Belvédèrestraat 29 | 1050 Elsene, Belgium
E: privacy@skipr.co

DATA PROCESSING POLICY – SKIPR

Last version: April 2022

Hi! Welcome to Skipr! We are glad you use our solution in order to enable your organisation to set up and implement a future proof Mobility Plan.

Using the Skipr web app and mobile app leads to the processing of personal data by Skipr. Therefore, we have adopted this Data Processing Policy that we kindly request you to read.

You can be reassured that we will process the personal data in the best interest of your organization and employees. By reading this policy, you will be properly informed about our legal responsibilities with regard the the processing of personal data and the security measures we have adopted in order to ensure the personal data is processed in a safe way.

1. INTRODUCTION

Skipr NV/SA is a company incorporated and existing under the laws of Belgium, with registered office at BE-1050 Elsene, Belvédèrestraat 29, with VAT/company number BE-0712537.551 (hereinafter '**Skipr'**, '**we'** or '**us'**).

When you (hereinafter '**you'** or the '**Customer'**) rely on the Skipr Platform and/or App, Skipr:

- shall have access to Personal Data; and,
- will have to Process Personal Data on your behalf.

This Data Processing Policy (hereinafter: the '**Policy'**) applies to the Processing of Personal Data by Skipr for the Customer and determines:

- how Skipr will manage, secure and process the Personal Data; and,
- Both parties' obligation to comply with the Privacy Legislation.

By relying on the Services of Skipr, you acknowledge to have read and accepted this Policy and consequently the way Skipr processes the Personal Data.

2. DEFINITIONS

In this Policy, the following concepts have the meaning described in this article (when written with a capital letter):

App	the mobile app developed by Skipr through which the End-User can organize its intermodal travel;
Controller	the entity (being in this case: the **Customer**), which determines the purposes and means of the Processing of Personal Data;
Data Importer	the recipient of personal data/processor of Skipr in a third country, which is not subject to an adequacy decision of the European Commission;
Data Subject	the natural person to whom the Personal Data relates, as identified in **Annex I**;
Data Breach	unauthorised disclosure, access, abuse, loss, theft or accidental or unlawful destruction of Personal Data;
End-User	the people affiliated with the Customer that are allowed to use the Platform and the App (mainly employees and independent contractors);
Personal Data	any information relating to an identified or identifiable natural person (i.e. the Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Platform	the platform developed by Skipr used mostly by the Customer its fleet manager or HR-manager to manage/organise the mobility plan of the Customer (e.g. manage mobility budget and cards, approve expenses, etc.);
Privacy Legislation	**(i)** the Belgian Privacy Act of July 30, 2018; **(ii)** the General Data Protection Regulation 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ('GDPR'); **(iii)** Directive 2002/58/EC of the European Parliament and Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector ('e-privacy directive') (including all future legislative changes and amendments/revisions thereof; and/or **(iv)** all (future) applicable national laws regarding the implementation of the GDPR;
Process/Processing	ny operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, including, but not limited to: collection, recording, organisation, structuring, storage,

	adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data;
Processor	the entity (being in this case: **Skipr**) which Processes Personal Data on behalf of the Customer as Controller;
Services	all services, provided by Skipr to the Customer implying the Processing of Personal Data, including but not limited to: providing a right of access to the Platform, a license to the App and all support related thereto;
Sub-processor	any processor engaged by Skipr.

The Policy includes the following annexes:

Annex I	Overview of **(i)** the Personal Data, which parties expect to be subject of the Processing, **(ii)** the categories of Data Subjects, which parties expect to be subject of the Processing, the **(iii)** retention period for each Processing; and **(iv)** the use (i.e. the way(s) of Processing) of the Personal Data, the purpose and means of such Processing;
Annex II	Overview and description of the security measures taken by Skipr in order to protect the Personal Data that are being processed during the performance of the Services.

