## eduroam Data Mapping

<table>
<thead>
<tr>
<th>Name</th>
<th>Personal Data</th>
<th>Special Category</th>
<th>Data at Subject</th>
<th>Purpose</th>
<th>Location of PD</th>
<th>Retention Period</th>
<th>Comp</th>
<th>Proc</th>
<th>Transfer</th>
<th>Recipient</th>
<th>Controls Implemented</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>eduroam_RADIUS server logs</td>
<td>Outer EAP-Identity (username@institution_domain, username can be anonymised but not all users do that), Calling-Station-Id (users MAC address), Chargeable-User-Identity (users anonymous ID)</td>
<td>No Digital end users</td>
<td>debugging, providing quality service, monitoring load of system, dimensioning of the system, incident management and preventing fraud and misuse</td>
<td>(f) limited at a interest est</td>
<td>ETLR located in Netherlands (Surftel) and Denmark (DEIC)</td>
<td>TBD</td>
<td>G EA NT</td>
<td>not transferred</td>
<td>N/A</td>
<td>(RADIUS + EAP (SSL used), HTTPS), protective measures according to each hosting centre's security policy.</td>
<td>data received from ETLR</td>
<td></td>
</tr>
<tr>
<td>eduroam-F-ticks</td>
<td>realm, Calling-Station-Id (User's device MAC address),</td>
<td>No Digital end users</td>
<td>debugging, providing quality service, monitoring load of system, dimensioning of the system, incident management and preventing fraud and misuse</td>
<td>(f) limited at a interest est</td>
<td>ETLR located in Netherlands (Surftel) and Denmark (DEIC)</td>
<td>TBD</td>
<td>G EA NT</td>
<td>not transferred</td>
<td>N/A</td>
<td>protective measures according to each hosting centre's security policy.</td>
<td>data received from federation level RADIUS servers and optionally from home and visited institution RADIUS servers</td>
<td></td>
</tr>
<tr>
<td>eduroam Database: NRO information</td>
<td>name, e-mail, phone number</td>
<td>No Digital end users</td>
<td>performance of contract between GEANT and (N)RO</td>
<td>(b) contract</td>
<td>Croatia permanently</td>
<td>G EA NT</td>
<td>Srica</td>
<td>not transferred</td>
<td>N/A</td>
<td>protective measures according to each hosting centre's security policy.</td>
<td>data received form (N)RO</td>
<td></td>
</tr>
<tr>
<td>eduroam Database: institution information</td>
<td>name, e-mail, phone number</td>
<td>No Digital end users</td>
<td>performance of contract between GEANT and institution (IdP or SP)</td>
<td>(b) contract</td>
<td>Croatia permanently</td>
<td>G EA NT</td>
<td>Srica</td>
<td>not transferred</td>
<td>N/A</td>
<td>protective measures according to each hosting centre's security policy.</td>
<td>data received form (N)RO</td>
<td></td>
</tr>
<tr>
<td>eduroam Database: service locatio informaion</td>
<td>name, e-mail, phone number</td>
<td>No Digital end users</td>
<td>performance of contract between GEANT and institution (IdP or SP)</td>
<td>(b) contract</td>
<td>Croatia permanently</td>
<td>G EA NT</td>
<td>Srica</td>
<td>not transferred</td>
<td>N/A</td>
<td>protective measures according to each hosting centre's security policy.</td>
<td>data received form (N)RO</td>
<td></td>
</tr>
<tr>
<td>eduroam CAT (as of versio n 1.1)</td>
<td>eduPersonTargetedId or equivalent, real name, email address (administrator authentication)</td>
<td>No Digital end users</td>
<td>allowing administrators to upload and maintain the information needed to create eduroam installation programs (&quot;Installers&quot;) within their country / institution (CAT customization)</td>
<td>(b) contract</td>
<td>Netherlands (Surftel) the authorisation status of administrators is retained permanently, TBD</td>
<td>G EA NT</td>
<td>TBD</td>
<td>System sends emails with invitation tokens (one variant to institution administrators for sign-up, one variant to end-users for credentialing, one variant to NRO personnel for general status updates)</td>
<td>NRO personnel</td>
<td>protective measures according to each hosting centre's security policy.</td>
<td>data received from eduroam SP proxy</td>
<td></td>
</tr>
<tr>
<td>eduroam Managed IDP</td>
<td>eduPersonTargetedId or equivalent, real name, email address (administrator authentication)</td>
<td>No Digital end users</td>
<td>allowing administrators to upload and manage the information needed to manage their end user base to the end of creating eduroam installation programs (&quot;Installers&quot;) within their country / institution, and to authenticate their users in eduroam</td>
<td>(b) contract</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>System sends emails with invitation tokens (one variant to institution administrators for sign-up, one variant to end-users for credentialing, one variant to NRO personnel for general status updates)</td>
<td>NRO personnel</td>
<td>protective measures according to each hosting centre's security policy.</td>
<td>TBD</td>
<td>eduroam database, eduroam SP proxy, authentication, administrator input</td>
</tr>
</tbody>
</table>
 Instructions

