DATA PROCESSING POLICY OPTIMILE

Last version: August 2023

1 INTRODUCTION

OPTIMILE NV is a limited company with its registered offices at 9000 Ghent, Sassevaarstraat 46 box 201, Belgium, VAT BE-0648.837.849, RPR Ghent, division Ghent.

When OPTIMILE's customer (hereinafter the '**Customer**') relies on OPTIMILE's Platform, OPTIMILE performs Services for the Customer, and in doing so:

- will have access to Personal Data of Mobility Users; and,
- will have to Process Personal Data for which the Customer is responsible as a Controller in accordance with the Privacy Legislation.

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

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

2 DEFINITIONS

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

Assignment/Services:	All activities performed by OPTIMILE on behalf of the Customer and its Associated Companies implying the Processing of Personal Data (including, but not limited to: hosting, providing access to and facilitating the Platform) and any other form of cooperation whereby OPTIMILE Processes Personal Data of the Mobility Users on behalf of the Customer and its Associated Companies;
Associated companies:	Any company associated with a Party, according to Article 1:20 and 1:21 of the Belgian Companies and Associations Code (CAC);
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 OPTIMILE 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;
General Agreement:	The general contractual provisions governing the performance of the Services by OPTIMILE. Depending on the circumstances, this is either the CPO/(e)MSP contract or the terms of service of 'Mobiflow';
Personal Data:	Any information relating to an identified or identifiable natural person (i.e. the Data Subject), within the meaning of Privacy Legislation. In relation to the Assignment/Services, Personal Data shall refer to the information identified in Annex I;
Platform:	OPTIMILE's CPO and/or MSP platform or 'Mobiflow' platform on which the Customer relies to offer mobility services (which may vary on the basis of the contractual arrangements between OPTIMILE and the Customer, such as Charging-as-a-Service (CaaS) and/or Mobility-as-a-Service (MaaS));
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'), **(iv)** the (future) European privacy legislation, and/or **(v)** all (future) applicable national laws regarding the implementation of the GDPR;
Process(ing):	Any 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: **OPTIMILE**) which Processes Personal Data on behalf of the Customer as Controller;
Sub-processor:	Any sub-processor engaged by OPTIMILE.

All concepts relating to the Privacy Legislation have the meaning set out in the Privacy Legislation.

All concepts relating to the specific collaboration between the Parties (such as, but not limited to, Mobility User) have the meaning set out in the General Agreement.

The Data Processing 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, and **(iii)** the use (i.e. the way(s) of Processing) of the Personal Data, the purpose and means of such Processing and **(iv)** the retention terms during which the Personal Data shall be stored/processed;

Annex II: Overview and description of the security measures taken by OPTIMILE under this Data Processing Policy.

Annex III: Overview of the Sub-processors on which OPTIMILE relies while carrying out the Services.

3 ROLES OF THE PARTIES

3.1 In accordance with the Privacy Legislation, the Customer shall be considered the 'Controller' and OPTIMILE the 'Processor'.

4 USE OF THE SERVICES

4.1 The Customer acknowledges explicitly that:

- ✓ OPTIMILE purely acts as a facilitator of the Services so that the Customer bears sole responsibility for the way in which it uses the Services;
- ✓ OPTIMILE bears no responsibility with regard to adjustments and/or changes made at the explicit request of the Customer;
- ✓ The Customer is liable and responsible for the material and/or data provided by the Customer to OPTIMILE, as the Customer is liable for complying with the Privacy Legislation and/or any other regulations with regard to aforementioned material and/or data;
- ✓ The Customer shall be responsible to comply with all laws and regulations imposed on it by making use of the Services.

4.2 In case of misuse by the Customer of the Services, the Customer agrees that OPTIMILE can never be held liable in this respect nor for any damage that would occur from such misuse.

5 OBJECT

5.1 The Customer acknowledges that, as a consequence of making use of the Services of OPTIMILE, the latter shall Process Personal Data as provided by the Customer and its Associated Companies.

5.2 OPTIMILE shall 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.

5.3 Nonetheless, OPTIMILE shall only Process the Personal Data upon request of the Customer and in accordance with its documented instructions, as described in **Annex I**, unless any legislation requires OPTIMILE to carry out a particular Processing operation. In the latter case, OPTIMILE shall - prior to carrying out such a particular Processing operation - inform the Customer of that legal requirement, unless that law prohibits such information on important grounds of public interest.

