OVERVIEW OF LEGAL AND GDPR ROLES WITHIN A FEDERATED VPN SERVICE

AUTHORS: *Evelijn Jeunink & GÉANT eduVPN team*

RELEASE DATE: *March 2023*
RELEASED BY: *Commons Conservancy foundation – eduVPN program*

This project has been supported by NLnet

Based on the example of eduVPN, this document aims to present a clear overview of the legal framework and the General Data Protection Regulation (GDPR) roles that need to be defined for groups of organisations wishing to operate a federated VPN service. It is also meant to serve as a guideline for these organisations in helping them draw up privacy policies that can be easily understood, bearing in mind the complexity of these services. Having such privacy policies in place contributes to protecting the privacy of end users and their ability to exercise their privacy rights, as well as to strengthening the trust that participating organisations place in a federated VPN service, thereby driving increased participation in and use of these services.

Background:
eduVPN is a federated VPN service that is established in the higher education and research environment. While eduVPN operates specifically within that environment, the topics covered and the questions answered in this document can apply to any collaboration within a federated VPN service. The roles of the different parties in the eduVPN service are presented in the table in the appendix to this document. For every activity that involves personal data, the table provides details of the applicable GDPR role and legal grounds for processing of the data as well as any relevant legal documents. Where possible, references to templates or best practices are given.

A privacy statement for eduVPN covering all aspects of the service will be published on the eduVPN website where it can also serve as an example statement for organisations wishing to operate similar services. This type of general privacy statement aims to overcome the difficulties posed by the fact that multiple parties take part in the delivery of a federated service, by providing a complete and clear picture of the whole legal framework involved. All the (potential) instances of processing of personal data within the service are explained and references to additional information provided where necessary.

The roles and relationships defined in this document can be broadly grouped under two main areas:

- **Collaboration**
- **Innovation**

Collaboration:
The definitions of the legal and GDPR roles provided here are only applicable in a context in which several organisations share resources in order to offer a federated VPN service where users from one participating organisation can be granted access to a VPN managed by another participating organisation. Service offerings by a single VPN server operator to its members are outside the scope of this document.

Central infrastructure components:
The eduVPN setup comprises a central server infrastructure, composed of a discovery service and a software repository containing the client software, which integrates the participating VPN servers. This overview document considers the different parts of this central infrastructure and the responsibilities for the setup, management and maintenance of the servers. A single organisation is responsible for the central infrastructure of the eduVPN service.

Governance and contracting:
The organisation responsible for the central eduVPN infrastructure also has the responsibility for governance and contracting, including the following activities:

- Facilitating the governance committee in which participating organisations, or their representatives, take part
- Managing a confederation policy (version, edits, publishing) that governs the way in which participants offer the service to end-users
- Ensuring compliance with the confederation policy
- Offering a central place to publish relevant information for the participants and end-users (a general privacy statement)
- Entering into agreements with the participants

