external e-mail addresses of Members etc.).	EESC-COR Members & officials, officials etc. from other European institutions and bodies, subcontractors, European & world citizens. In this context any person as a potential e-mail sender/recipient is also a potential data subject.	GLOBAL ADDRESS BOOK EESC-COR Members & officials etc. Members & officials etc. from other European institutions and bodies E-mail message content (subject, body and attachments) E-mail message traffic information (sender, recipient, data, size) E-mail addresses and address book references Data fields for the e-mail messages: - message header (traffic information), - subject, - body and - attachments For the address book: - first name, - last name, - alias (user name for computer system) - committee - office number - phone number - unit - e-mail address - country, group & bureau (Members) For the address book of the other European institutions, the office number is not available. Users may constitute their own personal address book. This address book is not shared. This address book is not controlled by the DIIT. Log-files are used for solving technical problems and preparing anonymous statistics for	Message recipients: potentially anybody in the world having an e-mail address. Internal e-mail system users: Committee Members & staff. Address book (data fields as indicated in this notification): - Committee members & staff – e-mail services of other institutions – staff of other European institutions with whom bilateral agreements exist. Log-files: - administrators of the e-mail system (daily operations), - competent authorities in the context of investigations.	None	As long as the data subject is a Committee official/staff or member. As long as the data subject is present in the address book of the respective other institutions After deletion from the on-line address book, 6 months (maximum backup rotation time) E-mail messages: After deletion by the user, 6 months (maximum backup rotation time) Log-files: Maximum retention time 6 months (maximum backup rotation time)	In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.
J006	IT Incident handling	18-04-23	Directorate IIT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable	The purpose of processing is to assist EU institutions, bodies and agencies to detect, prevent and recover from cyber-attacks.	Individuals involved in IT security incident (perpetrator, victims or relays of a cyber-attacks), Individual owners of IT assets subject to specific vulnerability or infection, Individual owners of IT assets involved in malicious web or email traffic.	Security incident handling includes machine-based, automated processing of personal data, in particular for log management and correlation as well as network intrusion detection. Human intervention, in the form of security engineer or system administrator inspection or investigation, is far more limited. The information processed may contain personal data. The personal data that is collected is in connection with security incident handling tasks and operations. Below is an overview of these types of personal data: Any file (with user-id included) stored in, transmitted from / to a host involved in an incident (as victim, relay or perpetrator), Email addresses, User account name (for operating system, applications, centralised authentication services, etc.), Technical data (IP address, MAC address, etc.)	The IT Security Officer, IT security engineers and IT system administrators who may be called on to handle a security incident and who therefore need access to the technical details of the incident. Only the IT Security Officer and IT security engineers have access to the "CERT-EESC-CDR" functional mailbox. Information related to cyber-security incident might be transferred to CERT-EU in case of assistance request or simple notification.	Not applicable	Information and files used during incident handling are retained during the incident response procedure. The maximum duration of any retention for archival purposes will not exceed 2 years. This is for security reasons (e.g. an incident which seems initially benign may a posteriori be considered as the origin of a significant infection. The latter may be revealed several years after the original 'benign' incident).	In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.
J007	Telephony Management	18-04-23	Directorate IIT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable	To enable use of the telephone system at the EESC-COR. Measuring the capacity used and estimating the required capacity in the future, Follow-up on telephone charges for budgetary reasons and for cost-control. Billing of private telephone calls, Solving technical problems.	All staff, statutory or not, within the Committees and having a need for using the Committees' telephone system. All Members (including alternates, assistants & CCMI delegates and alternates) and having a need for using the Committees' telephone system.	The first set of data is composed of records known as "call data records". These records contain the number of the calling party (if available), the number of the called party, the date and time of the beginning and end of the communication, the cost of the communication (if it is an external call) and the number of the code if a service or private code was used to establish the communication. A second set of data is composed of the data provided by the telecommunications operators for the purposes of billing. This billing data contains the detailed list of calls with data similar to those contained in the call data records. A third group of data is composed of the data stored on the telephone set of the user. A fourth group of data is composed of that communicated by the internal user to the external world. A fifth group of data is composed of telephone directories containing all staff.	The persons responsible for recovery orders are informed of the amounts to be recovered from salaries in the case of private calls (i.e. only the amount to be recovered per user & no details of individual calls). The DIIT and its hierarchy for anonymous reports relating to the infrastructure. Competent persons working within the DIIT for ad-hoc reports relating to the telephone switchboard (e.g. follow-up of queries relating to usage of private or service codes or the use of service gsm's). The COR administration for reporting related to the COR gsm regulation. The EESC administration for reporting related to the EESC gsm regulation.	Not applicable	The data stored in electronic format (in the "call data records") are retained for a maximum period of 6 months.The data obtained from the telecommunications operators and used as the basis for billing are kept for the same duration as the financial files. Global bills (no personal data) from the operators are included in the financial files. The financial files for fixed telephony contain no information permitting direct identification of the data subject. The financial files for the use of service gsm's contains no information permitting direct identification of the data subject. The financial files relating to the recovery of private use of the service gsm contains a list of all dialled numbers and data related to roaming (if any). Anonymous data is kept indefinitely	In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.