5.4 Subsequent instructions may also be given by the Controller (in writing) throughout the duration of the Processing of Personal Data. These instructions shall always be documented by OPTIMILE. OPTIMILE shall immediately inform the Customer if, in OPTIMILE's opinion, instructions given by the Customer infringe the Privacy Legislation. In case the Customer insists that OPTIMILE carries out such instruction, the Customer agrees:

(i) that, as a Controller, the Customer bears full responsibility for the Processing activity and possible consequences of infringement of the Privacy Legislation; and,

(ii) that OPTIMILE is entitled to terminate the Assignment in accordance with the provisions of the General Agreement.

5.5 This Data Processing Policy exists without prejudice to the obligations to which the Customer, as a Controller, is subject by virtue of the Privacy Legislation. Hence, the Customer owns and retains full control concerning (i) the use and the Processing of Personal Data, (ii) the types of Personal Data Processed, (iii) the purpose of Processing, and (iv) the fact whether such Processing is proportionate.

Furthermore, the Customer is responsible for complying with all (legal) obligations incumbent on it, as well as for the accuracy, quality and lawfulness of the Personal Data communicated to OPTIMILE in the context of the performance of the Services, and for the way in which it acquired the Personal Data.

Therefore, the control over the Personal Data provided under this Data Processing Policy shall not belong to OPTIMILE.

5.6 In the event of a contradiction between this Data Processing Policy and the (privacy) clauses in other agreements (such as, but not limited to: the General Agreement or a previous data processing agreement between the Parties) existing at the time when this Data Processing Policy is agreed upon, this Data Processing Policy shall prevail.

6 SECURITY OF PROCESSING

6.1 Taking into account the state of the art, the costs of implementation, the nature, scope, context and purpose of processing and the risks involved for the Data Subjects, OPTIMILE implements appropriate technical and organizational measures for the protection of Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal Data, and, more in general, the confidentiality and integrity of Personal Data. Details on these measures are set forth in **Annex II**.

6.2 OPTIMILE shall only grant access to Personal Data undergoing Processing to those employees who need access for implementing, managing and monitoring the Services of OPTIMILE. These employees have committed themselves to confidentiality in accordance with **Article 9.2**.

7 SUB-PROCESSORS

7.1 The Customer acknowledges and accepts that OPTIMILE is entitled to use Sub-processors in order to fulfill the Services. In such a case, OPTIMILE shall ensure that the Sub-processors are bound by at least the same obligations as those by which OPTIMILE itself is bound under this Data Processing Policy. OPTIMILE shall be responsible for the Sub-processor's performance of said obligations.

7.2 OPTIMILE and the Customer agree on the list (in **Annex III**) concerning the current Sub-processors on which OPTIMILE appeals for the performance of the Services.

7.3 OPTIMILE 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 changes are made. If the Customer wishes to exercise its right to object, it shall notify OPTIMILE in writing and in a reasoned manner by the latest within thirty (30) days after the notification.

7.4 In the event that the Customer objects to a new Sub-processor and its objection is not deemed unreasonable, OPTIMILE will use its best efforts to **(i)** make a change to the Services available to the Customer, or **(ii)** recommend that the Customer makes a commercially reasonable change to his/her use of the Services, so as to avoid Personal Data being processed by the Sub-processor to which it has objected, without, however, causing unreasonable consequences for the Customer.

If OPTIMILE is, however, unable to make such change available to the Customer within a reasonable time (which shall not exceed thirty (30) days following the objection by the Customer), the Customer shall be entitled to terminate the General Agreement provided that:

- ✓ The Services cannot be used by the Customer without recourse by OPTIMILE to the Sub-processor opposed by the Customer; and/or
- ✓ Such termination solely concerns the Services which cannot be provided by OPTIMILE without appealing to the objected new Sub-processor;

  and this by providing written notice thereof to OPTIMILE within a reasonable period of time (which shall not exceed thirty (30) days following the reaction of Optimile by which OPTIMILE informed the Customer that a change cannot be made).

8 TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

8.1 OPTIMILE 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 Decision of the European Commission of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries (Decision 2021/914). Before the transfer takes place, the Data Importer has to guarantee OPTIMILE 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 OPTIMILE 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 OPTIMILE 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, OPTIMILE 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, OPTIMILE 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, OPTIMILE 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.

