European Committee of the Regions

Record of processing activity – Working document

Personal files

PART 1 - Record	
1. General Information	
Reference number	RE2-4
Last update	30/09/2024
Controller	European Committee of the Regions
Directorate	Directorate E
Unit	E.2 Recruitment and career
Contact details	dossierindividuelCdR@cor.europa.eu
Joint controller	N/A
Joint controllership arrangement	Available internally
DPO contact details	data.protection@cor.europa.eu
Processor(s)	The CoR uses the NDP IT platform provided by DG HR of the European Commission, the provision and support of which is ensured by DG DIGIT of the European Commission, as a processor on behalf of the controller (CoR), under a Memorandum of Understanding. The security measures are the same as for European Commission data. Access rights are controlled by the controller at the European Committee of the Regions.
Data processing agreement	Available internally
2. Purpose and description of the personal data processing	
Purpose(s) of the personal data processing	An individual file (DI for "Dossier Individuel" in French) consists of documents representing all the decisions taken by the institution, fundamental external documents relating to each member of staff and those responsible for the information encoded in the human resources management tools. The objectives of the IDs are, inter alia, to: -tracing the careers of staff; -verify the veracity of information stored in human resources management tools; -archive individual decisions taken by the Appointing Authority so that they can be consulted according to the legitimate needs of the relevant staff and services.
Categories of persons whose personal data are processed	- Officials - Contract and temporary staff - Seconded national experts (SNEs) – files kept only in hard copy

Categories of personal data processed	All personal data of the DI are provided by the staff members themselves or by the administration. Sources of documents in a DI: - private external documents initially provided by each staff member at the time of recruitment or throughout their career within the institution; - decisions taken by the institution, of which the staff is duly informed. A DI contains personal data in documents grouped according to a standard nomenclature, such as: - documents related to the application (CV, application form, diplomas, certificates of employment, medical fitness, declaration on honour, etc.); - career documents (contracts, appointments/establishments, transfers, end of probation period/assessment reports, certification, individual decisions taken by the Appointing Authority/AECE with regard to the staff member concerned, etc.); - personal and family documents (birth, nationality, passport, residence, marriage, divorce, childbirth certificate, military service certificate, banking information, etc.); - documents related to entry into service (fixing of statutory entitlements, declaration of arrival, travel expenses, installation allowances, removal allowances, etc.); - documents related to entitlements concerning personal circumstances (family allowances, granting of allowances, tax abatement, etc.); - documents related to personal information (address and person to be prevented, transfer of pension rights, etc.); - Miscellaneous documents.
Recipients of the personal data	Each staff member has unlimited online access to their own digitised DI through the SYSPER application. The data contained in the DI are also accessible to the following parties: - managers of the NDP system of the Directorate-General DIGIT of the European Commission who ensure the security of the NDP system and its database; - head of unit and managers in the Recruitment and career unit responsible for the management and security of the NDP system in liaison with DIGIT; - managers in the Rights and obligations sector within the limits of their powers; - the Internal control and LAM office in unit EI and its deputy Head of unit - managers responsible for handling administrative files whose management has been outsourced by the CoR (including rights and privileges) under a service agreement; - members of joint committees involved in procedures requiring access to certain personal data (promotion, certification, report committee, etc.) have restricted access for the duration of the work of such committees; - the Director (Deputy Director) of the Directorate for Human Resources and Finance, the Internal Audit Service, the Legal Service, the Disciplinary Board, the Court of Justice, the Court of Auditors and OLAF having a legitimate reason for consultation may be granted restricted access to DI within the limits of their duties.

	Each consultation of a DI by a third party is registered by the NDP system (name, access role, date and time of the consultation) and the holder is thus informed.
Transfers of personal data to a third country or an international organization	No
Retention period of the personal data	-The DI shall be kept until the rights of the official or of the staff member of the Staff Regulations and his or her dependents, including appeals, are extinguished for a period of 100 (one hundred) years from the date of recruitment of the official or staff member. -For SNEs, the retention period for the DI is set at 12 years following their departure from the CoR. -In the event that an official request for the transfer of DI for a staff member is transmitted by another institution (under Conclusion No 259/2012 of the College of Heads of Administration of 30 January 2013), this request and the acknowledgement of receipt of the transferred DI (via NDP or paper) shall be kept. Since October 2014, staff members leaving the CoR must also sign a declaration form stating that they have become aware that, under Conclusion No 259/2012, their individual file could possibly be transferred to another European institution.
General description of security measures, where possible	Concerning physical files Paper-based DIs are kept under key by the individual records manager and are accessible only in a locked secure room provided for this purpose. Access to a third party's personal paper file is strictly limited. DIs should only be consulted on site. Concerning electronic files Digitised versions of DIs are stored on the servers of the European Commission's Data Center. The CoR and DG HR have signed a Memorandum of Understanding. The CoR uses the IT platform provided by DG DIGIT which processes the data as a processor on behalf of the controller. The security measures are the same as for European Commission data. Access rights are controlled by the controller at the European Committee of the Regions. The security of the database and data transfer is ensured by DIGIT on the basis of the Memorandum of Understanding. The consultation of the digitised DI is recorded and available for information, both for the holder and the manager. Access to digital DI is strictly regulated and granted by the security manager to authorised persons, within the limits of the regulatory provisions, on the basis of a written request. Any consultation of a DI by a third party shall be recorded in the consultation history and the informed staff member.
Data protection notice	Published internally