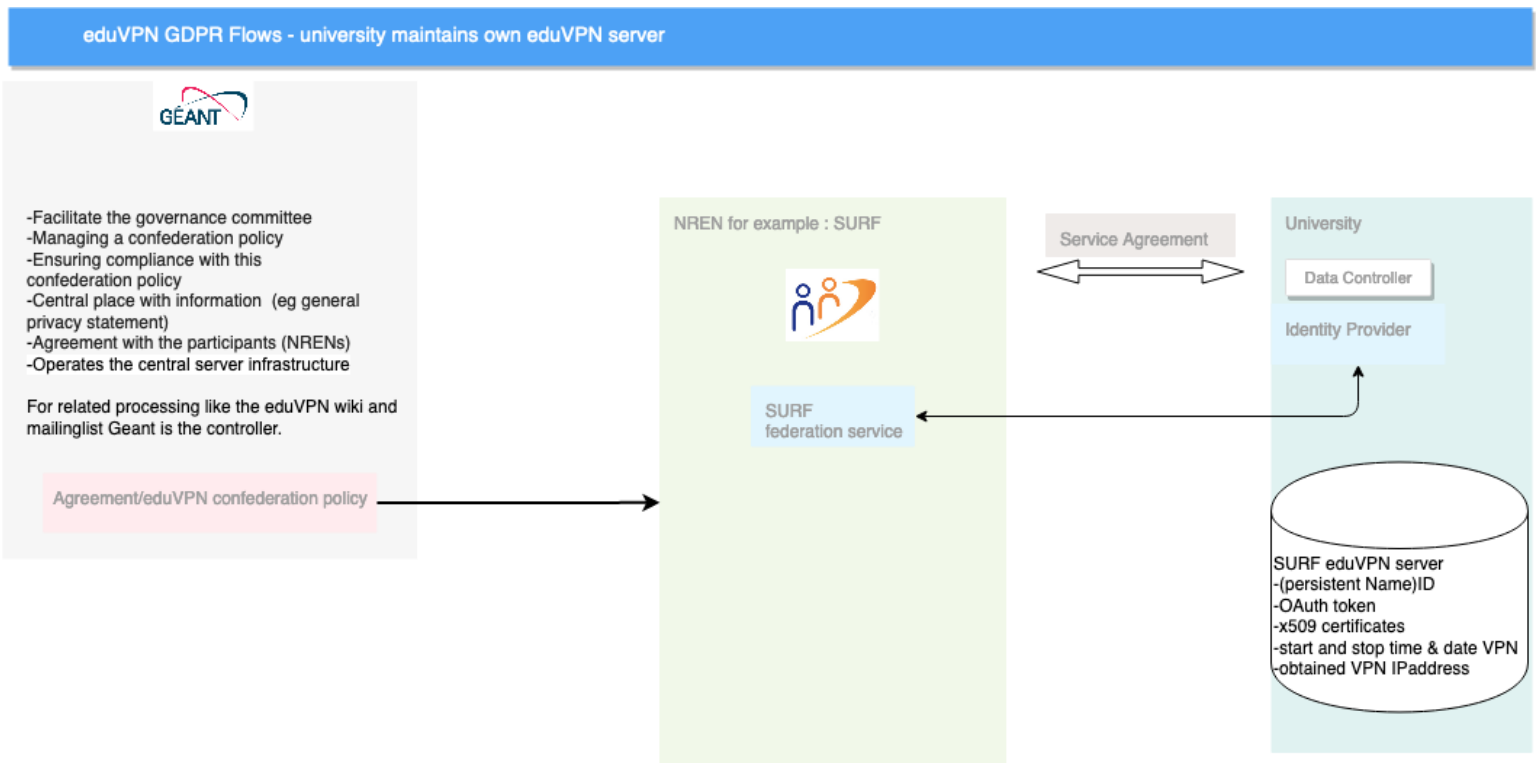
The committee is a representative body in which organisations participate directly or via delegation. The governance committee owns the confederation policy, which among other things describes and limits the personal data that is processed within the service. In the eduVPN setup, the use of a persistent name ID from the user (a randomly generated and pseudonymous identifier) is made obligatory. How compliance with the policy is enforced is also described in the confederation policy document.