J008	User Account Management	18-04-23	Directorate I/IT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable.	User account management for the IT system of the European Economic and Social Committee and the Committee of the Regions (EESC-COR) to enable day-to-day operation of the IT System at the EESC-COR.	All Staff, Statutory or not, within the Committees and having a need for using the Commitees' IT System. All Members (including Alternates, Assistants, CCMI Delegates and alternates & their collaborators) and having a need for using the Commitees' IT System	BASIC DATA NEEDED TO CREATE A USER ACCOUNT: - Name - Alias (User-name for computer system) - Committee - Office number - Phone number - Unit - E-mail address - Country, Group, Bureau (y/n) for Committee Members - Expiry Date (e.g. end of contract, end of mandate) PASSWORDS: The application to create user accounts sets an initial random password. Users have to change it the first time they logon to the network. After that, the DIIT does not know the password of the users. The DIIT, may on request of the user, reset their password. Users must change their password regularly. LOG-FILES: Log-files are used for solving technical problems and for preparing anonymous statistics for trend analysis. The maximum retention time is 6 months. "LAST LOGON" A last "logon report" is generated on demand. This information is used to identify unused accounts. Unused accounts may be suspended or deleted. HELPDESK APPLICATION The Helpdesk register information about technical incidents and problems in a database application. This information is used for problem solving and trend analysis. PRINTING Multifunctional Devices (MFDs) are available which can be used for Printing, Copying and Scanning. Follow-me and secure Printing works as follows:	- Services of other Institutions – Information necessary to establish an e-mail directory – Staff of other European Institutions with whom bilateral agreements exist - Administrators of the IT system (technical problem solving and preparation of anonymous statistics), - Competant authorities (on request in the context of an investigation).	None	ONLINE INFORMATION: Time during which the account is active LOG-FILES: Maximum retention time of 6 months (except Security data)	In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.
J009	Office occupancy list	15-11-18	L2 INFRA	Head of Infrastructure's Unit (_InfrastructuresSC@eesc.europa.eu)	EESC and C	EESC-CoR JCA	Not applicable	The list is a dynamic database, containing information regarding the occupation of every office within the Committees' buildings. When the end date of contract is known (such as for trainees or contract agents) it is also included in the list, so that future office moves could be planned. The list is updated manually, immediately after receipt of a request.. The modifications of the list are done based on the approved move forms and on official communications regarding staff moves from the Committees' HR services. The database is necessary in order to know the Committees' buildings' occupation in real time.	All staff members hosted in the committees' buildings, as well a limited number of external agents.	First name, family name, Committee, office number, Unit, end of the date of the contract when communicated by HR, temporary absence, end of service date.	IT and HR services, and also the mailing services, as a part of the internal services.	No transfers to a third country or international organisation	Data are kept for as long as the office in question is occupied by the staff member, the Committees' member, the trainee or the external agent.	n/a
J010	Inventory	15-11-18	L2 INFRA	Infrastructure Unit — Directorate for Logistics (docinventaire@local)	EESC and C	EESC-CoR JCA	Not applicable	In accordance with the rules laying down the provisions of the Economic and Social Committee and the Committee of the Regions, conditions relating to the preservation of all 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 ASSETS 2 is the computerised system for managing the inventory of the Committees' assets. It includes all information relating to each item: inventory number, description, nomenclature code, department responsible, value of the item, delivery date, location, etc., as well as all the data required from an accounting perspective. It gives the option of indicating the name of the person professionally responsible for the item. This possibility is used in less than 1% of cases for items for personal use (such as medical furniture), but is essential for managing the inventory. Processing is necessary for the management and monitoring of all assets.	All staff occupying the Committees' buildings.	- User ID - surname - first name - office number - Committee.	Only the CIS of the Infrastructure Unit, the verification services, the internal audit service and the accounting officers have access to all ABAC ASSETS data. The CRA, IT and Security and the managers of units purchasing goods have access to the data of their department only. Access is requested from the CIS by the head of unit and is forwarded to the Local Profile Manager (LPM) of the corresponding Committee, which will request DIGIT support.	Not appplicable	The basic data are stored for the lifetime of the equipment in the inventory. Once the goods have been "written-off" or decommissioned, typically after a period of four to five years, the records on them are retained but users/assignees names are no longer accessible except under specific circumstances/conditions. (Historical information can only become accessible again after the re-activation of an item that was written off via administrative procedure - e.g. when a lost item which has been written off is found). Work is being considered to see if it is realistic to amend the system further to completely anonymise the retained data.	Access to the database is limited: only authorised persons have access to data relating to their department.