9 CONFIDENTIALITY

9.1 OPTIMILE shall maintain the Personal Data confidential and thus not disclose nor transfer any Personal Data to third parties, without the prior written agreement of the Customer, unless when:

- ✓ This Data Processing Policy deviates therefrom;
- ✓ Such disclosure and/or announcement is required by law or by a court or other government decision (of any kind). If the court or other public authority allows to, OPTIMILE shall then, prior to any disclosure and/or announcement, discuss the scope and manner thereof with the Customer.

9.2 OPTIMILE ensures that its employees, engaged in the performance of the Assignment, are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have contractually committed themselves to confidentiality. OPTIMILE ensures that such confidentiality obligations survive the termination of the employment contract.

10 NOTIFICATION

10.1 OPTIMILE shall use its best efforts to inform the Customer within a reasonable term 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, OPTIMILE undertakes to:

- ✓ Notify the Customer without undue delay following the detection of a Data Breach, and to provide assistance to the Customer as much as possible in the context of his/her 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 If a Data Subject invokes its privacy rights under the Privacy Legislation and the Customer itself does not have the ability to carry out the request, OPTIMILE shall assist the Customer in doing so (insofar as this is possible).

11.2 OPTIMILE shall promptly notify the Customer if it receives a request directly from a Data Subject invoking its privacy rights under the Privacy Legislation. OPTIMILE shall not respond to any such Data Subject request without the Customer's prior written consent, except to confirm that the request is sent to the Customer.

12 LIABILITY

12.1 OPTIMILE and the Customer 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. OPTIMILE and the Customer indemnify the other Party in this regard.

12.2 The contractual liability of OPTIMILE towards the Customer for a breach of this Data Processing Policy is limited as described in the General Agreement applicable between the Customer and OPTIMILE.

13 RETURN AND DELETION OF PERSONAL DATA

13.1 The Customer and OPTIMILE agree that OPTIMILE may retain the Personal Data in accordance with the retention periods set out in **Annex I** unless the further storage of the Personal Data (or a part thereof) is mandatory under specific national or European Legislation (such as, but not limited to, fiscal requirements). During this retention period or after the end of the provision of Services relating to the Processing, the Customer may request OPTIMILE to delete or return the Personal Data relating to its Mobility Users.

13.2 OPTIMILE will notify the Customer when (significant) changes are made to the retention periods. If the Customer wishes to exercise its right to object, it shall notify OPTIMILE in writing and in a reasoned manner by the latest within thirty (30) days after the notification.

13.3 After expiration of the retention period or after the end of the provision of Services relating to the Processing, OPTIMILE will only use anonymized data for analytical purposes and to further enhance its solutions.

14 DPIA

14.1 If a Customer has to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data in accordance with the Privacy Legislation (a 'Data Protection Impact Assessment' or '**DPIA**'), OPTIMILE shall assist the Customer in doing so to the extent that such Processing operations relate to the Personal Data that will be processed by OPTIMILE and taking into account the nature of Processing and the information available to OPTIMILE.

14.2 If a Customer has to consult a supervisory authority where a DPIA indicates that Processing would result in a high risk in the absence of measures taken by the Customer to mitigate the risk, OPTIMILE shall assist the Customer in doing so to the extent that such Processing operations relate to the Personal Data that will be processed by OPTIMILE and taking into account the nature of the Processing and the information available to OPTIMILE.

15 CONTROL

15.1 OPTIMILE undertakes to provide the Customer with all information, required by the Customer to allow verification whether OPTIMILE complies with the provisions of this Data Processing Policy.

15.2 In this respect OPTIMILE shall allow the Customer (or a third party on which the Customer appeals) to undertake inspections – such as but not limited to an audit – and to provide the necessary assistance thereto to the Customer or that third party. Inspections shall, where appropriate, be carried out with reasonable notice. Parties agree on a maximum of one inspection per calendar year.

15.3 The costs arising from an audit by the Customer shall be borne by the Customer, unless the audit establishes that OPTIMILE has significantly failed to fulfil its obligations under this Data Processing Policy.

16 TERM

16.1 The Data Processing Policy is applicable as long as the use of the Services by the Customer has not come to an end (i.e. formal termination in accordance with the provisions of the General Agreement between OPTIMILE and the Customer).

17 APPLICABLE LAW AND JURISDICTION

17.1 All issues, questions and disputes concerning the validity, interpretation, enforcement and/or performance of this Data Processing Policy shall be governed by and construed in accordance with Belgian law.

17.2 Any dispute concerning the validity, interpretation, enforcement and/or performance of this Data Processing Policy which can not be settled amicable, shall be submitted to the exclusive jurisdiction of the courts of OPTIMILE's registered office in Belgium.

