Protection of Personal Data

1 Preamble

GIREVE acknowledges the strategic and strictly confidential nature of the personal data. As a consequence, GIREVE undertakes to comply with the rules applicable in France and in the European Union regarding the protection of personal data ("personal data protection rules"). GIREVE undertakes to implement all necessary procedures to ensure their confidentiality and utmost security.

2 Description of processing

GIREVE may be required to process personal data in the context of the processing operations described in the table below.

Processing		Description	Purpose	GIREVE 's role (GPDR)
IOP Interoperability Platform	Authentication-Data	Data: List of identifiers of Clients of an eMSP, who subscribed to the Access Service. Process: Reception from eMSP and storage in GIREVE's Roaming Platform. Could be transmitted to CPO.	To ensure the proper execution of GIREVE Services	Processor, subcontractor of eMSP
			To transfer this authentication-data to CPOs connected to GIREVE's Roaming Platform and who have a Roaming Agreement with the eMSP	
			After anonymisation of the data, to carry out processing for statistical purposes and to improve GIREVE Services	
	Service Session	Data: A service session is a set of data that represents the provision of the service to the Client. It contains the Client's identification and other descriptive information (e.g.: charging start and end date, etc.) Process: Reception from CPO and eMSP, and storage in GIREVE's Roaming Platform. Could be transmitted to eMSP and to CPO.	To allow the mechanisms for service authorisation and registration of such authorisations	Processor, subcontractor of CPO and eMSP
			To allow the collection of service usage information (charging time, energy charged...) for B2B and B2C billing	
			To forward this information to the CPO and the eMSP for service tracking and billing purposes	
			To allow the invoicing of Operators by GIREVE.	
			After anonymization of the data, to carry out processing for statistical purposes and to improve the GIREVE Services	
	Reservation	Data: A Charging Point reservation is data that mainly includes the Client's identification details, the Charging Point identifier and times and duration of the reservation. Process: Exchanges from and to CPO and eMSP, and storage in GIREVE's Roaming Platform.	To enable the reservation mechanisms for Charging Points	Processor, subcontractor of CPO and eMSP
			To enable the collection of service usage information relating to the reservation service for B2B and B2C billing	
			After anonymization of the data, to carry out processing for statistical purposes and to improve the GIREVE Services	
			To allow the provision of neutral factual elements in the event of a dispute or recourse between two Partners.	

Processing		Description	Purpose	GIREVE 's role (GPDR)
Trust Services for ISO 15118 and Plug & Charge	ISO15118-P&C Vehicle Provisioning Certificate Issuance	Data: The Provisioning Certificate contains the PCID (Provisioning Certificate Identifier) which is an alias of the vehicle identifier (VIN) which is considered as a personal data. Process: the PCID is received from the OEM and is include inside the generated x509 certificate.	To allow Provisioning Certificate issuance. This certificate is mandatory for the ability of the vehicle to activate the Plug&Charge feature.	Processor, subcontractor of OEM
	ISO15118-P&C Provisioning Certificate Pool	Data: The Provisioning Certificate contains the PCID (Provisioning Certificate Identifier) which is an alias of the vehicle identifier (VIN) which is considered as a personal data. Process: Provisioning Certificate is received from the OEM or its subcontractor and is stored in the Provisioning Certificates Pool, in order to be available for transmission to eMSP	To forward Provisioning Certificate to the eMSP of the end user. This certificate is mandatory for the ability of the user to activate the Plug&Charge feature, for its eMSP contract, on a given vehicle.	Processor, subcontractor of OEM
	ISO15118-P&C Contract Certificate Issuance	Data: The Contract certificate contains the eMAId (eMobility Account Identifier) which identifies the contract between the end-user and its eMSP. This eMAId is usually assigned to a physical person, and thus is considered as a personal data. Process: the eMAId is received from the eMSP and is include inside the generated x509 certificate.	To allow Contract Certificate issuance. This certificate is mandatory for the ability of the user to activate the Plug&Charge feature and to associate it to its eMSP account.	Processor, subcontractor of eMSP
	ISO15118-P&C Contract Certificate Pool	Data: The Contract Certificate contains the eMAId (eMobility Account Identifier) which identifies the contract between the end-user and its eMSP. This eMAId is usually assigned to a physical person, and thus is considered as a personal data. Process: Contract Certificate is received from the eMSP or its subcontractor and is stored in the Contract Certificates Pool, in order to be available for transmission to CPOs and OEM.	To forward Contract Certificate to the OEM of the vehicle for which this certificate has been created. To forward Contract Certificate to any CPO connected to the Contract Certificate Pool, in order for them to make this certificate available for the vehicle.	Processor, subcontractor of eMSP

