

Last updated 5/6/2019

**PROTECTION OF PERSONAL DATA
NOTIFICATION OF PROCESSING OPERATIONS - EUI**

Name of Service: Real Estate and Facilities Service

1. Processing	
1.1 Name of the processing	EUI Helpdesk
1.2 Description of the processing	<p>The EUI Helpdesk is the single point of contact for support/information requests re. REF and ICT Services submitted by both EUI and non-EUI users. Support requests (tickets) are filed in the customer portal of the software <i>Xperience</i> which resides on EUI grounds and of which the EUI owns regular license.</p> <p>Support requests can be filed:</p> <ul style="list-style-type: none"> • By authenticating to the customer portal at https://helpdesk.eui.eu • Via Email by addressing eui.helpdesk@eui.eu • Via Phone by calling ext. 2600 (+39 055 4685 600) <p>Requests are then categorised, integrated with additional data (when and if missing) and processed by the relevant technical support unit.</p>
1.3 Name of the Data Controller	Director of the REF Service (Mrs Kathinka España)
1.4 Organisational Unit of the Controller	Real Estate and Facilities Service (REFS)
1.5 Name of the Delegated Controller (optional)	Member of the REF Service (Mrs Huguette Gonnelli)
1.6 Name and First Name of the Processor(s) (if any)	<p>Mrs Laura Bechi member of REF Service</p> <p>Mr Martin Legner member of ICT Service</p>
1.7 Name and First Name of the External Processor (if any)	Basis Information Technology S.r.l. Service Provider
1.8 Automated Processing	When a user files an EUI Helpdesk support ticket either via Customer Portal, Email or Phone.
1.9 Manual or Electronic Processing	<p>Manual processing: N/A</p> <p>Electronic processing: the Helpdesk operators process tickets verifying that all necessary data are available and may integrate any missing data by consulting other EUI databases like CPR or SMART. This information is visible within the ticket and may be shared with internal and outsourced technical units for the resolution of the ticket itself.</p>
1.10 Storage Medium	Data is stored on EUI's two server farms in Badia Fiesolana and Villa Salviati. Data relating to support requests filed via Phone are collected outside the EUI, on the server farm of the service provider.

1.11 Comments	
2. Purpose and Legal Basis	
2.1 Purpose of processing	The data are collected and processed to provide the support service required to the data subject after registering/authenticating. The other personal data that may be collected through automated logs (i.e. when filing a support request via Phone) serves to ensure the efficiency and timeliness of processing operations.
2.2 Legal Basis	<ul style="list-style-type: none"> - Annex I, Chapter II B) of the Convention setting up the EUI; - Art. 8 C), third bullet of President's Decision N° 36/15 of 04/11/2015; - Art. 1e of Staff Regulations applicable to permanent staff members of the European University Institute, as laid down by High Council Decision n°6/2014 of 5 December 2014 laying down the Service Rules of Administrative Staff; - Art. 10 and 80(4) of the Conditions of Employment of Other Servants of the European University Institute, as laid down by High Council Decision N° 6/2014 of 5 December 2014 laying down the Service Rules of Administrative Staff.
2.3 Lawfulness of processing	The processing of personal data is lawful because processing is necessary to perform an institutional task represented by the administration of the EUI Helpdesk in accordance with Article 5 b) i) of EUI President's Dec. No. 10/2019 regarding Data Protection at the EUI .
3. Data Subjects/Data Fields	
3.1 Types of Data Subjects	<p>EUI members like:</p> <ul style="list-style-type: none"> • Administrative staff • Academic staff • Alumni (Friends of the EUI) • External Contractors and/or Consultants • Fellows • Out-sourced staff • Researchers • Retired Staff • Trainees • Visitors <p>Non-EUI users like:</p> <ul style="list-style-type: none"> • Prospect members • External participants to conferences • Summer school students • etc.
3.2 Data Fields	<p>The following personal data are collected automatically via existing databases and visible to the Helpdesk operators in the customer portal:</p> <ul style="list-style-type: none"> • Name • Function • Affiliation expiration • Unit • Contact details (email address and business telephone number) • Location information (Building, Office/Flat number and Desk/Room) <p>The following personal data can be provided on a volunteer basis by the Data Subject and will be recorded accordingly:</p> <ul style="list-style-type: none"> • Mobile telephone number • Alternative email address

	<p>When requesting support via Phone, the following additional data is collected:</p> <ul style="list-style-type: none"> • Originating number • Waiting time • Duration of the phone call
4. Rights of data subjects	<p>By registering to the Customer Portal, the data subject is informed that the processing of the personal data is performed in accordance with article 16 of the President's Decision n. 10/2019 regarding Data Protection at the EUI .</p> <p>Right of information: Data subjects are informed on their rights and how to exercise them via a specific Privacy Statement, available at the DPO Registry. A link on the login page of the EUI Helpdesk portal redirects Data Subjects to the EUI Data Protection webpage.</p> <p>Rights of access and rectification: the data subject has the right to access and verify which personal data are stored and may also ask for his personal information to be corrected or deleted by addressing a request to the Data Controller of the REFS at Data ControllerREFS@EUI.eu, who shall reply within 30 working days. .</p> <p>If data subjects believe that there has been a breach on the data protection principles of the President's Decision n. 10/2019, they have the right to address a complaint to the Data Controller of the REFS (Data ControllerREFS@EUI.eu) with simultaneous notification to the EUI Data Protection Officer Data_Protection_Officer@EUI.eu</p>
5. Retention Period	Data is kept for at least five years after the creation of the ticket.
6. Historical Purposes	Data are used to compile reports and statistics of operational efficiency and sustainability.
7. Recipients	
7.1 Inside the EUI	<p>The collected data will be treated confidentially and used only by teams in charge of user support activities, by supervisors to manage the service and by Directors to assess quality assurance. Aggregated data, such as number of total tickets per Unit, is used for the Annual Activity Report of the two Services involved.</p> <p>The REF and ICT Services do not share personal data collected with third parties other than the designated providers, contractors and subcontractors involved in the support process chain.</p>
7.2 Outside the EUI, inside the EU/EEA	<p>The REF and ICT Services do not share personal data collected with third parties unless required to do so by law enforcement.</p> <p><i>Please refer also to Art. 17 of President's Decision 10/2019.</i></p>
7.3 Outside the EUI, outside the EU/EEA	N.A.
8. Technical and organizational security measures	<p>The EUI is committed to ensure that the personal information of users is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and help prevent unauthorised access and maintain data security.</p> <p>The security of the personal data is safeguarded through adequate technical and organisational security measures in compliance with Article 11 (Security of processing) of the President's Decision No. 10 of 18 February 2019 regarding Data Protection at the EUI.</p> <p>Technical measures</p> <p>Secure access controls are enforced using tools and technologies to ensure that access rights are granted according to the need to know principle and at least privileged. Users can access data and EUI's resources after successful authentication using their own credentials (login and password). The ICT Service makes available tools and support to ensure that data in transit are transferred encrypted unless users decide otherwise.</p>

	<p>Organisational measures</p> <p>Internal processes have been put in place to ensure the level of security appropriate to the risks represented by the processing and the nature of the personal data to be processed and to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.</p> <p>In case of a data breach the Controller shall communicate the personal data breach to the data subjects without undue delay.</p> <p>A Declaration on confidentiality and protection of personal data is signed by newcomers and current staff when the renewal of their contract is confirmed.</p> <p>Members of EUI staff who have access to the library users' personal data are required to protect it in a manner consistent with the Privacy Statement for this processing operation.</p>
<p>9. Complementary information</p>	