3. USE OF THE SERVICES

3.1 Parties agrees that:

- In accordance with the Privacy Legislation, the Customer shall be considered the 'Controller' and Skipr the 'Processor'.
- Skipr acts as a facilitator of the Services. Therefore, the Customer shall be responsible on how and to what extent it makes use thereof;
- The Customer is responsible for all acts and ommissions of the End-Users (i.e. in case the End-User does (not) take sufficient measures to protect its account on the App/Platform);
- Skipr allows the Customer to make adjustments and/or changes to the Personal Data and shall never consult or adjust these Personal Data itself, unless the Customer requests Skipr to do so;
- The Customer is responsible for the material and/or data provided by the Data Subject. The Customer is, as Controller, thus responsible for complying with the Privacy Legislation and/or any other regulations with regard to aforementioned material and/or data;
- The Customer shall comply with all laws and regulations (such as but not limited with regard to the retention period or rights of the Data Subject (cf. **Article 11**)) imposed on it by making use of the Services.

3.2 The Customer shall avoid any misuse of the Services, the Platform and/or the App. In case of misuse by the Customer or the End-Users, the Customer agrees that Skipr can never be held liable in this respect nor for any damage that would occur.

4. OBJECT

4.1 The Customer acknowledges that as a consequence of making use of the Services, Skipr shall Process the Personal Data.

4.2 Skipr shall always Process the Personal Data in a proper and careful way and in accordance with the Privacy Legislation and other applicable rules concerning the Processing of Personal Data.

More specifically, Skipr shall adopt all necessary security measures (cf. **Annex II**) and provide all its know-how in order to perform the Services in accordance with the rules of art.

4.3 Skipr assures that itshall only Process the Personal Data upon the Customer's request and in accordance with the latter's instructions unless any legal obligation states otherwise.

4.4 The Customer keeps full control concerning the following: (**i**) how Personal Data must be Processed by Skipr, (**ii**) the types of Personal Data Processed, (**iii**), the purpose of Processing, and (**iv**) the fact whether such Processing is proportionate.

5. SECURITY OF PROCESSING

5.1 Skipr takes the security of the Processing activities very seriously. Taking into account the state of the art, Skipr implements appropriate technical and organisational measures for the protection of **(i)** the Personal Data – including protection against careless, improper, unauthorised or unlawful use and/or Processing and against accidental loss, destruction or damage – **(ii)** the confidentiality and integrity of Personal Data, as set forth in **Annex II**.

6. SUB-PROCESSORS

6.1 The Customer agree that Skipr may engage third-party Sub-processors in connection with the performance of the Services. In such case, Skipr shall ensure that the Sub-processors are at least bound by the same obligations by which Skipr is bound under this Policy.

6.2 The current Sub-processor(s) on which we appeal for the performance of the Services are listed on here: [hyperlink] , which includes the identities of those Sub-processors and their country of location.

Skipr shall update the list whenever a Sub-processor changes (e.g. a new Sub-processor was added, a Sub-processor was substituted, etc.) and will notify the Customer when (significant) changes are made. If you wish to exercise its right to object, please notify Skipr in writing by the latest within thirty (30) days after the list was updated.

6.3 If the objection is well founded, Skipr will use reasonable efforts to **(i)** make available a change in the Services or **(ii)** recommend a commercially reasonable change to the Customer's use of the Services to avoid Processing of Personal Data by the objected new Sub-processor without unreasonably burdening the Customer.

If Skipr is, however, unable to make available such change within a reasonable period of time (which shall not exceed thirty (30) days following your objection), you may terminate the the Services if:

- You cannot use the Services without appealing on the objected new Sub-processor;
- Such termination only concerns the Services which cannot be provided by Skipr without appealing to the objected new Sub-processor;
- You notify Skipr of your wish to terminate the the Services to Skipr within a reasonable time.

6.4 Skipr takes responsibility for the acts and omissions of its Sub-processors to the same extent as if it would be performing the Services itself, directly under the terms of this Policy.