J011	Interinstitutional exchanges -	28-11-18	T1 TMU	dt-strategy@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable	Organising the selection of applicants and management of interinstitutional exchanges of staff of the horizontal and language services	Linguists/Translators, Translation assistants	The following data will be collected and processed: In the application: name, date of birth, current grade, home institution and unit, date of entry into service and starting grade, desired host institution in order of priority, knowledge of languages, training, professional experience, any specialisations, working arrangement (full time, part time), signature. In the assessment report drawn up by the head of the host unit (drafted only on the request of the participant): name, period concerned, employment-related data, name of head of host unit, main activities, assessment by head of host unit, signature. In the questionnaire completed by the applicant to evaluate the exchange (optional): name, home institution, host department/unit, personal opinion on various aspects of the exchange, signatures. In the CV: any data that the applicant chooses to provide in the CV (there is no set CV format).	- Those persons responsible for managing interinstitutional exchanges within the Translation Directorate (notably the heads of unit concerned and the coordinator in TMU). The horizontal or language units and services seeking or requested by applicants. - Depending on the post involved in the exchange, the data may be provided to the human resources managers of the translation or horizontal services of the European Economic and Social Committee (EESC), the European Committee of the Regions (CoR), the European Commission and the European Central Bank, which will be able to grant access to the heads of unit of their Directorate-General for the purposes of selection and reports. - The necessary administrative data regarding successful applicants will be provided to the other relevant services of the EESC and CoR.	No such transfer is taking place.	The data will be stored for 12 months dating from the end of the exchange. At the end of this period, the data will either be deleted or made anonymous, so that they can be processed for historical or statistical purposes. For the applicants who were finally not seconded to other institutions the retention period is 12 months after the reception of the request in order to consider their application for the next exchange period.	Electronic files including application forms, CVs and reports are stored in the functional mailbox of DT Strategy (limited access); on a password protected USB, stored in a lockes cupboard in the office of the file manager responsible for the exchanges. Paper files are stored in a locked cupboard in the office of the file manager responsible for the exchanges.
J012	Catering service	02-06-19	L2 INFRA	Head of the Infrastructure Unit — Directorate for Logistics — Joint Services — Catering Service Email: restaurant-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	BaxterStore y	Processing is necessary in order to follow up requests and ensure quality of service in accordance with the remit of the Catering Service and the terms of the catering contract between the Committees and BaxterStorey.	All staff and users of catering who have sent a complaint to the Catering Service and/or BaxterStorey.	The database includes the following contact details: Surname, first name and e-mail address as well as a description of the complaint.	Catering service	Not applicable	The storage period is one year. After this period, the information included will be kept and made anonymous for the purpose of redundancy analysis of service problems over longer periods.	The database is located on a secure server belonging to the Committees in Brussels.
J013	EMAS service	28-06-19	L2 INFRA	Infrastructure unit – Logistics Directorate – Joint Services – EMAS. environment@eesc.europa.eu or environment@cor.europa.eu	EESC and C	EESC-CoR JCA	N/A	Processing is necessary to follow up requests and ensure good quality service in line with the mission and objectives of the environmental management system. Any staff member of the Committees can contact the EMAS Service to report a problem related to environmental management or to obtain information and advice.	Any staff member and user who has sent a request to the EMAS Service.	The database includes the following information: Surname, name, e-mail address and description of the request.	EMAS Service	Not applicable	The retention period is one year. After this period, the information retained will be kept and anonymised for the purpose of analysing the redundancy of service problems over longer periods.	The database (an excel table) is located on a secure server belonging to the Committees in Brussels.
J014	Events organised by EMAS	28-06-19	L2 INFRA	Infrastructure unit – Logistics Directorate – Joint Services – EMAS (environment@eesc.europa.eu) or (environment@cor.europa.eu)	EESC and C	EESC-CoR JCA	Not applicable	The data collected are necessary for the organisation, management and follow-up of the event. They are also necessary to ensure the success of the event and to inform staff about the actions taken.	Staff members, external guests.	The database includes the following the elements: pictures, videos, names and surnames of people participating in actions/conferences, quotes from participants (staff members) in newsletters or posters. If need be, the files containing the photos can be slightly altered, so that they can be used for the purposes for which the materials were made.	Access is restricted to EMAS staff. Some photos of speakers and participants could be published on the intranet as part of an event.	Data will not be transfer to a third country or an international organisation.	The retention period is 10 years. After this period, the retained photos will be deleted from the EMAS server.	Data are stored on the Committees' servers. Access is limited to EMAS staff and operators.