Annex I – Overview of Personal Data, Data Subjects, use and retention period of Personal Data

I. Overview of the Personal Data, which Parties expect to Process*:*

- Name and surname natural person;
- Address;
- Telephone number (fixed/ mobile);
- Email address;
- Date of birth;
- Location data;
- Voluntarily provided information (f.e. in the chat application for taxi services provided on the Mobility Platform);
- Pin code;
- VAT number;
- Bank account number;
- Account information (date of activation, last use);
- Language preference;
- Information regarding the taxi driver specifically (status (active or not), picture, information regarding the cab (car brand, license plate));
- Information regarding the use of the mobility services (date of a ticket purchase, etc.);

II. The categories of Data Subjects whose Personal Data shall be Processed:

- Mobility User – natural person;
- Charge point owner/operator – natural person;
- Taxi driver – natural person.

III. The use (= way(s) of Processing) of the Personal Data and the purposes and means of Processing:

Use of Personal Data:
- Performing the Services/Assignment for the Customer and its Associated Companies.

Means of Processing:
- Software of OPTIMILE.

Purpose of Processing:
- The execution of the General Agreement between Parties: facilitating the Platform enabling the Customer to provide Charging-as-a-Service (CaaS - electric vehicle charging services) and/or Mobility-as-a-Service (MaaS - mobility services such as public transportation) to the charge point owners/operators and/or Mobility Users.

IV. The term(s) during which the (different types of) Personal Data shall be stored:

The Customer and OPTIMILE agree on following proportionate retention periods for Personal Data that are being Processed by Optimile in the Platform in the course of the Assignment:

A. General

Method of Personal Data processing	Personal Data	Processing purpose	Retention period
Account information	Salutation, first name, last name, email address, phone number, language preference and address (account/profile information)	Account administration	Duration of the Data Subject's use of the Platform + 3 years after termination of said use. If relevant, OPTIMILE may retain these Personal Data longer when the Customer has outstanding debts towards OPTIMILE. In this case, the Personal Data are only removed after the necessary payments to OPTIMILE.

(Technical) inquiry for support	First name, last name, email address, phone number and all other Personal Data voluntarily provided to OPTIMILE	Support	Duration of the Data Subject's use of the Platform + 1 year after termination of said use.
Processing of information regarding the use of an account (status)	Date of activation of the account, date when the account was last used	Fraud detection	Duration of the Data Subject's use of the Platform + 3 years after termination of said use. If relevant, OPTIMILE may retain these Personal Data longer when the Customer has outstanding debts towards OPTIMILE. In this case, the Personal Data are only removed after the necessary payments to OPTIMILE.

B. Related to charge point owners/operators

Method of Personal Data processing	Personal Data	Processing purpose	Retention period
Registering additional users	Salutation, first name, last name, email address, phone number, language preference, address and bank account number	Registering additional users on the Platform	Duration of the Data Subject's use of the Platform + 3 years after termination of said use. If relevant, OPTIMILE may retain these Personal Data longer when the Customer has outstanding debts towards OPTIMILE. In this case, the Personal Data are only removed after the necessary payments to OPTIMILE.
Information relating to charging sessions	Token	Registering the use by third parties (data subjects in that case) of charge points	3 years after the last charging session with that specific token.

C. Related to customers - Mobility Users

Method of Personal Data processing	Personal Data	Processing purpose	Retention period
Collection of Personal Data in order to generate a ticket for public transport	• Train (NMBS): first name, last name, email address, date of birth, date, location and language preference • Bus (De Lijn): first name, last name, email address, phone number, location and language preference	Providing public transport services to the Mobility Users	Duration of the data subject's use of the app and, optionally, the Platform + 3 years
Collection of Personal Data when the Mobility User rents a bike	• First name and last name	Registering the Mobility User's purchase of a ticket to rent a bike	Duration of the Data Subject's use of the app and, optionally, the Platform + 3 years
Collection of Personal Data when the Mobility User books a taxi	• Mobility User: first name, last name, phone number and location • Taxi driver: information regarding his/her status (active or not), picture and information regarding the cab (car brand, license plate)	Providing taxi services to the Mobility Users	Duration of the Data Subject's use of the app and, optionally, the Platform + 3 years
Analysing and reporting of the Mobility User's use of mobility services	Location data and information about the use of mobility services (which	• Providing Mobility Users with information	10 years (solely used for statistical purposes regarding the use of certain mobility services)

	mobility services the Mobility User has used in the past)	of his/her use of the mobility services • Gaining insights of the Mobility Users' use of mobility services in general in order to improve our services	
Communication between the Mobility User and taxi services	• Mobility User: first name, last name, email address, language preference and the content of conversations with the taxi driver • Taxi driver: the content of conversations with the Mobility User	Providing chat facilities for the taxi services embedded in the App	1 month