7. TRANSFER TO third PARTY CONTROLLERS

7.1 The Customer acknowledges that when requesting a Service – in particular, a specific mobility service (e.g. car rental) – via the App, Personal Data may be transferred by Skipr to third party controllers (such as, mobility transport providers) in order to enable the correct execution of the requested Service. Hence, the Customer recognizes that Skipr shall act as an intermediary party between the Customer and such third party controllers. In that light, the Customer hereby accepts that Skipr may transfer Personal Data (cf. **Annex I**) for the performance of the Services to the third party controllers identified here: [hyperlink].

8. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

8.1 Skipr assures the Customer that a transfer of personal data to a third country or international organisation shall always be subject to **(i)** an adequacy decision by the Commission or **(ii)** one of the following safeguards:

- Closing a **data transfer agreement** with the third country recipient, which shall contain valid standard contractual clauses ('**SCC**'), as adopted by the European Commission. Before the transfer takes place, the Data Importer has to guarantee Skipr that an adequate level of privacy compliance is ensured in this third party country; and/or;
- **Binding corporate rules**. As it is the case for standard contractual clauses, the Data Importer has to guarantee Skipr that an adequate level of privacy compliance is ensured in the third party country; and/or;
- **Certification mechanisms**.

8.2 Every transfer to a third country or international organisation, not recognized by an adequacy decision, is subject to **an assessment by Skipr** to determine if there is anything in the law and/or practices in force of said third country that may infringe on the effectiveness of the appropriate safeguards in place (as identified above).

Where required on the basis of aforementioned assessment, Skipr shall identify and implement **appropriate supplementary measures** to govern any data transfer to such international organization or a third country without adequacy decision to ensure the level of data protection as required by EU law.

Furthermore, Skipr shall take all reasonable efforts to oblige the Data Importer to implement sufficient guarantees and measures to protect the Personal Data and ensure the effectiveness of the protection of the SCC's, binding corporate rules and/or certification mechanisms.

8.3 In case of non-compliance by a Data Importer or where protections in the third country are not adequate, Skipr shall – at its sole discretion - either:

- Suspend the transfer of Personal Data to the Data Importer / such third country until the issue has been solved; or,
- Terminate the transfer of Personal Data to the Data Importer / such third country and request the Data Importer to delete the Personal Data in its possession.

8.4 In practice, Skipr performed/added some additional checks to its process:

- **Data mapping**: Skipr mapped all of its data flows (in particular, with regard to data transfers to third parties/countries);
- **Contact with (Sub-)processors**: Skipr contacted the Data Importers to ensure that the Processing is carried out in accordance with the agreements made and with the requirements from the Schrems II-decision.
- **Transfer tool identification:** Skipr re-assessed the transfer tools (e.g. European Commission's adequacy decisions, Standard Contractual Clauses…) it or its (Sub-)processor relies on to transfer Personal Data to (Sub-)processors located in third countries;
- **Legal assessment of recipient country -** Skipr is assessing the privacy laws of all third countries to which Personal Data is being transferred. Accordingly, Skipr wishes to establish if these third country recipients provide adequate and effective data protection;

- **Adequacy assessment -** Skipr is requesting (Sub-)processors that are transferring Personal Data to third countries (in which effective protection equal to the GDPR cannot be guaranteed, such as the United States) to provide an overview of the supplementary measures they have taken or intend to take to ensure the safety and security of the data transfer and Processing.
- **EEA alternatives –** Prior to each transfer of PPersonal DData to a third country (especially where no equivalent level of data protection can be guaranteed) Skipr will assess the necessity of such data transfer by investigating whether there are no alternative options or parties that would ensure that the data is being Processed within the European Economic Area ("**EEA**");
- **Vendor cooperation assessment -** Skipr will terminate the cooperation with (Sub-)processors transferring Persona lData to or located in third countries that are unable to guarantee an equivalent level of data protection.
- **Other procedural & organisational steps -** upon finalising the vendor assessment, Skipr will implement the necessary procedural and organisational steps;
- **Periodic monitoring & evaluation -** Skipr endeavours to evaluate on an ongoing basis the transfer of Personal Data to third countries (with regard to necessity, compliance, security…). This includes monitoring developments in such countries that could affect the (earlier) assessments made by Skipr.

