Technical and organizational measures / security concept and sub processors

GIREVE Roaming Platform, GIREVE Trust Platform and GIREVE Digital Portal are hosted by GIREVE's providers on servers established in the European Union and Switzerland. GIREVE undertakes to ensure that its hosting providers: (i) implement all the technical means, in accordance with practices required to ensure the logical security of the access to the GIREVE Roaming Platform, GIREVE Trust Platform and GIREVE Digital Portal, as well as to prevent any intrusion from unauthorised persons, whatever the nature or technique used; (ii) undertake to restrict the access to the server center of the GIREVE Roaming Platform, GIREVE Trust Platform or GIREVE Digital Portal, and to implement an internal procedure to ensure that unauthorised persons may not access that room.

Within the scope of the Agreement and its Appendix 6 "Protection of Personal Data", the following technical and organizational measures (TOMs) including a corresponding security concept are agreed between the Data controller (The Contracting Party) and the Data processor (GIREVE).

1 Measures for the pseudonymization and encryption of personal data

1.1. Encryption

Encrypting personal data is a common way to protect it against being read by unauthorised persons. In particular, encryption is suitable to protect data against outside influences such as hacking and espionage. Encrypting means a process by which clearly legible information is converted to a sequence of characters which cannot be read or interpreted. Measures in connection with the encryption of personal data:

☒Encryption of confidential data during transport and over data networks

☒Secrecy of the private keys of a certificate

2 Measures to ensure confidentiality

Among others, measures regarding the implementation of the mandate of confidentiality are those which are part of admission and access control or access inspection. The technical and organizational measures should ensure adequate safety of personal data including protection against unauthorised or illegitimate processing and against unintentional destruction or unintentional damages.

2.1. Physical access control

[redacted]Physical access to business rooms of Data processor

This means measures preventing unauthorised individuals to enter buildings of Data processor in which personal data are processed.

☒Definition of authorised people

☒Access control System with personalized badge reader, magnetic card or Chip card including access code, personally given keys

☒Definition of access rules of external people

☒Documentation about granting and revocation of access authorisations

☒Restrictive key allocation

☒Visitors stays only accompanied by associates of the Data processor

[redacted]Physical access to data centers of Data processor

Additional implemented measures to prevent unauthorised individuals to enter data centers of Data processor in which personal data are processed.

☒Logging of access to server rooms (automatically by access control system or by designed lists)

☒Video surveillance in server room

☒Door status monitoring for server room

☒Automatic door pull-in device for entrance and exit in server rooms

☒Stays of external companies / technicians in server rooms only under the constant supervision of employees of the contractor

2.2. Logical access control

This means measures to prevent unauthorised individuals using the data processing systems and processes.

☒Defaults for setting passwords:

☒	Minimum length
☒	Usage of characters, special characters (including numbers)
☒	Use of trivial passwords
☒	Regular change of the password
☒	Prohibition of password transfer
☒	Rules for storage and transfer in data processing systems

☒Defaults of the password management applications to use

☒Locking the screen in case of inactivity by time
☒Regular renewal of access authorisations for user access to the network of:

☒	Employees
☒	Externals

☒Regular conditional access checks for administrators of:

☒	Network and network services
☒	Server
☒	Risk identified applications

☒Isolation of internal networks by setting up firewall systems
☒Usage of on Virtual Private Networks (VPN) with User/password as authentication criteria

2.3. Data access control

This means measures ensuring that individuals authorised to use the data processing systems can only access data within the scope of their access authorisation. Measures must be taken that personal data cannot be read, copied, changed or erased without authorisation during processing, use and after storage.
☒Usage of individualized and user related authorisation information
☒Differentiated authorisation concept based on data and application level (roles)
☒Logging of granted authorisations

2.4. Separation control

This means measures to ensure that data collected for different purposes are processed separately.
☒Logical data separation or internal multi-client capability
☒User profiles
☒Access authorisations

3 Measures to ensure integrity

On the one hand, measures for implementing the requirement of integrity are those which are also part of input control, on the other hand, however, those which generally contribute to the protection against unauthorised or illegitimate processing, destruction or unintentional damaging.