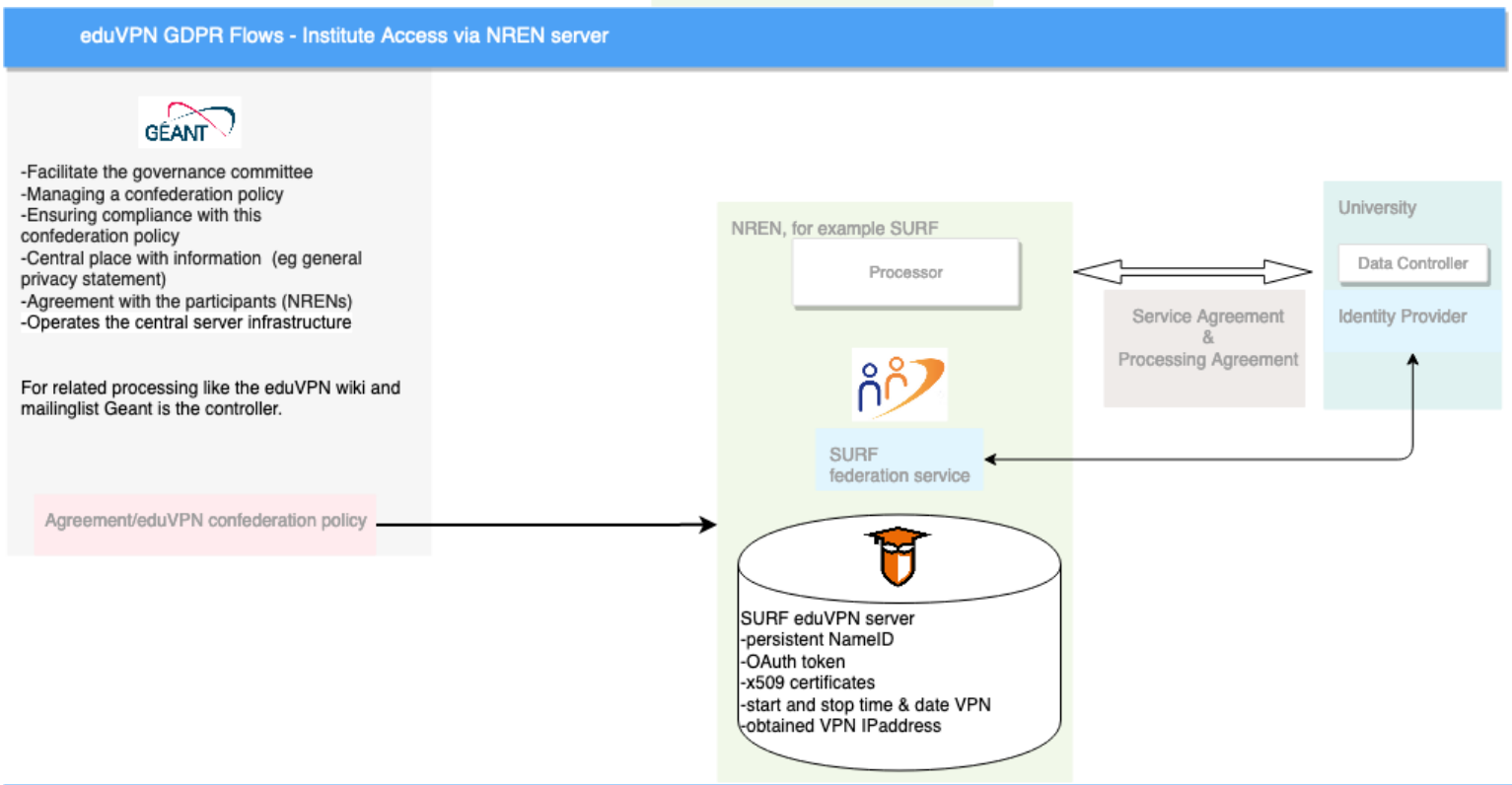
The parties involved are typically VPN server operators that take part in the service. It is important to note who is responsible for the authentication of the end-users in the eduVPN setup. The VPN server processes an identifier as a result of the authentication process. When providing the VPN connection to the user the VPN server processes some data related to the use of the service, for example the time the VPN connection was established, the time the VPN connection was closed, etc. Moreover, the VPN server operator determines which data of a user of an institution is processed when using the service. The federated VPN service confederation policy established in the eduVPN configuration sets limits on the personal data processed. This is done to make the service as privacy friendly as possible. The VPN server operator as controller of the processing publishes a privacy statement.