9. CONFIDENTIALITY

9.1 Skipr shall maintain the Personal Data confidential and thus not disclose nor transfer any Personal Data to third parties, without your permission, unless when such disclosure and/or transfer is required by law or by a court or other government decision (of any kind). In such case Skipr shall, prior to any disclosure and/or announcement, inform you in full transparency on the scope and manner thereof.

9.2 Skipr ensures you that its personnel, engaged in the performance of the Services, is informed of the confidential nature of the Personal Data, are well aware of their responsibilities and are bound by written confidentiality agreements. Skipr ensures that such confidentiality obligations survive the termination of the employment contract.

9.3 Skipr ensures you that the access of its personnel to the Personal Data is limited to such personnel performing the Services in accordance with the Policy.

10. NOTIFICATION

10.1 Skipr will use its best efforts to inform you as soon as reasonably possible when it:

- Receives a request for information, a subpoena or a request for inspection or audit from a competent public authority in relation to the Processing of Personal Data;
- Has the intention to disclose Personal Data to a competent public authority;
- Determines or reasonably suspects a Data Breach has occurred in relation to the Personal Data.

10.2 In case of a Data Breach, Skipr:

- Notifies you without undue delay after becoming aware of this Data Breach. In the event you wish so, Skipr shall provide – to the extent possible – assistance with respect to your reporting obligation under the Privacy Legislation;
- Undertakes – as soon as reasonably possible – to take appropriate remedial actions to make an end to the Data Breach and to prevent and/or limit any future Data Breach.

11. RIGHTS OF DATA SUBJECTS

11.1 Skipr shall promptly notify you if it receives a request from a Data Subject invoking its privacy rights under the Privacy Legislation. Skipr shall not respond to any such data subject request without your prior written consent.

11.2 If a Data Subject requests to exercise his/her rights, you must assist the Data Subject in its request. Only if you do not have the ability to correct, amend, block or delete the Personal Data (as required by Privacy Legislation), Skipr shall assist you (as long as commercially reasonable).

12. LIABILITY

12.1 Parties are each individually liable towards authorised supervisory authorities and/or Data Subjects for claims and/or fines that are the result of their own breach of or non-compliance with **(i)** the provisions of this data processing policy, and **(ii)** the Privacy Legislation or other applicable rules concerning personal data. Skipr and the Customer indemnify each other in this regard.

12.2 The liability of Skipr for a breach of this data processing policy is limited as described in the applicable contractual documentation (i.e. the B2B Terms and Conditions).

13. RETURN AND DELETION OF PERSONAL DATA

13.1 Upon termination of the Services, the accounts of the Customer will be deactivated and the Personal Data shall no longer be available for the Customer. You can request to receive an export of its data. In any event, Skipr may, at its sole discretion, determine the format of the export.

13.2 Skipr shall retain the Personal Data for six months to ensure export or reactivation request of the Customer can be fulfilled. Skipr shall never access the inactive Personal Data. As soon as the six months ends, Skipr will anonymise the Personal Data, which will then solely be used for improvement of the Platform/App and statistical purposes.

13.3 In case a Data Subject's profile is being removed from the solution by the Customer, all Personal Data relating thereto will immediately be anonymised as well.

13.4 All the foregoing does not apply, and Skipr may therefore continue to retain the Personal Data if – and only to the extent that – it is required to do so pursuant to a legal obligation imposed on Skipr (e.g. mobility budget).

14. CONTROL

14.1 Skipr is willing to provide you with all information, required to allow verification if we comply with the provisions of this Policy.

14.2 In this respect Skipr shall allow you to carry out inspections – such as but not limited to an audit – and provide the necessary assistance thereto.