J015	Management of call for tende	27-10-23	Directorate L	DL - Joint Services EESC-CoR HEAD OF UNIT - PRINTSHOP/DISTRIBUTION AUTHORISING OFFICER BY SUB-DELEGATION RUE BELLIARD 99 - OFFICE BVS 0141 B-1040 BRUSSELS - BELGIUM tenders-printshop@eesc.europa.eu DL - Joint Services EESC-CoR HEAD OF UNIT - INFRA AUTHORISING OFFICER BY SUB-DELEGATION RUE BELLIARD 99 - OFFICE BVS 1132 B-1040 BRUSSELS - BELGIUM patrick.deschryver@cor.europa.eu DL - Joint Services EESC-CoR HEAD OF UNIT - SECU AUTHORISING OFFICER BY SUB-DELEGATION RUE BELLIARD 99 - OFFICE BVS 1132 B-1040 BRUSSELS - BELGIUM	EESC and C	EESC-CoR JCA	N/A	Management and administration of procurement procedures	All persons associated with the third parties whose details are included in submitted tenders and in contracts.	Personal data collected and further processed concern the tenderer and its staff or subcontractors (natural persons). Information can relate to the following data: • name; • function; • contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, company and department, country of residence, internet address); • certificates for social security contributions and taxes paid, extract from judicial records; • bank account details (IBAN and BIC codes), VAT number, passport number, ID number; • information for the evaluation of selection criteria: expertise, technical skills and languages, educational background, professional experience, including details on current and past employment; declaration on honour of not being in one of the exclusion situations referred to in the Financial Regulation.	For the purposes detailed above, access to your personal data is given or may be given to the following people: • EESC staff responsible for the management of the procurement procedure and tender evaluation (and/or the equivalent staff in other EU institutions in the case of an inter-institutional call for tenders); • people and bodies with monitoring or inspection responsibilities in the application of Union law (e.g. internal audits, Financial Irregularities Panel, European Anti-fraud Office – OLAF, Court of Auditors, EESC Data Protection Officer, European Data Protection Supervisor); • the EESC legal service and the competent jurisdiction, in the event of an appeal; • members of the public: in the event that you are awarded a contract by the EESC, part of your personal data will be made public, in accordance with the EESC's obligation to publish information on the outcome of procurement procedures deriving from the budget of the European Union. The information will concern, in particular, your name and address, the amount awarded and the name of the project or programme for which you are awarded a contract. It will be published in supplement S of the Official Journal of the European Union and/or on the EESC website for procurement above EUR 15 000.	Not applicable	Personal data are kept as follows: • Files relating to tender procedures, including personal data, are to be retained in the department in charge of the procedure until it is finalised, and in the archives for a period of at least five years following the date on which the European Parliament gives discharge for the financial year of the last payment (see Article 75 of the Financial Regulation). • Until the end of a possible audit, administrative or judicial procedure, if one such procedure started before the end of the above period.	Information is held in locked archives managed by the controller of the unit concerned (IMP, INFRA or SECU) or by his subordinates. Access is possible to others only by written request. Copies may be held by the financial managing officer of the operating service responsible for the execution of the contract, under the responsibility of his/her financial authorising officer and Head of unit.
J016	Directorate for translation - st	05-10-20	Directorate T	Deputy Director of Directorate T, dt-management@eesc.europa.eu	EESC and C	EESC-CoR JCA	None	Performance statistics.	Staff working as translators in the Translation Directorate.	Name, surname, staff catеory, number of pages translated.	DT Management (Heads of Unit, Language coordinators, individual staff members (they only get their own data))	Not applicable	5 years.	Access to report is restricted to Heads of Unit and Language Coordinators
J017	Multifactor Authentication usi	18-04-23	Directorate I/IT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	Microsoft Ireland.	Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their mobile phone. By requiring a second form of authentication, security is increased as this additional factor isn't something that's easy for an attacker to obtain or duplicate. Multifactor authentication is enabled for webmail and Terminal Services Gateway (TSG).	EESC-COR Members & officials.	Overall, the personal data handled by Multifactor Authentication consists of directory entries: -Name -Alias (User-name for computer system) -Committee -Office number -Phone number -Unit -E-mail address -Country, Group, Bureau (y/n) for Committee Members -Second factor Information for the second factor is mandatory to use the service. While the second factor isn't necessarily based on the phone number as provided by Sysper/Agora for staff and members respectively, these numbers, if present, are used to pre-populate the corresponding field in the second factor setup. Users can change it to another phone number or move to an authentication method not using phone numbers at all.	Access to your personal data is provided to the EESC-COR staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law. For services related to Multifactor Authentication, Microsoft acts as data processor. Contact details: Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.	None	Time during which the user account is active.	All personal data in electronic format are stored on the servers of the EESC-COR and its contractors based on its service. The EESC-COR actively configures customer data location (at rest) of the service. The service is offered from data centres in EU Member States, respectively Ireland or the Netherlands. No content data will be stored outside the EU territory. Push notifications are an exception. Any log files generated by using Multifactor Authentication Services can be analysed in the US, and while EESC-COR cannot technically avoid this, strong contractual safeguards apply to this data. Any data in transit is protected by strong encryption. In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.
J018	DL Intranet Revamp Project (	29-10-20	Directorate L	DL Intranet Revamp Project Group - mgmt-logistique-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	N/A	The EESC and COR have four Intranets: EESC Intranet, MYCOR, DT Intranet and DL Intranet. The first three have been redesigned/renewed over the last 5 years. However, the DL Intranet has not changed substantially for the last 10 years. It is outdated in terms of content and style. There is a clearly a need for an updated version, aligned with the structure of the three other Intranets. It is also the aim to improve it so as it becomes a more user-friendly intranet that puts the users first. In order to reach the above-mentioned objective, it has been decided to organize and launch a general survey (see annex) for Staff, which is anonymous, with the only exception of question 11 stating as follows:"If you wish to participate to improve the DL intranet, please leave your name and contact details here"	Staff members that confirm their wish to participate to improve the DL intranet.	Personal data collected and further processed concern the name(s) and the contact detail(s) of the Staff members wishing to participate to improve the DL Intranet, in accordance with their reply to question 11 of the Survey.	For the purpose detailed above, access to the personal data collected and further processed is or may be given to the EESC & CoR staff responsible of DL Intranet Revamp Project Group.	No transfer(s) of personal data to a third country or an international organisation is foreseen in the execution of the projet.	Personal data will be kept until the date of the complete execution of the project, planned for the 31/12/2021.	The processing operation will done manually and/or by electronic means by the EESC & CoR staff responsible of DL Intranet Revamp Project Group.