Processing		Description	Purpose	GIREVE 's role (GPDR)
All Services	Traces of technical exchanges	Data: any data contained in exchanged messages from or to partners. See details above. List below as a reminder: • List of identifiers of Clients of an eMSP • Service session description (and the related user Id) • Booking of a charging point (and the related user Id) Process: Reception from CPO and eMSP, and storage in GIREVE's Roaming Platform.	To enable maintenance, monitoring and diagnostic To allow the provision of neutral factual elements in the event of a dispute or recourse between two Partners.	Processor, subcontractor of OEM, CPO and eMSP

3 Duration

The duration of the processing carried out by GIREVE is limited to the duration of performance of the services provided for in the Agreement and cannot in any event exceed the duration of the Agreement plus the applicable statutory limitation periods.

4 Warranties

GIREVE warrants the Contracting Party the compliance with its statutory and regulatory obligations, in particular those under the personal data protection rules and compliance with the obligations under this Appendix.

The Contracting Party will carry out any prior formalities required under the personal data protection rules with a supervisory authority and will inform the data subjects concerned by the processing of personal data, where applicable.

5 Obligations of the processor

GIREVE undertakes to take all necessary measures pertaining to the compliance by itself and by its personnel with its obligations and especially:

- not to process or consult the data except within the framework of the documented instructions and authorisations received from the Contracting Party, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by a mandatory rule resulting from Union or Member State law to which GIREVE is subject; in such a case, GIREVE shall inform the Contracting Party of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- take all measures to help prevent abusive, malicious or fraudulent use of the data and files;
- immediately inform the Contracting Party if, in its opinion, an instruction infringes the personal data protection rules.

The Parties agree that an instruction shall be deemed to be given where GIREVE acts within the framework of this Appendix and the Agreement.

GIREVE further undertakes to take into account the nature of the processing and to implement appropriate and reasonable measures to assist the Contracting Party, by appropriate technical and organisational measures, insofar as this is possible in:

- fulfilling its obligation to respond to requests for exercising the data subject's rights (in particular, right of access, right to rectification or erasure, right to restriction of processing, right to object or right to portability);
- ensuring compliance with its obligations concerning security, notification of personal data breaches to supervisory authorities and communication of personal data breaches to data subjects, impact assessment, and prior consultation (in accordance with Articles 32 to 36 of European Regulation 2016/679), taking into account the nature of processing and the information available (GDPR, Art. 28(3)(f)).

6 Security

In accordance with the personal data protection rules, GIREVE undertakes to take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and files and, in particular, prevent their distortion, alteration, damage, accidental or unlawful destruction, loss, disclosure and/or access by third parties not previously authorised.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,

GIREVE shall implement appropriate technical and organisational measures to protect personal data and ensure a level of security appropriate to the risk.

The means used by GIREVE to ensure the security and confidentiality of the data are described below:

- physical security:
  - Data centre access is protected. An internal procedure and material means are put in place to ensure that no outsider or unauthorised person can access this room.
  - Physical access to GIREVE's premises is protected (double secret code).
- logical security:
  - GIREVE guarantees that it has taken into account the computer security requirements and undertakes to implement all technical means in accordance with the state of the art, necessary to ensure the logical security of access to computer applications and hosted data and prevent any intrusion by unauthorised persons, whatever the nature or technique used.
  - All critical systems, i.e. systems hosting critical features, are redundant.
  - A data backup plan is defined, implemented and monitored.
  - A major disaster recovery plan is defined.
  - All flows are encrypted. Access to the interoperability platform by operators' and partners' systems is protected by IP filtering and mutual authentication (client certificate) for eMIP flows and by an exchange of communication-tokens for OCPI flows.
  - All flows are traced. These traces contain the time stamp of the flow, its sender and recipient, and the feature nature of the exchange.
  - Any access via man-machine interface is encrypted and password protected.
  - Application access rights are assigned to the actors as strictly necessary and are based on role and user profile management.
  - All workstations are protected by regularly and automatically updated anti-virus software.

- organisational security:
  - The employment contracts of GIREVE employees include confidentiality and workstation usage clauses.
  - The subcontracting contracts with companies in charge of the hosting, supervision and maintenance of the systems include clauses relating to security and confidentiality.
  - GIREVE may change the means used to ensure the security and confidentiality of data and files. In this case, GIREVE undertakes to replace them by means that are at least equivalent.