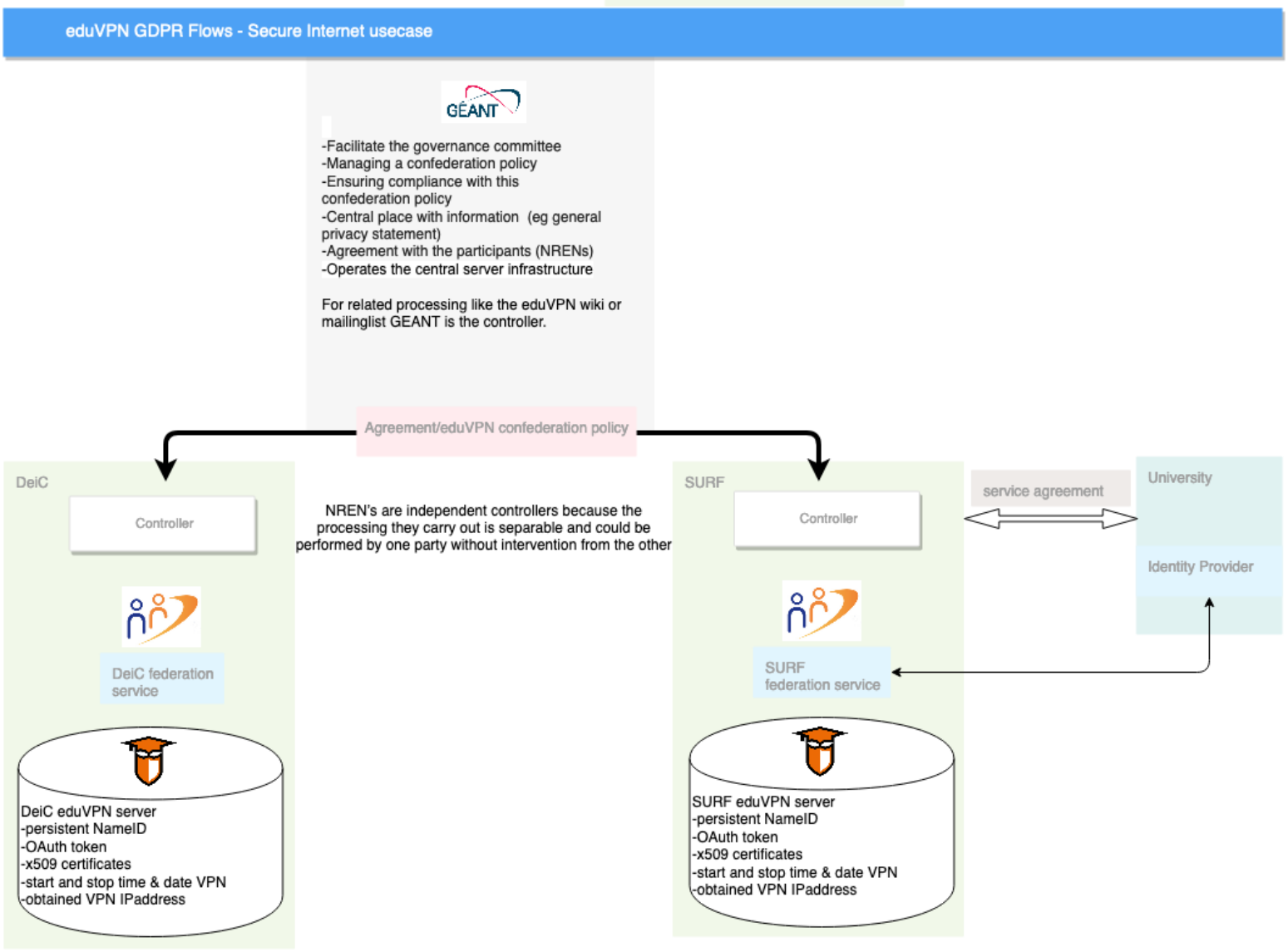
In the higher education and research environment, federated VPN service users can also use the servers of other VPN server operators provided that these allow Guest Access. In this case, these VPN server operators not only process the data of their own users but also that of the users of other VPN server operators. The confederation policy describes how this is done to provide assurance to the organisations providing Guest Access, as well as to the individual guest users.