15. TERM

15.1 This Policy lasts as long as the Services have not come to an end.

16. UPDATES

16.1 This Policy may be updated from time to time by Skipr, in which case Skipr shall notify you through its website or the App/Platform. In any event, the latest version of this Policy can always be accessed on the Skipr website, as well as on the App/Platform.

16.2 You can find our archived Policy here: [hyperlink].

17. CONTACT | DPO

17.1 Skipr has appointed a Data Protection Officer (or "**DPO**") to ensure its compliance with Privacy Legislation. If you have any questions with regard to this Policy or the manner in which we Process the Personal Data, please contact our DPO via email: privacy@skipr.co.

***

Annexes:

- Annex I – Processing activities
- Annex II – Description of security measures

Belvédèrestraat 29 | 1050 Elsene, Belgium
E: privacy@skipr.co

Annex I – Processing activities

I. DESCRIPTION OF THE PROCESSING ACTIVITIES

CUSTOMER & END-USER ONBOARDING & LIFECYCLE MANAGEMENT (PLATFORM | APP)

|1|PLATFORM

Purpose: Managing the account of the Customer and staff / freelancers / shareholders (being the End-Users) on the Platform, from onboarding (creation of the account) on the Platform until offboarding.

Data Subjects:
- ✔ End-Users of the Platform (Customer and staff / freelancers / shareholders)

Personal Data:
- ✔ First name
- ✔ Last name
- ✔ (Business) email address
- ✔ Company name
- ✔ Home address
- ✔ Proof of address
- ✔ Driver license data
- ✔ Gender
- ✔ Date of birth
- ✔ ID data
- ✔ Phone number
- ✔ Device OS
- ✔ GPS Location
- ✔ User IDs

Retention: For the duration of the Services. Retention up until six (6) months (max.) following termination of the Services.

|2| PUBLIC USERS (APP)

Purpose: Managing account of public users (being the End-Users) in the App, from onboarding (creation of the account) on the Platform until offboarding.

Data Subjects:
- ✔ End-Users of the App

Personal Data:
- ✔ First name
- ✔ Last name
- ✔ (Business) email address
- ✔ Company name
- ✔ Home address
- ✔ Work address
- ✔ Date of birth
- ✔ Gender
- ✔ Phone number
- ✔ Device OS
- ✔ GPS Location
- ✔ User IDs

Retention: For the duration of the Services. Retention up until six (6) months (max.) following termination of the Services.

BOOKING ROUTING REQUESTS / MOBILITY SERVICES

*Please note that the descriptions and retention terms provided below only relate to the Personal Data stored and processed by Skipr within the App or Platform. Depending on the type of rooting request, Personal Data may be transferred to third party controllers (e.g. Poppy, DeLijn, etc.; See: **Article 7**). Skipr has no control over the processing (incl. retention) of the Personal Data by such entities. Please consult their respective privacy documentation for more information.*

|1| ALWAYS REQUIRED

Purpose: Booking, enabling and processing routing requests and mobility services in the App.

Data Subjects:
- ✔ End-Users of the App

Personal Data:
- ✔ First name
- ✔ Last name
- ✔ (Business) email address
- ✔ Geolocation based on IP address (incl. beginning and ending routes taken, routes searched, distance and time and date)

Only when booking:
- ✔ Last four numbers of credit card
- ✔ Gender
- ✔ Reservation information (i.e. date)
- ✔ License plate
- ✔ MOBIB card number
- ✔ Date of birth

Retention: For the duration of the Services. Retention up until six (6) months (max.) following termination of the Services.

|2| ADDITIONAL INFORMATION DEPENDING ON REQUESTED MOBILITY SERVICE

Purpose: Enabling mobility sercices and execution of End User request, payment for requested services, including transfer to mobility partner (bikes, cars, scooters & public transport).