J019	Microsoft 365	18-04-23	Directorate IIT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	Microsoft Ireland.	The DIT is operating the future collaboration platform of the Commitee which is based on the cloud-based solution "Microsoft 365" provided by Microsoft. This enables the members and staff of the Committee to work on any corporate or in certain cases on private devices and facilitates collaboration with internal and external stakeholders. The licence agreement for using Microsoft 365 covers the following applications: - Teams - SharePoint Online - OneDrive for Business - Office Online apps (Word, Excel, PowerPoint, OneNote) - Outlook with Exchange Online There are other applications which are included in the license which are not used.	- ESC-COR Members & Staff - External to the organisation - All collaborators are granted access to use the Microsoft 365 platform as guests with limited rights.	The Microsoft 365 platform distinguishes between the following data categories: - Identification data - Content data - Service generated data - Diagnostic data 1) Identification data contains personal data necessary for the proper identification of the user and the corresponding user account, including exhaustively: - Username, Email address and account status - User personal data (last name, first name) - Function-related data (Unit, Telephone numbers) This information is copied to all Microsoft 365 data centres around the globe used to provide the service that allows global access and access control to the Committee's environment in Microsoft 365. 2) Content data includes any content uploaded to the Microsoft 365 platform by its users, such as documents, and multimedia (e.g. video recordings). Such data is stored by the user in Microsoft 365 but not otherwise processed by the service 3) Diagnostic data (also known as telemetry data) is related to the data subjects' usage of office client software. The DIT has applied technical measures to disable sharing of diagnostic data with external parties, including Microsoft. 4) Service generated data contains information related to the data subjects' usage of online services, most notably the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activity in Microsoft 365. Event data like account logins will allow to monitor all activity in the cloud environment of each user. Any of these categories may contain personal data. The operation of this platform requires the processing of data categories by Microsoft, for the following specific purposes:	Within the EESC-COR: DIT, Microsoft 365 administrators DIT, Security Team members DIT Microsoft 365 administrators and IT Security Team members can view identification data, diagnostic data and service generated data. They can access identification data, diagnostic data and service generated data in view of investigating issues for a specific user. For the most part they access aggregated data without any mention of personal data. Outside the EESC-COR: Microsoft's personnel managing the databases on Microsoft cloud servers and their sub-processors' personnel on a need-to-know basis. A list of sub-processors that has been agreed upon. Microsoft commits to have in place written agreements with all sub-processors that are at least as restrictive in terms of data protection and security as their data processing agreement with the Committees. The activities of all sub-processors are in scope of third-party audits. Microsoft's personnel may access service generated data on a need-to-know basis. Microsoft's sub processors that provide services to Microsoft may access service generated data on a need-to-know basis.	Data is transferred to countries outside the EU or EEA. If users access the Microsoft 365 service from outside the EU/EEA, personal data may be transferred to a corresponding location in order to provide the service. To enable the global service provisioning of Microsoft 365, Microsoft copies identification data to all Microsoft 365 data centres around the globe used to provide the service. This copied identification data remains under the control of Microsoft and is used to verify the user authentication details and grant access to Microsoft 365 resources of the Committee. Service generated data is not necessarily processed outside of the EU. Microsoft is authorised to transfer it to Microsoft Corp., located in the USA, and the network of sub-processors. This type of data contains information on the usage of the service. The data is aggregated before being transferred but may contain identifiable information Data is transferred to international organisation(s) - No	1. Data category Identification Data - Identification data is stored for as long as the user account is active 2. Data category Service generated data (log files) - Up to six months 3. Data category Content data in Microsoft 365 and any personal data included therein - Up to 180 days upon expiration/termination of the subscription 4. Data category Diagnostic data - Up to five years	There are appropriate measures in place to restore access and availability to personal data in a timely manner in the event of a physical or technical incident. Access Control: Azure Multifactor Authentication (MFA) will act as the primary authentication solution, linking access to the cloud environment and to on premise authentication. Azure MFA supports Multi Factor Authentication (MFA), allowing several options such as phone calls or use of Mobile App (Microsoft Authenticator) In terms of confidentiality, Data Loss Prevention (DLP) rules can be created at the Office365 Security & Compliance Center. With the Customer Lockbox feature of Microsoft 365, the DIIT controls how and when Microsoft engineers may access the data to give support. Microsoft's Microsoft 365 solutions provide the administrator with the ability to audit user interaction with Microsoft 365 systems, safeguarding the ability of the DIIT's incident response team to investigate personal data breaches and security incidents. The functionalities also include access of the administrator to third-party ISO, SOC, and other audit reports, as well as Audited Controls, which provides details about the various controls that have been tested and verified by third-party auditors of Microsoft 365. Log Analytics is a key service Microsoft provides to grant administrators a detailed view of the infrastructure of the