The Contracting Party may also require amendments to the security and confidentiality measures, if required by law, authorities or internal auditors.

In case of a data protection audit conducted by the Contracting Party itself at GIREVE, any change of any means used to ensure data security and confidentiality may be raised. The Contracting Party undertakes to specify the special security measures that it considers necessary in relation to the nature and risks associated with the treatment. The implementation of these special security measures by GIREVE will result in an analysis, especially in terms of technical compatibility and feasibility, and, if appropriate, a quotation.

7 Data breach

GIREVE agrees to notify the Contracting Party without undue delay after having become aware of any personal data breach, namely a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This notification must be sent to the person designated as the legal contact of the GIREVE's Identification Form, by email. It will describe, where possible, the nature and consequences of the personal data breach, and the measures already taken or proposed to be taken to address the personal data breach.

GIREVE undertakes to actively collaborate with the Contracting Party to ensure that they are able to meet their regulatory and contractual obligations. As the controller, the Contracting Party is solely responsible for notifying the data breach to the competent supervisory authority and, where applicable, to the data subjects.

8 Sub-processing

GIREVE may not engage another processor ("sub-processor"), within the meaning of the personal data protection rules, for all or part of the services, especially to a country which is not a Member of the European Union, without having obtained the prior, written and express agreement of the Contracting Party.

The Contracting Party authorises GIREVE to engage sub-processors for the hosting services, supervision and maintenance of the solutions.

The authorised sub-processors are bound by a sub-data processing agreement with GIREVE which reflects the obligations of this appendix.

GIREVE may, at its sole discretion, revoke, replace or appoint sub-processors subject to informing the Contracting Party by email and giving the Contracting Party the opportunity to object to such changes.
Where its sub-processors fail to fulfil their data protection obligations, GIREVE shall remain fully liable to the Contracting Party for the performance of those sub-processor's obligations.

9 Transborder data flows

For any transfer of personal data to a third county, not belonging to the European Union, or to an international organisation, GIREVE must obtain the prior written authorisation of the Contracting Party. If such authorisation is granted, GIREVE undertakes to cooperate with the Contracting Party to ensure:
- compliance with the procedures for complying with the personal data protection rules, for example in case an authorisation from the CNIL is required;
- where applicable, the conclusion of one or more agreements to regulate such transborder data flows. GIREVE particularly undertakes, if needed, to sign such agreements with the Contracting Party and/or to obtain the conclusion of such agreements from its sub-processors. To this end, the Parties agree that the standard contractual clauses issued by the European Commission will be used to provide a framework to transborder data transfers.

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

10 Maintenance of a record

As a processor, GIREVE undertakes to maintain a record of all categories of processing activities carried out on behalf of the controller, in accordance with the provisions of the General Data Protection Regulation. GIREVE will make the record available to the Contracting Party on request.

11 Storage of data

At the end of the Agreement, GIREVE undertakes to return the files and data containing personal data to the Contracting Party under the conditions stipulated by the Contracting Party and then to delete all manual or computerized files that store the personal data collected, unless a mandatory rule resulting from Union law or Member State law applicable to the processing operations hereunder requires otherwise.
GIREVE has the right to keep the anonymised data for statistical processing purposes, including at the end of the Agreement.
If Union law or Member State law requires the storage of personal data, GIREVE shall inform the Contracting Party of this requirement.

12 Cooperation

GIREVE undertakes to cooperate with the Contracting Party to ensure:
- the management of requests related to the exercise of data subjects' rights and notably of their right of access to their data. If a data subject contacts GIREVE directly to exercise his or her rights of access, rectification, deletion and/or objection or for any other request related to the protection of personal data, GIREVE will communicate to the Contracting Party the requests received without undue delay. GIREVE may respond to the request of a data subject only on instructions from the Contracting Party;
- the making available all the information necessary to demonstrate compliance with the rules provided for in this Appendix.
- the conduct of a data protection audit by the Contracting Party; GIREVE undertakes to respond to the Contracting Party's audit requests made either by itself or by a trusted third party appointed by it, recognised as an independent auditor;
- the carrying out of an inspection by a competent authority at GIREVE or at the Contracting Party and relating to the processing which are the subject matter hereof;
- the carrying out of any impact assessment that the Contracting Party would decide to carry out, in order to assess the risks of the processing to the rights and freedoms of natural persons and to identify the measures to be implemented to deal with these risks, and the consultation with the supervisory authority.