Data Subjects:
- ✔ End-Users of the App

Personal Data:

Bike renting
- ✔ Height

Car & scooter renting (e.g. Poppy)

Confirmation by the driver (i.e. Yes/No; specific or elaborated information is not required) of the following:
- ✔ Driver license
- ✔ Judicial or damage claim data of the last 5 years
- ✔ Mental or physical state allows use of the car or scooter
- ✔ Motor liability insurance
- ✔ Authorized driver approval

Purchasing public transport tickets
- ✔ MOBIB Card number

Retention: For the duration of the Services. Retention up until six (6) months (max.) following termination of the Services.

SUPPORT

|1| USER SUPPORT

Purpose: Providing support to the Customer and/or End-Users regarding (the use of) the Platform and/or App.

Data Subjects:
- ✔ End-Users of the App and Platform

Personal Data:
- ✔ First name
- ✔ Last name
- ✔ (Business) email address
- ✔ Home address
- ✔ Date of birth
- ✔ Gender
- ✔ Phone number
- ✔ Device OS
- ✔ User IDs
- ✔ IP-address

Retention: Until closure of the support request. Data may be further retained in anonymized / statistical format for development and service optimization purposes.

|2| BUG FIXES

Purpose: Analysing and fixing detected bugs in the App.

Data Subjects:
- ✔ End-Users of the App and Platform

Personal Data:
- ✔ Device / phone information (category, brand name, model name, marketing name, operating system (version))

Retention: Until closure of the bug fix has been completed. Data may be further retained in anonymized / statistical format for development and service optimization purposes.

PAYMENT & INVOICING

|1| MOBILITY BUDGET

Purpose: Managing of mobility budget (approve/disprove expense requests, upload money to End-User's budget, etc.).

Data Subjects:
- ✔ End-Users of the App

Personal Data:
- ✔ First name
- ✔ Last name
- ✔ (Business) email address
- ✔ Phone number
- ✔ Booking history
- ✔ Credit card information
- ✔ Expenses

Retention: Seven (7) years (cfr. Belgian regulation on mobility budgets)

|2| MOBILITY CARD

Purpose: Enabling mobility card services and payment for requested mobility services.

Activation mobility card

Data Subjects:
- ✔ UBO of the Customer

Personal Data: Additional information of UBO of company is required
- ✔ First name
- ✔ Last name
- ✔ Copy of ID (incl. picture)
- ✔ Proof of (fiscal) address

	✔ Nationality	✔ Country of birth
	✔ Job title/function	✔ National registration number
	Use of mobility card	
Data Subjects:	✔ End-Users of the App	
Personal Data:	✔ First name	✔ Last name
	✔ Company name (employer)	
Retention:	Seven (7) years	
|3| INVOICING		
Purpose:	Managing of mobility budget (approve/disprove expense requests, upload money to End-User's budget)	
Data Subjects:	✔ Customer's staff (invoicing) or representative	
Personal Data:	✔ First name	✔ Last name
	✔ (Business) email address	✔ Company name (employer)
	✔ Job title/function	
Retention:	Seven (7) years after expiration / payment	

II. THE USE (= WAY(S) OF PROCESSING) OF THE PERSONAL DATA AND THE PURPOSES AND MEANS OF PROCESSING:

	USE OF PERSONAL DATA	
	✔ Collect	✔ Align, combine and create
	✔ Store	✔ Consult
	✔ Structure and analyse	✔ Transfer
	✔ Retrieve	✔ Update
	✔ Consult	✔ Erase and destroy
	MEANS OF PROCESSING	
	✔ Platform	✔ App
	✔ Electronic communication	✔ Third party software (Sub-processors)
	PURPOSE	
	✔ Hosting the Platform	
	✔ Maintaining the Platform/App	
	✔ Supporting the End-User in case of problems/requests	
	✔ Enabling End-Users to:	
	o Book train/bus/metro/etc. tickets	o Rent scooters/cars
	o Plan trips	o Request and use their mobility card
	o Rent bikes	o Manage their mobility budget (approve/disprove expense requests, upload money to their budget,

Belvédèrestraat 29 | 1050 Elsene, Belgium
E: privacy@skipr.co

Annex II – Description of security measures

This document gathers elements of the security context of Skipr. It elicits security objectives, regulation and policies as well as environment threats.