Innovation:
Building and managing a federated VPN service typically requires the use and maintenance of software. This means that technical governance should be in place, including for further development of the service. Relevant issues in this respect are decision-making regarding protocols/software components including the app, intellectual property and licensing of the software and, where applicable, the brand and release of the client apps

The eduVPN setup in pictures







APPENDIX 1: OVERVIEW OF LEGAL AND GDPR ROLES WITHIN THE EDUVPN SERVICE

General aim

This overview aims to provide an insight into the legal/GDPR roles applying to the entities participating in the eduVPN service, as part of the eduVPN legal project funded by NLnet. This document is co-authored by GÉANT, SURF and the eduVPN-team. A supplementary list of detailed actions such as additional agreements/policies that are needed based on the entities and GDPR roles identified here will also be drawn up and made available alongside this document. Finally, an easily understandable description of the whole framework from a privacy perspective (privacy statement) aimed at end users and any parties who are interested in joining the service will be produced and published on the eduVPN website.

The general aim of the eduVPN legal project is:

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

Controller: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data […]" (GDPR, art. 4)

Processor: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (GDPR, art. 4)

Data subject: "identified or identifiable natural person[s]." (GDPR, art. 4)

GÉANT: GÉANT is a membership organisation 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 specialised internet service provider dedicated to supporting the needs of the research and education communities within a country.

Institute: an organisation using the services of an NREN and that is a member or part of the constituency of the NREN. Typically these 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 they are part of the 'commons' by explicitly allowing anyone to build and extend on what is created within their project. The technical governance of eduVPN – meaning the software, protocols and copyright on these components – is managed by the board of the eduVPN programme under the Commons Conservancy.

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

Global eduVPN governance committee (the committee):
Current definition: "The Gegoc is a committee composed of 5 members designated by the eNOs [eduVPN National Operators] for a period of 2 years. It is responsible for defining the global service framework."
This committee will be reorganised into a representative body tasked with ensuring that eduVPN governance is aligned with the applicable legal/privacy framework. All NRENs that signed the policy will be represented and have a say in the way the service is organised and personal data is processed by the NRENs.

eduVPN confederation policy (the policy): the policy signed by the NRENs providing eduVPN Secure Internet to their constituencies.

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 acts as the overall coordinator of the technical and organisational aspects that make delivery of the service possible. • GÉANT is responsible for the setup, management and maintenance of the servers required for the eduVPN central server infrastructure. • The central server infrastructure consists of two hostnames with a few identical servers behind it: the hostnames are repo.eduvpn.org and disco.eduvpn.org. Technically the repo server consists of two parts, one is where the server software is hosted and the other where clients' software is hosted. • The disco.vpn.org servers ensures that the eduVPN client discovery that makes it possible for the users to connect to their eduVPN server can be provided. 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 involves modifying the list of servers on disco.eduvpn.org on request of the NREN. • The repo.eduvpn.org servers ensures that the eduVPN software can be downloaded. • These servers are managed by NRENs, currently SURF and DeiC, 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 setup 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 authorised by GÉANT to offer and deliver the service to its institutes and users.