3.1. Transfer control

This means measures to ensure that personal data cannot be read, copied, changed or erased without authorisation during electronic transmission, transport or storage on data carriers, and that it can be verified and determined at which locations a transfer of personal data by data transmission installations is intended.
☒Encrypted transmission protocol, especially on public transmission (i.e. ssl, tls)
☒Usage of virtual private networks (VPN)
☒Privacy compliant disposal of data, data carries and print outs based on the security concept
☒Careful selection of transport staff

3.2. Input control

This means measures to ensure that it can be checked and determined afterwards whether and by whom personal data in data processing systems and applications have been entered, changed or erased.
☒Legal form of contracts for the data processing of personal data with subprocessors, including appropriate regulations for control mechanisms
☒Procuring self-disclosures from service providers with regard to their implementing the data protection law
☒Written (including via mail) confirmation of oral instructions
☒Use of logging and logging analysis systems
☒Determining authorised persons preparing data carriers and editing data

4 Measures to ensure availability and resilience

4.1. Availability control

This means measures ensuring that personal data are protected against incidental destruction or loss. These measures must be designed in a way to ensure permanent availability.
☒Central purchasing of software and hardware
☒Usage of centrally approved and released standard software from secure sources
☒Regular back-up-process or mirror hard disks, e.g. RAID-procedure

☒Decommissioning of hardware (especially of servers) takes place after testing the data carriers used therein and, if necessary, after backup of the relevant data sets.
☒Uninterrupted electricity supply in server rooms
☒Multilayer antivirus and firewall architecture
☒Emergency planning (emergency plan for security and data protection violations including specific handling instructions)
☒Early alert system for fire, water and high temperature in server rooms
☒Fire doors
☒IT supervision by qualified employees who are trained continuously
☒Regular testing of data recovery in accordance with the data protection concept

4.2. Order control

This means measures to ensure that personal data processed by a sub processor of the contract data processor are processed only in accordance with the processor's instructions and requirements.
☒Define criteria for selecting sub processors (references, certifications, seals of quality)
☒Detailed written regulations (contract/agreement) of the assignment relationship and formalization of the entire sequence of the assignment including the use of sub processors, clear regulations regarding competencies and responsibilities
☒Ensuring that contract data processing is controlled and documented
☒Contractual agreement with sub processors to commit both internal and external staff to data secrecy

4.3. Resilience

This includes for example measures, that must already be taken before the contract data processor starts to process the data. In addition, continuous monitoring of the systems is required.
☒Load-Balancing
☒Dynamic processes and connection of extra storage
☒Regular stress tests of the data processing systems
☒Define the stress limit for the respective data processing system above the necessary minimum
☒Regular training of the staff deployed (both management and other internal or external employees) to act in accordance with the requirements of integrity and confidentiality of data processing (at least once a year)

5 Measures to quickly restore the availability

In order to ensure recoverability, sufficient safeguards as well as plans for measures are required with which running operations can be recovered in case of disaster scenarios (if necessary, also the basis of the safeguards).
☒Back-up concept
☒Redundant data storage
☒Double IT infrastructure for processes with high availability requirements
☒Backup data center

5.1. Procedures for periodical review, assessment and evaluation

A regular review, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure the safety of processing shall be carried out in the framework of the implementation of:
☒Internal audits by the relevant authorities (e.g. auditors, data protection officers, information security officers, process controls through quality management

6 Subprocessor of the Data processor

	Company name, contract partner for data protection questions	Content of assignment	Place of data processing	Transmission of / access to personal data of the Data controller
1	Rampar Bâtiment Crisco Duo, 7 avenue de la Cristallerie 92310 Sèvres, France Contact partner: dpo@rampar.com	IT hosting and monitoring	• Paris area (France) • Geneva area (Switzerland)	Transmission and storage.
2	Google Cloud Platform Contact : https://support.google.com/cloud/contact/dpo.	IT hosting	Europe (EU)	Transmission and storage.
3	Niji 14 bd des Frères Voisin 92 130 Issy-les-Moulineaux, France Contact: dpo@niji.fr	Information System low level design, coding for and systems creation and maintenance	• Issy-les-Moulineaux (France), • Rennes (France)	Access