It will be reviewed on a regular basis and will in particular serve as a support for new systems integration and for new features analysis.

1. SECURITY OBJECTIVES

We list here the security objectives that Skipr technical team aims to reach for the system to-be. Those objectives are divided in three categories: confidentiality, availability and integrity. The obje

ctives should enable business to gain confidence in the system to-be to support safely Skipr ambitions in the future.

1. As a web client inside a mobile application
2. As a public API
3. As a web hosted solution

1.1. Confidentality

Confidentiality consists in preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information, to only authorized persons according to their role and function.

Protect information access

- ✔ Skipr End-User
  - o End-User can only access own data through authenticated session
- ✔ Skipr employee(s)
  - o By default skipr employees have no access to End-User data
  - o Exception of Skipr employees with role "technical service"
- ✔ Third party
  - o By default third party have only access to data required for usage of their service (e.g. provider x requires phone number to communicate ticket)
- ✔ External
  - o No external party should be able to access End-User data

Prevent information disclosure

- ✔ Skipr End-User
  - o Not relevant
- ✔ Skipr employee
  - o Should not be able to disclose any End-User personal data
- ✔ Third party
  - o Not relevant
- ✔ External
  - o Not relevant

1.2. Availabilty

Availability consists in ensuring timely and reliable access to and use of information, in compliance with Skipr objectives.

- ✔ The software has to be highly available as it is intended to be used at all times by End-Users.
- ✔ It has to sustain 100 requests per second and scale according to the load as high concurrency as to be expected.
- ✔ Health checks and errors monitoring have to be set and trigger alarms notifications on anomaly detection.

1.3. Intigrity

Integrity consists in guarding against improper information or destruction, and includes ensuring information non-repudiation. Skipr data is expected to be:

- ✔ Attributable – Data ought to demonstrate who handled it, when it was operated and used, and what it is about.
- ✔ Legible – Data ought to be simple, stored permanently and the source should be preserved.
- ✔ Contemporaneous – Data ought to be recorded as it was operated or used, and at the time it was executed.
- ✔ Original – Source information ought to be accessible and protected in its original form.

- ✔ Accurate – There should be no errors on the data, and it should comply with the set protocol.

2. REGULATIONS AND POLICIES

We list here the regulations and policies that the system (to-be) has to comply with. Those regulations and policies are divided in three categories: privacy, financial and IT system security. Privacy is already discussed in this and other policies. Compliance will always be evaluated at different steps of systems development life cycle ('SDLC'):

2.1. Financial

- ✔ AML Principles
- ✔ KYC Compliance
- ✔ PCI - Not required

2.2. IT system security

- ✔ ISO 27001 - No strict compliance but aim to follow the principles.

3. ENVIRONMENT THREATS

We list and classify here the potential threats to which the system to-be could be exposed. The objective is to help feature and development options evaluation regarding security.

Skipr integration is threatened by its environment for its **attractiveness** on the following points:

- ✔ access to End-User data (see GDPR for privacy issue analysis)
- ✔ access to provider service - free ride
- ✔ achieve money laundry

System to-be is **exposed** on the following points:

- ✔ As a mobile application
- ✔ As a public API
- ✔ As a web hosted solution

Skipr integration can be under risk from the following **actors**:

- ✔ Internal by accident
- ✔ Internal with malicious intent
- ✔ External by accident
- ✔ External with malicious intent

Finally, Skipr integration has to mitigate risk on those typical information system category of **threats**:

- ✔ Destruction of information
- ✔ Corruption of information
- ✔ Theft of service
- ✔ Disclosure of information
- ✔ Denial of service
- ✔ Elevation of privilege

4. SECURITY

Our platform implements security by design. In terms of confidentiality, we ensure to only give access to data for which the End-User is authorized by its role. In terms of integrity, we check data for tampering or alteration by unauthorized End-User. In terms of availability, we provide data to authorized End-Users only when they need it. More specifically, we set as an internal practice to follow OWASP security principles:

- ✔ Minimal attack surface area: during the conception phase as well as the implementation of our analyst and developers pay attention to reduce as much as possible impact and scope of the code involved in a new feature.
- ✔ Secure defaults: by default we have set high standards in terms of password and authentication, notably relying on Firebase two factor authentication via text messages.
- ✔ Least privileges: our devops make sure that system as well as physical End-Users and roles on our servers are limited to the strict necessary privileges.

