OVERVIEW OF LEGAL AND GDPR ROLES WITHIN THE EDUVPN SERVICE

General aim

This overview aims to give an insight into the legal/GDPR roles connected to the entities participating in the service eduVPN. It is part of the eduVPN legal project funded by NLnet. The overview is made in cooperation with GÉANT, SURF and the eduVPN-team. Complementary to the overview there will be a listing of detailed actions like additional agreements/policies that are needed based upon the overview of entities and GDPR roles. The last step is an easy understandable description of the whole setup from a privacy perspective to inform the end user and parties interested in joining the service.

The general aim of the eduVPN legal project is:

- to give assurance about GDPR compliance;
- to contribute to the privacy of the end users and their ability to exercise their privacy rights;
- to serve the further development of the service.

Definitions GDPR: controller, processor, data subject (GDPR definitions can also be part of the Explanatory notes)

GÉANT: GÉANT is a membership organization acting with and for its members to further research and education networking in Europe and globally. The members of GÉANT are the NREN's within Europe.

NREN: National Research and Education Network, a specialized internet service provider dedicated to supporting the needs of the research and education communities within a country.

Institute: an organization using the services of the NREN as a member or in another way part of the constituency of the NREN. Typically this are universities, colleges of higher education, university medical centres and research institutions

The Commons Conservancy: a foundation with a shared legal infrastructure which makes it possible for projects to act as a legal entity. Projects under the flag of the commons conservancy must be 'free and open' meaning the project is part of the 'commons' by explicitly allowing anyone to build and extend on what is created in the project. The technical governance of eduVPN –

meaning the software, protocols and copyright on these components - is done by the board of the eduVPN program under the Commons Conservancy.

The GÉANT eduVPN projectteam (eduVPN team): a team of eduVPN experts from the NREN's that initiated and developed the service that work together to operate the service as a GÉANT project team.

Global eduVPN governance committee (the committee):

Current definition: the Gegoc is an instance composed of 5 members designated by the eNOs for a period of 2 years. It is responsible for defining the global service framework

The committee will be redefined into a representative body to make sure the governance is setup in line with the legal/privacy framework. All NREN's that signed the policy are represented and have a say in the way the service is organized including the personal data that is processed by the NREN's.

EduVPN confederation policy (the policy): the policy signed by the NREN's providing eduVPN Secure Internet to their constituency

GDPR overview eduVPN

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
GÉANT providing the eduVPN central server infrastructure	GÉANT acts as the legal entity providing the eduVPN central server infrastructure connecting the participating VPN servers. This allows NRENs and their participating institutions to offer eduVPN to their users. GÉANT facilitates the service and has the overall coordination - technical and organizational - to make the service possible. GÉANT is responsible for the setup, management and maintenance of the servers required for eduVPN central server infrastructure. The central server infrastructure consists of two servers: repo.eduvpn.org and disco.eduvpn.org. Technically the repo server exists out of parts, one is where the server software is hosted and the other where clients software is hosted. The disco.vpn.org server ensures the eduVPN client discovery that makes it possible for the users to connect to their eduVPN server. The eduVPN server of the NREN is visible in the app/client and can be chosen by the user. Providing the back-bone service to the NREN operationally means to modify the list of servers on disco.eduvpn.org on request of the NREN. The repo.eduvpn.org server ensures that the eduVPN software can be downloaded. These servers are managed by SURF and SIKT on behalf of GÉANT The disco and repo server logging has been turned off so no personal data is processed.	None		eduVPN has a distributed federated set-up that uses existing authentication systems/identity management systems (out of scope here). For the sake of clear privacy governance, a distinction is made between the eduVPN central servers and the eduVPN servers that are maintained by the NRENs and institutions. After signing the NREN is connected to the infrastructure and is authorized by GÉANT to offer and perform the service to its institutes and users.

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
GÉANT as the contracting party and offering the central components of the service	Complementary to the above operational task, GÉANT is the contracting party for the service and facilitates and coordinates the central addition components of the service. It concerns at least: Facilitate the global eduVPN governance committee in which the NRENs (also outside Europe) participate Managing the eduVPN confederation policy (version, edits, publishing) Ensuring compliance with the policy Offering the eduVPN website Enter into agreement with the NREN's The personal data processed is the contact information needed for the above tasks and website cookies.	Controller The legal ground of processing personal information is legitimate interest to provide the service	NREN's that wish to connect to the central server infrastructure need to sign an agreement with GÉANT. This agreement regulates: The delivery of the service (connecting to the central server infrastructure) by GÉANT; The description and guaranties concerning the processing of personal data by GÉANT; The commitment of the NREN to the eduVPN confederation policy (a further elaboration of the current compliance statement) as administered by the global eduVPN governance committee; The participation of the NREN in the global eduVPN governance committee. GÉANT publishes a privacy statement giving an overview of all the (potential) processing of personal data within the eduVPN service and where additional information about the processing of personal data can be found. GÉANT publishes a Cookie statement on the eduVPN website.	
NREN providing eduVPN Secure Internet to their own constituency	The NREN sets up an eduVPN server and connects it to the eduVPN backbone. The NREN provide Secure Internet to users who have installed an eduVPN client on their device. Only users of which the institution has agreed upon the Secure Internet service can use the Secure Internet service. (*It is possible that this is implemented as an opt out as part of the authentication policy of a NREN*) The name of the country is visible in client/app and can be chosen by the user to setup a Secure Internet connection.	Controller The legal ground of processing personal information is legitimate interest to provide the service	The eduVPN confederation policy Legitimate interest assessment Service agreement Secure Internet NREN – Institute Privacy policy NREN	The NREN can be regarded as the controller if the governance is set up in such a way that it can be said that each participating NREN has influence on determining i) the personal data (fixed dataset/attributes) that are processed, ii) the purpose (obtaining secure access for end users) and iii) the resources (linked vpn-servers within eduVPN). The NREN's are independent controllers (differentiated from joint controllership) because the processing they carry out is separable and could be performed by one party without intervention from the other*.

