Standard Operation Procedures	SOP_038
Effective Date: 24/10/2019	**Public**

Data protection compliance support

Special Requirements	This procedure is a controlled document maintained by Quality Management. It may not be deleted without comparable controls. Please note that this document becomes uncontrolled once printed. Make sure by always referring only to the Repository that you have the right version in use. Deviations from the provision of this document need to be recorded in the Exception Request Workflow. The procedure should be updated when there are changes in EFSA with respect to what is stated in the document (e.g. Relevant Standards, legislation, and documents, change in procedure, etc.). The person responsible for maintaining this procedure up to date is the Lead author with the support of the QM.

Process Responsibility	Process owners are accountable this procedure being adhered to within their respective or unit. All relevant staff is responsible for the correct implementation of the procedure. Responsibilities for performing specific steps are outlined in the document.

SCOPE AND OBJECTIVES

This SOP clarifies the steps related to the process E12.05 Personal Data Protection Management, to be followed in different processes to achieve compliance with personal data protection rules as well as the steps to be followed by the Data Protection Officer in the pursuit of his tasks.

- The Executive Director (ED) is responsible for the implementation of the data protection obligations of EFSA ;
- The Heads of Unit (HoU) and Heads of Department (HoD) assume the role of Controller in the sense of the Data Protection Regulation (EU) 2018/1725, which means that they shall guarantee compliant personal data processing in the context of the management processes and systems they are in charge of ;
- The Data Protection Officer (DPO) is responsible for ensuring the coherent internal application of the provisions of the Regulation (EU) 2018/1725 and for advising the Controllers on fulfilling their obligations;
- The European Data Protection Supervisor (EDPS) ensures that all EU institutions and bodies respect people's right to data protection and privacy when processing their personal data

RELEVANT STANDARDS, LEGISLATION AND DOCUMENTS

- The Treaty of the Functioning of the European Union, i.e. Article 16
- The Charter of Fundamental Rights of the Union, i.e. article 7 and 8
- Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (hereafter referred to as 'the Data Protection Regulation')
- Comprehensive information and documents are available in the Data Protection Workspace on DMS, accessible via the BuS Service Catalogue
- For daily assistance, advice and correspondence on data protection at EFSA, a functional mailbox is in use, managed by the DPO: DataProtectionOfficer@efsa.europa.eu

ABBREVIATIONS AND DEFINITION

Controller	The unit or any organizational entity in EFSA, which alone or jointly with others determines the purpose and means of the personal data processing. The controller thus is the business owner of a process, which at EFSA usually concerns the HoU or HoD level
DPIA	Data Protection Impact Assessment – For activities likely to result in high risks to the rights and freedoms of natural persons, the controller shall carry out an ex ante assessment of the impact of the processing on the protection of personal data. The DPIA shall be prepared in the situations indicated and taking account of the modalities detailed in Article 39 of the Regulation
DPO	Data Protection Officer. The designation, position and tasks of the DPO are detailed in Art. 43 till 45 of the Regulation - DataProtectionOfficer@efsa.europa.eu
ED	Executive Director
EDPS	European Data Protection Supervisor - the independent supervisory body established by the Data Protection Regulation (Chapter VI of the Regulation) http://www.edps.europa.eu/ - edps@edps.europa.eu
EUIs	Institutions, Bodies and Agencies of the European Union
ISO	The Information Security Officer of EFSA
Personal data (PD)	Any information relating to an identified or identifiable natural person ('data subject' - DS)
Personal data processing activity	Any operation or set of operations which is performed on personal data, whether or not by automated means, such as their collection, recording, storage, alteration, retrieval, consultation, disclosure by transmission, dissemination, making available online

Processor	Any physical or legal person, including contractors and external consultants of EFSA, processing personal data on behalf of a controller. The processor acts on documented instructions from the controller
Recipient	A natural or legal person, public authority, agency or any other body to whom personal data are disclosed, whether a third party or not
Record	Each controller shall maintain a record of processing activities under his responsibility. The information to be contained in the Record is detailed in Article 31 of the Regulation
Register	A list of the Records on processing operations at EFSA collected in The Data Protection Workspace and that shall be publicly accessible
PROCEDURE 1	DOCUMENTING PERSONAL DATA PROCESSING – RECORD & DATA PROTECTION IMPACTA ASSESSMENTS (DPIA)
	Previous SOPs in the process:
Step 1	1.0 Identification of personal data processing operations in the Controller's remit (sub steps below refer to alternative ways for identification)
Controller, DPO	1.1 The Controller identifies new or modified personal data processing within his remit 1.2 Alternatively, the DPO may identify processing to be documented in a Record based on an inventory of data processing and cross-checking with the Controller 1.3 Sporadically, personal data processing may be identified via other means (via Commission implementing rules, information from data subjects etc.)
Step 2	2.0 Records drafting (Article 31 of the Regulation
Controller with support of the DPO	2.1 For each personal data processing operation, the Controller compiles some essential information and prepares the Record using the EFSA Record template 2.2 The DPO checks and completes the Record, i.e. drawing attention to the information it should contain, including the name and contact details of the controller & DPO, the purpose of the processing, the legal basis, the categories of data subjects and personal data concerned, recipients and any transfers to third countries or international organisations, a general description of security measures applied, the retention period, information provision to data subjects on the way to exercise their rights pursuant to the Regulation. 2.3 The controller validates the Record which is sent to the DPO for insertion in the Register.
Step 3	3.0 Data Protection Impact Assessment (DPIA) (Article 39 of the Regulation)

Controller with the support of DPO	3.1 Whereas all processing operations at EFSA need to be documented in Records (*step 2*), only some of them need to undergo a DPIA. The DPIA is needed when, (1) the process is on an EDPS list of risky processing (*to be established*), or (2) it is likely to result in high risks resulting from the DPIA threshold assessment questionnaire 3.2 The controller is responsible for the DPIA drafting and can rely on the assistance, guidance and advice of the DPO. The relevant DPIA template shall be used which reflects the requirements in Article 39(7) of the Regulation. The DPIA process is intended to provide reasonable assurance that controllers adequately address any risks to the rights and freedoms of the individuals concerned. By documenting risks and possible mitigation measures in a structured manner, the DPIA helps achieving the '*data protection by design'* principle in the Regulation. 3.3 The Data Protection Impact Assessment (DPIA) to be documented in the risk register linked to the E12.8 Personnel Data Protection Management process variant
Step 4	4.0 Consultation with the EDPS under Article 40 of the Regulation
Controller with support of the DPO	4.1 In case the outcome of the DPIA report (*step 3*) is that with the application of mitigation measures, residual risks to the rights and freedoms of data subjects remain too high, or in case the controller has doubts whether the risks are appropriately mitigated, the EDPS shall be consulted in application of Article 40 of the Regulation.
Step 5	5.0 Publicity – Records register & DPIA reports
DPO	5.1 All Records (*step 2*) become part of the Register of personal data processing maintained centrally by the DPO of EFSA. The Register is updated and reviewed regularly and it is accessible internally to all staff via DMS. The Regulation prescribes that it shall become publicly accessible (Art. 31.5 of the Data Protection Regulation) 5.2 Although not specifically required in the Regulation, the EDPS recommends as a good practice the publication of the DPIA reports (*step 3*), except for information security details
Step 6	6.0 Updating of the Record and/or the DPIA
Controller with support of the DPO	6.1 Should the processing operation undergo substantial modifications on aspects related to data protection, the Record shall be updated as described in *step 2* and the register shall be updated accordingly 6.2 Likewise, also DPIA reports shall be reviewed on a periodical basis, including extraordinary reviews as appropriate.