Annex II – Description of security measures

1. Physical access control

Unauthorised persons are to be denied access to:

- OPTIMILE's office and;
- data processing equipment used to process information of OPTIMILE. Data processing equipment will be kept in access-controlled areas.

OPTIMILE has taken measures to prevent and detect unauthorized access and access attempts. The building where OPTIMILE has its office includes a regular assessment of burglary attempts and an alarm system. Moreover, OPTIMILE's office is secured with an electromagnetic key card system.

OPTIMILE provides an electromagnetic key card end physical key to every employee and freelancer. These key cards and physical keys are personal and may not be shared with others. At the end of the employment agreement, the employee or freelancer will return his or her key card. In the event of theft or loss, the employee or freelancer will inform OPTIMILE immediately. A visitor (i.e. someone who does not receive a key card) must identify or authenticate himself or herself before he or she may enter OPTIMILE's office. Visitors are not allowed to roam OPTIMILE's office unattended.

Our main Sub-processor AWS applies following physical access measures to its data centres:

- AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.
- Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.
- Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.
- Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.
- AWS monitors its data centers using its global Security Operations Centers, which is responsible for monitoring, triaging, and executing security programs. It provides 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.
- Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

We have a minor 2nd sub processor Gandi, applying following physical access measures to their used data centers:

- Fire and very early smoke detection (VESDA);
- Neutral gas (nitrogen) fire suppression system;
- Water leakage detection;
- Intrusion detection;
- 24/7/365 on site security guards with controlled access.

2. Access control to information of OPTIMILE

Data processing systems and information media will be protected by logical access mechanisms such as a login and a password. Access to OPTIMILE's data processing systems is determined on a personal level for every employee or freelancer. This access is determined taking into account which access is needed for the execution of the employee or freelancer's job (access on a need-to-know basis). This is also documented in a policy internal access.

Login or access credentials are therefore personal and are never to be shared with others without OPTIMILE's written authorization. Authorised employees or freelancers are not allowed to circumvent access restrictions to information assets by using their own login or access credentials to make copies of such assets and distributing them to unauthorized persons, unless such copies are distributed for legitimate business purposes. As a general principle, confidential information and Personal Data may not be copied.

OPTIMILE will regularly review access authorizations and requests to its information assets by, among others, reviewing allocated user accounts which provide access to OPTIMILE's infrastructure, systems and applications. Such review will be documented.

AWS is OPTIMILE's main cloud provider. AWS deploys state-of-the art security measures. You can find more information regarding its security measures via Cloud Security – Amazon Web Services (AWS).

AWS' security measures include, but are not limited to:

- Data 'at rest' is encrypted using the AES-256 algorithm;
- Data 'in transit' is encrypted, while being transferred, using the TLS 1.3 protocol;
- End-user credentials are stored in a separate MySQL 8.0 database. End-user passwords are hashed with the PBKDF2 algorithm;
- Data collected and stored on the Platform is stored in a separate MySQL 8.0 database;
- Daily backups of the data are stored in an AWS private network for 7 days and are encrypted using the aforementioned mechanisms;
- Data Subjects who are deleted from the Platform their Personal Data will be erased – only evaluations will be kept for statistical purposes without any possibility of identifying the Data Subject;
- Any media (photographs, possible videos, etc.) are stored on 'AWS S3' and thus not publicly available – these files are only accessible through AWS Cloudfront CDN, thereby using URLs which expire after 5 minutes.
- Databases in the AWS cloud run in a private network, access is only accepted from the backend system which runs in the same private network. These accesses are secured by using credentials which have minimum privileges required by the system to fulflll business functions;
- Scheme changes to the databases are not done manually but automatically by the backend system with SQL scripts implemented by developers and tested on QA and staging environments before running them in production;
- The backend system runs in a private network, each instance of which runs in an isolated Docker container. This additional isolation prevents possible attackers who might have gained access to the private network from accessing or modifying backend system runtime memory or configuration;
- All communication coming from the internet via the AWS APIs is done via HTTPS protocol;
- Authorization and authentication mechanisms are implemented using the OpenId Connect protocol and Keycloack. This protocol and open source application are widely adopted and mature, thus strengthening the overall system security;
- Developers that access the AWS cloud in order to monitor or upgrade the infrastructure have their own set of credentials and authentication is done via 2-factor method. For 90 days, an audit is maintained, tracking access and actions of developers in the AWS cloud.