GÉANT as the contracting party that offers 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 addition of components to the service.
	• This includes at least:
	  ○ Facilitating the global eduVPN governance committee in which the NRENs (also outside Europe) participate
		• Controller
		• The legal ground of processing personal information is legitimate interest to provide the service
			• NRENs 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 guarantees concerning the processing of personal data by GÉANT;
			  ○ The commitment of the NREN to the eduVPN confederation policy (a further elaboration of
				○

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
	○ Managing the eduVPN confederation policy (version, edits, publishing) ○ Ensuring compliance with the policy ○ Offering the eduVPN website ○ Entering into agreement with the NRENs • The personal data processed is the contact information needed for the above tasks and website cookies.		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 provides Secure Internet to users who have installed an eduVPN client on their device. • Only users whose institution has agreed to using the Secure Internet service can use the Secure Internet service. (*It is possible that this could be implemented as an opt-out as part of the authentication policy of an NREN*) • The name of the country is visible in the client/app and can be chosen by the user to set up a Secure Internet connection. • 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 an identifier as a result of this authentication process, typically this is a so-called persistent ID *(not implemented as the only allowed option yet)* • When 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 transfer of the OAuth token needs to be explicitly 'approved' by the user before being transferred via the browser to the eduVPN client. • 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.	• 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 • NREN Privacy Policy	• 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 types of 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 NRENs 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 parties. • 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 set limits on the user data that is collected. • The NREN participates in the Global eduVPN governance committee and has a vote in decision-making. • The eduVPN confederation policy describes the way in which compliance and enforcement of the policy are ensured.

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
	• 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 privacy statements of SURF and DeiC provide examples that could be used to create a template*)			
NREN providing Secure Internet to guest users	• eduVPN users can also use the server of another NREN where the NREN provides the Secure Internet service including guest access. • It is a requirement of the policy to enable guest access for Secure Internet • The NREN not only processes the data of its own institutions but also the 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 • The NREN's Privacy Policy should address guest use and data processing by an NREN other than the user's 'own' NREN . • The eduVPN confederation policy setting out limits on the personal data processed.	The NREN that offers Secure Internet can be regarded as a 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 for the users of other NRENs than for its own users. This will depend on the way the other NREN/institution has set up identification/authentication until this is fixed in the policy. The policy should describe and establish limits on the personal data being processed so that NRENs can take responsibility for this. The policy should have strict provisions in place regarding 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 Institute Access on a NREN vpn- server	• The service can be used by institutions to establish a safe encrypted connection between the user of the institution and the institution network. • The service runs on the vpn-server managed by the NREN. This is the case for two NRENs at present. Most institutes deploy their own server. • The institution determines which personal data is required to set up the connection	• Processor	• processing agreement NREN-Institute • service agreement NREN Institute (the relations between the NREN and GÉANT concerning the central server infrastructure are described in this agreement) • Institute' privacy policy	Institutions can decide for themselves whether they want to use eduVPN. The institutions purchase the eduVPN service from the NREN for their own users and/or visitors.

Entity	Tasks and processing of personal data	GDPR role and processing ground	Relevant legal documents	Explanation/questions/comments
	following the authentication method of their choice. • The institution is offered the possibility of managing 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.			
NREN providing Institute Access, Institute deploys its own server	• The NREN provides the connection to the eduVPN backbone, i.e. the user can find the name of the in the client/app to set up a connection to the institute. • The NREN and the Institute establish a connection on the authentication infrastructure provided by the NREN. This connection is out of scope for this overview.	• None	• service agreement NREN Institute • Institute's privacy policy	
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 • Institute's privacy policy	• The participating institutions are responsible for their own organisational and technical implementation of eduVPN. • Technical and organisational requirements should be met to ensure the proper use and quality of the service (servers should be responsive, software up to date etc.).There should be a recommendation concerning personal data, for instance stating that institutions will as a preference use attributes that are not directly reducible to users identities, e.g. student numbers.
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	• An MoU about trademark usage, software governance etc. should be signed between the Commons Conservancy and GÉANT	
SURF	• Client App releases • Privacy by design principles: no tracker or telemetric functions • High-level statistical data from MS, Google and Apple	• none		Task to be transferred to GÉANT or the Commons Conservancy