The table above should be filled with all data which is collected or processed by Geant Services according with Article 30 from GDPR. Below are described all the table’s points and also the information they shall be provided to complete this exercise. You can find as well the match between GDPR requirements and the points from Data Mapping marked with ().

1 Name - Name of the service or project and dataset, if applicable;

2 (30 1c) Personal Data - Any information relating to an identified or identifiable natural person, it means that could be identified, directly or indirectly through this data,
   - Name,
   - Birth dates
   - Address
   - Email address, IP address, Mac Address,
   - Id card, social security number, VAT number
   - Job title, academic qualifications,
   - Banking details;

3 (30 1c) Special Category - Check if special categories of personal data are processed, eg. racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. Article 9 of GDPR describes Special categories of Personal data a that can revealing, and the processing of for the purpose of uniquely identifying a natural person, data concerning genetic data, biometric data health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.
   - Medical records
   - Genetic and biometric data
   - Ethnic origin
   - Political opinions
   - Membership of a trade union
   - Religion
   - Sexual orientation
   - Criminal activity (criminal records)

4 Data Format - Physical or Digital;

5 Data Subject - Natural persons who’s personal data are collected and processed;

6 (30 1b) Purpose - What is the purpose of data collecting and processing. Personal Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

7 Legal Bases - Describe legal bases for data processing as defined in Article 6, one of the following: (a) consent, (b) contract, (c) legal obligation (law), (d) protect vital interest of data subject of another person, (e) public interest or exercise of official authority (law), (f) legitimate interests Eg.:Contract, Clauses, Terms and Conditions, Agreements, Disclaimers, etc.

8 Location of Personal Data - Where personal data are stored, database/server, country;

9 (30 1f) Retention Period - The Personal Data only should be keep for the period previous defined based on Business, Legal or Contractual purposes or Obligations;

10 (30 1a) Controller Contacts - The controller means the natural legal person (authority, agency or other body), that is responsible to determines the purposes and means of the processing of personal data. This point should include the contacts of the Data Protection Officer nominated.

11 (30 1a) Processor Contacts - The processor means a natural or legal person (authority, agency or other body), witch processes personal data on behalf of the controller. If applicable, this point should include the contacts of the Data Protection Officer nominated.

12 (30 1e) Transfer - Description of other services, systems, applications, databases where data are being sent.

13 (30 1d) Recipient - If applicable, name recipient of personal data;
14 (30 1g) Controls Implemented - Describe what controls are in place to protect personal data as defined in Article 32. (a) pseudonymisation, encryption; (b) confidentiality, integrity, availability and resilience; (c) backup; (d) regularly testing, assessing and evaluating the effectiveness of technical and organisational measures. Eg.: Anonymised (Encryption) 32a) / Backup 32 c) / Encrypted Channel 32 b) / Access Control 32 2);

15 Interfaces - Who receive and who send personal data - Service, Applications / What are the channels used for communication / What kind of services are connected eg. internet, firewall, storage devices (Cloud Systems);