J020	Background checks for contri	25-01-22	L1 SECU	Security Service, Directorate L, Joint Services (secu@eesc.europa.eu).	EESC and C	EESC-CoR JCA	N/A	The Security service collects and uses your personal information to make an informed decision on whether to grant access to the Committee's premises. Belgian authorities and EU Institutions and Bodies (European Commission, European Parliament, European Council, Council of the European Union, European External Action Service, European Economic and Social Committee, Committee of the Regions, European Defense Agency) ('EUI') have signed in May 2019 a Memorandum of Understanding for the implementation of Security Verification's of external contractors. The verification is at the request of European Institutions and Bodies and will result in either a positive or negative security advice for each individual assessed, granted by the Belgian National Security Authority. Any employee of an external contractor who will be subject to a security verification will give his permission to initiate the security verification necessary to obtain a security advice. If the employee of the external contractor refuses to be subjected to a security verification, s/he may express her/his refusal by indicating it on the consent form and sending it, by registered mail. The firm will electronically transmit in an Excel sheet the following data of the person(s) involved: last name, first name, function or profession, nationality, Belgian national number, ID or passport number, date and place of birth, address, company and company ID number.	External contractors staff.	In order to carry out this processing operation the Security Service collects the following categories of personal data: •Last name and first name; •Address; •Function or profession; •Nationality; •Date and place of birth; •Nationality; •Belgian national number, •ID or passport number; •Date and place of birth, •Company and company ID number; The provision of personal data is mandatory to meet the contractual requirement on services provided on the premises of the Committees. If the personal data are not provided, possible consequences are refusal of access rights to Committees buildings.	Access to the personal data is provided by the consent form filled in to the Committees staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. The consent form is sent to the Belgian Ministry of Foreign Affairs, who will then have access to the personal data. The information we collect will not be given to any third party, except to the extent and for the purpose that we may be required to do so by law. However, when a negative security advice is received, the Committees will inform about it the other institutions and bodies participating in the MoU.	Data will not be transfered to a third country or international organisation	The Security service only keeps the personal data for the time necessary to fulfil the purpose of collection or further processing, namely for five years from obtaining the security advice, which constitutes the latter's maximum validity period	In order to protect your personal data, the EESC/CoR has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the EESC. Decision 2/2018A on information security policy of the EESC and of the CoR, adopted on 4/6/2019, provides for security measures for the protection of both Committees' information systems and the information processed therein against threats to the availability, integrity and confidentiality of these systems and information. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.
J021	Management of Dir. T office i	21-02-22	T1 TMU	Translation Management Unit - Directorate for translation head-of-unit-tmu@eesc.europa.eu	EESC and C	EESC-CoR JCA	Not applicable	Data are processed in order to know the DT office occupation in real time. The DT office occupancy list is a database, containing information regarding the occupation of every office used by the DT. Any announcement of arrival or departure is also included in the list to facilitate future office moves. The list is updated manually.	All DT staff members (whatever status) and future staff (external recruitment or internal move).	Name, first name, office and phone number, unit, role, temporary absence and start or end of service/contract date.	These persons responsible for managing office moves within the Directorate for Translation (notably the heads of unit concerned and the coordinator in TMU under the supervision of the Director).	There is no transfer of personal data to third countries or international organisations.	Data are kept for as long as the office in question is occupied by the DT staff member (whatever status).	
J022	Migration of Email archives to	19-05-22	Directorate IIT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA	Cloudficient Solutions GmbH	Data (emails) will be transferred from the current on-premise Exchange backend to Exchange Online, part of Microsoft 365. This includes archived emails in the Enterprise Vault, as well as any contents in users' live mailboxes. Cloudficient makes the migration efficient and manageable.	EESC-COR Members & Staff	- Email addresses - Email messages - Archived email messages	Access to your personal data is provided to the EESC-COR staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law. The subprocessor does not access or store the data.	No direct transfer outside the EU. The controllers and processors have agreed to Standard Contractual Clauses. The location of the processing is fixed in these standard contractual clauses as a location inside the EEA. The contract stipulates the processor is using a third party ISO27001 datacenter provider based in Germany. This provider will house the databases where the limited metadata for the data subjects is stored. This datacenter provider will have no access to this metadata.	Cloudficient will only store metadata needed to perform the migration. These metadata are used for the sole purpose of orchestrating the migration. They are stored on a temporary basis and removed after the migration process, i.e. when the project closes. The tenant and metadata are decommissioned thereafter.	While the Cloudficient solution facilitates the transfer of email data from the Committees on-premise infrastructure to the Committees Microsoft 365 tenant, e-mail data does not leave the Committees security boundaries. These data are not stored. Cloudficient does not have access to any e-mail content. Content is sent directly from Enterprise Vault to the staging cache of Microsoft 365. Data in transit are encrypted using TLS 1.2 (standard