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
	The institute of the user serves as the Identity Provider and is connected to the authentication infrastructure of the NREN (for example at SURF this is SURFconext). The processing of personal data within the authentication infrastructure is not part of this framework. The NREN processes as a result of this authentication process a identifier, typically this is a so called persistent ID *(not implemented yet as the only allowed option)* By approving the application and choosing the secure internet instance (the NREN) by the user the NREN also processes a list of certificates created by the user and an OAuth token (a session key). The identifier – persistent ID - is randomly generated and pseudonymous. The mapping of the identifier to the associated user shall only be made when the NREN is required to do so pursuant to the law, a judicial decision or abuse The NREN provides the VPN connection to the user and processes the following data related to use of the service: ○ The time the VPN connection was established. ○ The time the VPN connection was closed. ○ The IP addresses assigned to the user's VPN client ○ The amount of data that was transferred by the VPN client. The NREN determines which data of a user of an institution is processed when using the service. The institution of the user has no access to the data. The eduVPN confederation policy signed by the NREN sets the boundaries of the personal data that is processed The NREN publishes a privacy statement.			The NREN has to sign the eduVPN confederation policy which describes the personal data that is processed when offering Secure Internet. The policy should require the use of a persistent NameID from the user. This identifier is randomly generated and pseudonymous. The policy should also limit the user data that is collected. The NREN participates in the Global eduVPN governance committee and has a vote in the decision making. The eduVPN confederation policy describes the way in which compliance and enforcement of the policy is reached.

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
	(*The privacy statements of SURF and DEiC set an example that can be transformed to a template*)			
NREN providing Secure Internet to guest users	As a user of eduVPN you can also use a server of another NREN if this NREN is providing the Secure Internet service including guest access. It is a requirement of the policy to enable guest access for Secure Internet The NREN does not only process the data of their own institutions. They will also process personal data of users of other NRENs/institutions.	Controller The legal ground of processing personal information is legitimate interest to provide the service	Service agreement Secure Internet NREN – Institute The legitimate interest assessment Privacy policy NREN should address quest use and data processing by another NREN the user's 'own' NREN . The eduVPN confederation policy limiting the personal data.	The NREN that offers Secure Internet offers can be regarded as controller even in the case of guest users. This means that each of the participating NRENs is independently responsible for its own part of the data processing on their own server. The confederation eduVPN policy must provide certainty regarding the processing of personal data to the NRENs offering guest Secure Internet and the data subject when acting as a guest user. It may be the case that the NREN is processing more or different personal data from users of other NRENs than the NREN does for its own users. It is depending on the way the other NREN/institution has set up the identification/authentication until this is fixed in the policy. The policy should describe and limit the personal data being processed so that NRENs can take responsibility for the processing of the personal data. The policy should be strict on the processing of additional metadata. Applicable law international guest Secure Internet. GDPR applies in the following situations*: EU guest using a non-EU server Non-EU guest using a European server
NREN providing	The service can be used by institutions to establish a safe encrypted connection between the user of the institution and the institution network.	Processor	processing agreement NREN-Institute	Institutions can decide for themselves whether they want to use eduVPN. The institutions purchase the

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
Institute Acces on a NREN vpn-server	The service runs on the vpn-server managed by the NREN. This is the case for two NREN's at this moment. Most institutes deploy their own server. The institution determines which personal data is required to setup the connection. They follow their authentication method of their choice. The institution is offered the possibility to manage the logging on the NREN VPN server for their own users. Therefore the NREN has no influence on that part of personal data that is processed. For this part the NREN will be the processor.		service agreement NREN - Institute (the relations between the NREN and GÉANT concerning the central server infrastructure is describe in this agreement) privacy policy Institute	eduVPN service from the NREN for its own users and/or visitors.
NREN providing Institute Access, Institute deploys its own server	NREN provides the connection to the eduVPN backbone, i.c. the name of the institute can be found by the user in the client/app to setup a connection to the institute. NREN and the Institute establish an connection on the authentication infrastructure provided by the NREN. This connection is out of scope in this overview.	None	service agreement NREN -Institute privacy policy Institute	
Institute providing Institute Access	Personal data consist of authentication data and logging data	Controller The legal ground of processing personal information should be decided by the Institute	service agreement NREN -Institute privacy policy Institute	The participating institutions are responsible for their own organizational and technical implementation of eduVPN. There are technical and organizational requirements to use the service in a proper way and to ensure the quality of the service (servers should be responsive, software up to date etc.).There should be an recommendation concerning personal data, for instance the preference that institutions will use attributes that are not directly reducible to users identities, e.g. using student numbers.

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
The Commons Conservancy	Technical governance limited to decision making regarding the protocols/software components including the app, licensing /IE. European eduVPN trademark has been assigned to the Commons Conservancy	none	Between Commons Conservancy and GÉANT an MoU should be signed about trademark usage, software governance etc	
SURF	App release Privacy by design principles: no tracker or telemetric functions High level statistic data from MS, Google and Apple	none		Task to be transferred to GÉANT or the Commons Conservancy