3. Device security

Device security – laptops

Each OPTIMILE laptop shall be:

- protected by a sufficiently strong password and;
- accessible only to the employee.

In the event of malfunctioning, defects, theft or loss, the OPTIMILE employee will inform OPTIMILE immediately and will respond in a timely and correct manner in accordance with OPTIMILE's internal Data Breach Procedure.

Device security – portable media

Information of OPTIMILE and/or Personal Data processed in the context of this Data Processing Policy may not be stored on (privately owned) portable media carriers (for example USB sticks, memory cards, CDs, DVDs, external hard drives, etc.) that can easily be lost or stolen, unless adequate encryption technologies are used which are approved by OPTIMILE prior to the storage.

OPTIMILE has implemented the necessary internal policies governing device security. These policies set out the details of OPTIMILE's employees' and freelancer's responsibilities regarding the use of their laptop or portable media.

4. Availability control

OPTIMILE will implement measures to guarantee and monitor the proper functioning of the network and information systems and take the actions necessary to ensure the availability of these systems.

OPTIMILE ensures that the performance of its employee's or freelancer's tasks does not result in the loss, unavailability or destruction of the information or the applications. If an incident occurs, OPTIMILE's employee or freelancer is obliged to immediately inform OPTIMILE, where appropriate in accordance with OPTIMILE's internal data breach procedure.

OPTIMILE communicates its approved cloud services to its employees or freelancers.

OPTIMILE will put in place an appropriate backup system and processes in accordance with its documented backup procedure.

5. Network, software and service security

OPTIMILE will put in place reasonable measures for the protection of terminal equipment, servers and other infrastructure elements against unauthorised access (e.g. firewalls) under its control.

In case of suspicion of malfunctions, defects, occurring errors, virus danger, data espionage or other circumstances affecting the network, software of service security, the employee will inform OPTIMILE immediately in accordance with the internal data breach procedure.

Unauthorized persons are not allowed to make copies of purchased software or software produced by OPTIMILE itself.

6. Password security

All OPTIMILE's employees or freelancers must use a separate password for each of their work-related accounts and must use that password only for a work-related purpose.

Passwords shall never be sent in unencrypted form via email or another electronic communication tool, unless where it concerns one-time passwords (OTP). This also applies to passwords that the employee or freelancer sends to third parties to create a mobility-account.

Passwords shall never be stored in plain text.

If there is a reason to believe that someone else is aware of the password, the password shall immediately be changed. Any password that is compromised or expected to be compromised will be replaced immediately.

When using a software tool, OPTIMILE adheres to the logical access procedure of this tool, which may require passwords to have one or more of the following characteristics:

- Lower case characters;
- Upper case characters;
- Numbers;
- Punctuation;
- Special characters such as *,$,µ,! etc.;
- No commonly used passwords;
- No reuse of other field's values (e.g. name).

Annex III – List of Sub-processors

At the time of communication of this Data Processing Policy, OPTIMILE will call upon the following Sub-processors for the execution of the Assignment:

Name Sub-processor	Location of Processing	Nature and purpose of Processing	Sub-Processor Security Measures
AMAZON WEB SERVICES (AWS)	EEA: Germany (back-up: Germany)	Cloud service provider	Cloud Security – Amazon Web Services (AWS)
ATLASSIAN	EEA: Germany	Internal documentation tool Support ticketing and roadmap management	Privacy Policy & Data Processing Addendum Atlassian Sub-processors
Hotjar	EEA: Malta	Analytics service provider	Hotjar Data Privacy measures
SENTRY.IO	United States of America	Sentry offers an application monitoring solution designed to identify, monitor, and alert developers to errors, bugs, and other performance issues that are occurring in their applications.	Privacy Policy & Data Processing Addendum
GANDI	EEA: France and Luxembourg	Cloud service provider	Privacy Policy
Freelancers	Depends on the location of the freelancer(s)		OPTIMILE ensures that freelancers are bound by the same terms as this Data Processing Policy by concluding a data processing agreement with all freelancers that have access to Personal Data.