J023	Audit and mapping of Human	12-01-23	Directorate E	EESC Dir A RMP - coord-HR-mapping@eesc.europa.eu CoR Director for HR - Agnieszka.Kudlinska@cor.europa.eu	EESC and C	EESC-COR JCA	The processor has been selected by FWC No BUDG/19/PO/01 and is: BDO LLP	Audit and mapping of human resources against the workload of activities, in particular legal and administrative obligations for the implementation of the specific contract PF AUDIT/2022/PO/R/01, based on Framework contract No BUDG/19/PO/01 "Supply of technical assistance services in the field of audits and controls".	All staff (officials and other agents) of the EESC and Joint Services.	The personal data are processed by four different processing methods: • Staff survey using EU Survey (on a voluntary basis) - Entity of employment (directorate, unit, service, etc.) - Work contract details (duration) - Entry into service (at the EESC) • Gathering of detailed data on workload, activities and ways of working using Excel files (job profiling): - Entity of employment (directorate, unit, service, etc.) - Category - Working time related information - Job description and tasks • Staff focus groups (concerning a representative sub-set of staff from each directorate/entity): - Entity of employment (directorate, unit, service, etc.) - Category, job title - Information from meetings • Staff interviews (concerning staff with management responsibilities): - Name, gender, age - Entity of employment (directorate, unit, service, etc.) - Category, job title - Work contract details (type, duration, entry into service, etc) - Working time related information - Job description and tasks - Information from meetings - Career related information	Only the processor is the recipient of the personal data, who will provide an anonymous report and recommendations to the competent management of the EESC, which, insofar as finding and recommendations concern the joint services, will forward this information to the competent management of the CoR. The processor is: BDO LLP 55 Baker Street London W1U 7EU UNITED KINGDOM email: budget3@bdo.co.uk	Yes, to the United Kingdom. The European Commission, by its implementing decision 2021/1772 of 28 June 2021, recognised the United Kingdom under the GDPR and the LED, as providing an adequate level of data protection.	The processor shall only keep personal data for as long as necessary for the purposes for which they were collected. You can also find the privacy statement of the processor at the following address: https://www.bdo.co.uk/en-gb/privacy-statement/individuals-connected-to-our-clients	A restricted Sharepoint site has been set up to store documents containing the data with restricted access to EESC Directors, contact points, the RMP sector and the audit team at BDO LLP. Within the Sharepoint site an even more restricted folder has been set up for temporary storage of sensitive data. Where it is possible, BDO PLL is liaising with the staff member directly to gather information or arrange meetings.
J025	Management of book loans a	28-09-23	Directorate D	EESC Information Centre, Information Centre and Document Management Sector (ICD), Directorate D – Communication and Interinstitutional Relations biblio@eesc.europa.eu CoR Documentation Centre, Directorate A, unit A1 Services to members, documentation@cor.europa.eu	EESC and C	EESC-CoR JCA	Provider of the ALMA database: Ex Libris (Germany) Official legal form: GmbH	Personal data are used to provide access to the services offered by the Information/Documentation Centre: book loans, access to electronic content, book renewals and reminders, book borrowing via the inter-library loan system, responses to various document research requests.	The personal data relate to EESC and CoR staff and members.	We collect the following personal information: surname, first name, email address, material borrowed or consulted. On an optional basis (based on consent) the Centre may collect office and telephone numbers (professional or personal).	Only authorised staff: EESC Information Centre staff, CoR Documentation Centre staff and the contractor Ex Libris, producer of the ALMA database.	We do not intend to transfer any data to third countries or international organisations.	Staff members' data will be retained throughout their career at the EESC/CoR, and those of Committee members during their term of office, plus an additional 24 months for statistical purposes.	Access to the ALMA database is secured by a username and password (authorised staff and administrators: only EESC Information Centre staff and CoR Documentation Centre staff).
J024	Online and hybrid events orgi	05-10-23	Multiple services	Functional mailbox addresses of the relevant responsible services: mgmt-IIT-sc@eesc.europa.eu secu@eesc.europa.eu mgmt-logistique-sc@eesc.europa.eu dtmanagement@eesc.europa.eu environment@eesc.europa.eu restaurant-sc@eesc.europa.eu	EESC and C	EESC-COR JCA	European Commission , in case the registration to the event is made via EU-Learn	We collect and process your personal data to produce a video and/or audio recording of staff meetings, information sessions and trainings organised by the EESC-CoR Joint Services. Such meetings may take place online, in a hybrid format or in-person. The purpose of the recordings is to enable staff who were not able to participate in the event to follow the session at a later stage, and to generate cost and time efficiency savings for the institution by reducing the need to repeat sessions as well as to retain knowledge.	Speakers and participants to the event	We will collect only the following personal data from the event participants necessary for the processing operation: - Name and surname - Images of (certain) participants during the event (where consent is given to be filmed in case of face-to-face events or when the participant chooses to switch on the camera during online/hybrid meetings), and audio recording of participants who speak during the event. Images of participants who are present in the physical meeting/conference room might also be recorded. - Information that participants choose to share in the written chat function during the event Depending on the online event tool used to hold the meeting, the following personal data might also be processed: - IP address - Cookies - Connection data - Email address Please refer to the data protection notice of EU-Learn in case the registration to the event is made using EU-Learn.	Any person who has access to the CoR and EESC intranet	No	The recordings will be kept for maximum 10 years	Only persons who have access to the EESC and CoR intranet have access to the recordings. In case of registration via EU-Learn, the personal data submitted for the registration are subject to the security measures used by EU-Learn and described in the European Commission's Learning Management System (EU-Learn)(DPR-EC-00967) and in the European Commission's Identity and Access Management Service (IAMS)(DPR-EC-03187).