- ✔ Defense in depth: any action in our control interface are log in audit trail, enabling traceability of access and actions per any individual or system.
- ✔ Fail securely: by design our code includes the more restricted privilege and data access as fallback scenario in case of failure.
- ✔ Distrust services: this is particularly true for MSP, our MSP services are the gatekeepers of any data that comes to our Core platform. They ensure compliance of data before any propagation to internal services.
- ✔ Separation of duties: we ensure strict separation of duty notably on the superuser of our control interface that can only act on the systems at system level or for action to correct issue at user level. Superuser has not access to any system that would enable expense or fraudulent usage on behalf of the user.

5. RELIABILITY AND STABILITY OF THE PLATFORM

Our development team is committed to provide code and architecture for the MaaS platform following principles that lead to high standards of quality and security. All platform changes are reviewed by peers through Github, we apply a pull request approach to merge code on master branches to force peer review and therefore increase quality and reduce potential bugs. All the code before being merged is functionally tested with Postman requests collections (automated testing). Code editors of every developer are running code linters that forces alignment of formatting.

We implement alerts and monitoring solution to reduce risk and time of unavailability of the MaaS solution. These measures mitigate the risk of severe degradation of the service. By design, we implement our API for the Mobile application to support degraded mode and therefore limits impact on user side in case of incidents at MaaS platform level. As mentioned in the scalability section, our microservices approach makes it easier to scale up and down to react to peaks of activity without degrading the user experience.

Our recovery procedure allows us to get the whole infrastructure stack and data back online in a matter of minutes. Relying on 3 principles:

- ✔ The data back-up are scheduled on high frequency and safely stored on distributed and reliable cloud storage.
- ✔ The whole infrastructure is defined by configuration files, which means a fully working environment can be spawned by applying the complete set of configuration files
- ✔ The procedure to follow is automated in scripts and fully documented

To ensure stability of the system, our development process follows the principles of continuous integration and deployment. Concretely, we implement unit and functional tests with adequate coverage. Those tests are run in a CI/CD mode at each build of a service and deployment of the service. Furthermore, functional tests run via postman test runner are executed by our CI/CD solution to validate each deployment and prevent regression.

6. SCALEABILITY

The MaaS platform is architectured as micro-services which by essence enable it to scale easily and smoothly as would be required, for example for a large increase in user base. We deploy each microservice in a specific docker instance which allows for scaling of very specific resource at a time. This makes the whole system very flexible but also optimizes cost. The scalability is also supported by the use of a NoSQL mongoDB solution. The NoSQL systems are easier to scale as they are based on documents that can be spread over several instances much more easily than tables of a SQL system. Also our preferred tool MongoDB has built-in support for replication and sharding (horizontal partitioning of data) to support scalability. Finally, as our solution will be deployed on Google Cloud services we benefit from the ability to scale horizontally (adding more servers) and vertically (increasing CPU/RAM power) on demand and automatically based on configurable thresholds.

7. ACCESS PROTECTION

Our load balancer is configured to only allow https connection to our private VPC (kubernetes ingress). Between them, the micro services are communicating through GRPC and do not expose any public IP. The load balancer in front of our cluster is of layer type 7.

Therefore, no direct network access is possible to the services. If further visibility is required on one of those instances, a SSH tunnelling through a bastion service is available for temporary activation.

All credentials and sensitive information are encrypted and stored in google cloud secrets.

Only related services have access to these secrets using a dedicated service-account role.