J026	E-mail Address Book Manag	05-01-24	Directorate IIT	mgmt-IIT-sc@eesc.europa.eu	EESC and C	EESC-CoR JCA		The SECABC platform, developed, operated and administered by DIGIT, enables the European Insitutions to securely share their address book data and the secure email certificates. The roles and responsibilities of all European Institutions that are connected to the SECABC platform are set out in a "Master Data Processing Agreement" which has been signed by the EESC and the CoR.	EESC-CoR members & officials, officials etc. from other European institutions, subcontractors.	For exchanging or storing the address book and email certificates: name, surname, email address, business phone number, gender code, location, department, Institution.	Personal data is only transmitted to other participating European Institutions through the SECABC platform. Such transmissions take place in compliance with the agreed purposes of processing.	None	Personal data will be stored for as long as the EESC and COR are parties to the "Master Data Processing Agreement". Every time a new address book file is uploaded, the existing data of is overwritten by this new data and no copy of the old data is retained. This means that the EESC-COR can decide on the personal data processed and included in these files. In case of termination of the agreement, all personal data will be deleted within one month.	In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.
J027	EESC-CoR EU Open Doors I	17-04-24	Multiple services	Head of the Visits and Publications Unit, Directorate D – Communication and Interinstitutional Relations, European Economic and Social committee, Rue Belliard 99-101, 1040 Brussels openday@eesc.europa.eu Head of the D2 Events and local dialogues unit, Directorate D – Communication, European Committee of the Regions, Rue Belliard 99-101, 1040 Brussels, openday@cor.europa.eu	EESC and C	EESC-CoR JCA	Contracted Service providers CREASET Pracsis GOPA.CO M	Data is used: for the organisation and management of the event for accreditation purposes for communication and publicity purposes for financial purposes	EESC & CoR staff EESC & CoR Members Visitors Service providers contracted for the organisation and/or delivery of the event	The following personal data may be processed in the context of the EU Open Day 2024 at the EESC and CoR in Brussels: i) General public (visitors) - Photos and/or videos of identifiable persons or groups being taken by CoR and EESC communication department. - Photo Booth data: Pictures and email addresses are entered into the booth by visitors during the Open Day if visitors would like to have the photos emailed to them. They are under no obligation to enter these details and the photo booth does not retain nor transfer the email addresses Recordings: Photos and/or videos and/or audio recordings of identifiable persons or groups. Special lanyards are available at the information desk in JDE reception hall so identify visitors who prefer not to be photographed or filmed by the EESC or CoR. Notices will be posted in JDE reception as well as around the building to inform visitors of these lanyards. ii) Service providers (legal person): - Organisation Name - Country Represented - Email Address - Website - Phone Number - Street, Number, P.O. Box - Postal Code - City, Town, Area - Country - Key contacts from the organisation iii) Service provider contacts (natural person): - Last Name	The respective organising teams within Units D2 in the EESC and the CoR; Security and accreditation colleagues	No transfers will take place	Accreditation Data obtained for these purposes are transferred to the Security service and then deleted by the organising teams in units D2 in both the EESC and CoR. The Security service retains data for one year, according to the record on accreditation (J001) and to the related data protection notice •Pictures and videos that are going to be used as communication material will be kept for a period of 30 years in accordance with EESC Decision No. 206/17 A and CoR Decision No 15/2018); •Pictures and videos that are not going to be used as communication material will be kept for 12 months after the event. •Data of staff and members necessary for the organisation and management of Open Day will be kept for 12 months after the event. •Data of contractors are to be retained in the department in charge of the procedure until it is finalised, and in the archives for a period of at least five years following the date on which the European Parliament gives discharge for the financial year of the last payment (see Article 75 of the Financial Regulation), or, as the case may be, until the end of a possible audit, administrative or judicial procedure, if one such procedure started before the end of the above period.	Personal data collected by the EESC are stored on the EESC's servers. Personal data collected by the CoR are stored on the CoR's servers. The access to all personal data as well as all information collected in the context of the meeting/event is only available to a defined population of users, namely the respective organising teams within units D2 in the EESC and the CoR. Contractors used in the framework of the "Open Day" event will take some pictures. Pictures will be published on the intranet and EESC internet web pages. Processors are obliged to respect the data protection clauses of the contract.

J028	Transmission of personal dat	22-04-24	Directorate I/IT	niall.ohiggins@eesc.europa.eu	EESC and C	EESC-COR JCA	European Commission and its contractor ServiceNow	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 DIT (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 restore access and availability to personal data in a timely manner in the event of a physical or technical incident. A well-defined information security policy is in place and is regularly reviewed for improvements; The team from EC regularly undertakes training and awareness programs for staff, as well as audits and reviews of data protection policies and procedures.