Remerge

DATA PROCESSING AGREEMENT

(Non-EU entities)

This Data Processing Agreement (“**DPA**”) is entered into as of the date of last signature below (“**Effective Date**”) by and between

(Client Legal Name)
Address Line 1
Zip code, Country

(“**Customer**” or the “**Data Controlle**r)

and

(Remerge - Choose the Correct Entity)
Address Line 1
Zip code, Country

(“**Partner**” or the “**Data Processor**”).

This DPA may refer to Controller and Processor each as a “**Party**” and collectively as the “**Parties**.”

1. INTRODUCTION

This DPA forms part of the Insertion Order (IO) or Main Agreement between the Controller and Processor, dated on or about the date hereof, as well as any other agreements that reference this DPA for the processing of Personal Data (as defined below) (collectively, the "**Agreement**"). This DPA supersedes and replaces any previous data processing agreements, addendum, attachments, exhibits, or standard contractual clauses that the Controller and Processor may have previously entered into concerning the Agreement(s). This DPA outlines the Parties’ obligations regarding the Processing of Personal Data, and the Parties agree as follows:

2. DEFINITIONS

“**Applicable Law**” means any applicable (a) law or regulation, mandatory guidance, or statutory code of practice in force from time to time in any applicable jurisdiction; or (b) judgment or any other requirement of any competent court or regulatory authority.

"APPI" means Act on the Protection of Personal Information (Act No. 57 of 2003), which is the Japanese law that governs the collection, use, and management of personal information to ensure the privacy and protection of individuals' data in Japan.

“**CCPA**” means the California Consumer Privacy Act, as amended from time to time, and associated regulations.

“CPRA” means California Privacy Rights Act of 2020, which is a comprehensive data privacy law in California that enhances consumer privacy protections established by the California Consumer Privacy Act (CCPA).

"**Customer Data**" has the meaning given in Clause 3.1.

"Data Controller" or “Controller” means a natural or legal person which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

"**Data Processor**" or "**Processor**" means the entity processing personal data on behalf of the Controller

"**Data Protection Law**" means all Applicable Laws relating to the Processing, protection and privacy of Personal Data and the privacy of electronic communications as amended and/or superseded from time to time, including as applicable the APPI, CCPA, CPRA , GDPR, LGPD, PDPA and Swiss DPA.

"**Data Subject**" means the individual whose Customer Data is Processed by Processor pursuant to the Agreement and this DPA.

"**DPA**" means this Data Processing Agreement or Data Processing Addendum

"**GDPR**" means: (i) the EU General Data Protection Regulation 2016/679 ("**EU GDPR**"); and (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); and (iii) any and all national Data Protection Laws made under, pursuant to or that apply in conjunction with any of (i) or (ii); in each case as may be amended or superseded from time to time.

"LGPD" means Lei Geral de Proteção de Dados, which is the Brazilian General Data Protection Law (Lei No. 13.709/2018), regulating the processing of personal data and ensuring the privacy and protection of individuals' data in Brazil.

"PDPA" means Personal Data Protection Act 2012 (Act 26 of 2012), which is the Singaporean law that governs the collection, use, and disclosure of personal data, ensuring the protection of individuals' data privacy in Singapore.

"PIPA" means the Personal Information Protection Act (Act No. 10465), which is the South Korean law that governs the collection, use, and management of personal information to ensure the privacy and protection of individuals' data.

"**Permitted Purpose**" The specific purposes for which the Processor is authorized to Process Personal Data on behalf of the Controller, as detailed in Annex 2 Part B of this DPA. This includes any other purpose that the Controller may subsequently agree to in writing.

"**Personal Data**" means any and all data (regardless of format) that (i) is defined as "personal data", "personal information", "personally identifiable information" or any analogous concept under Data Protection Law, (ii) identifies or can be used to identify, contact or locate a natural person, or (ii) otherwise pertains in any way to or could be reasonably associated with an identified natural person or their device (whether computer, mobile, connected TV or otherwise), including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location.

"**Process**," "**Processes**," "**Processing**," and "**Processed**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"**Restricted Processing**" means: (i) where the EU GDPR applies, a transfer of Personal Data to, or Processing of Personal Data in, a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data to, or Processing of Personal Data in, any country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; (iii) where the Swiss DPA applies, a transfer of personal data to, or Processing of Personal Data in, any country which is not determined to provide adequate protection for personal data by the Federal Data Protection and Information Commission or Federal Council (as applicable); and (iv) where another Data Protection Law applies, a cross-border transfer of Personal Data to, or Processing of Personal Data in, any other country which is contrary to any data transfer restrictions that apply under that Data Protection Law.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"**Standard Contractual Clauses**" means: (i) where the EU GDPR applies or Swiss DPA applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the DPA 2018 ("**UK Addendum**"); and (iii) where another Data Protection Law applies, the Standard Contractual Clauses or other appropriate cross-border transfer mechanisms approved by an appropriate data protection authority or similar body that is adopted or permitted under that Data Protection Law.

"**Swiss DPA**" means Switzerland's Federal Data Protection Act of 1992 and (from 1 September 2023) revised Federal Data Protection Act (each as amended or superseded).

3. DATA PROCESSING AND RELATIONSHIP OF THE PARTIES

3.1. Pursuant to this Agreement, Processor will Process the Personal Data described in Annex 2, Part B of this DPA ("**Customer Data**") for the Permitted Purpose in the course of providing services to Controller pursuant to the Agreement.

3.2 Partner shall process the Personal Data as a Data Processor on behalf of Data Controller solely for the limited and specified purposes set forth in Annex 2, Part B of this DPA (the "Permitted Purpose").

3.2.1 Processor shall process the Personal Data according to the instructions provided by the Data Controller, which are documented and specific. The Controller shall provide any further instructions in writing, which the Processor may reject if they violate applicable data protection laws or this DPA. In such cases, the Processor will promptly inform the Controller in writing, specifying the reasons for rejection.

3.3. Processor shall not use, combine or otherwise exploit Customer Data to (i) create user profiles or user segments or (ii) for any purpose other than the Permitted Purpose, or (iii) on behalf of or for the benefit of a third party.

3.4. The Parties acknowledge that Partner is a “Third Party” under the CCPA. As such, Partner shall provide the same level of privacy protection to Customer Data as is required of Customer under CCPA.

4. COMPLIANCE WITH LAW

4.1. Each Party shall individually and separately be responsible for complying with the obligations that apply to each one under Data Protection Laws.

4.2. As a Data Controller, the Customer, shall: (a) provide all necessary transparency information (including privacy notices) required by Data Protection Laws to Data Subjects whose Personal Data its Processes pursuant to this DPA and the Agreement, (b) obtain consent or have another lawful basis under Data Protection Laws in respect of its Processing of Personal Data pursuant to this DPA and the Agreement, (c) publish appropriate contact details that Data Subjects may contact to exercise their data subject rights under Data Protection Laws against that Party; and (d)l handle data subject rights requests and will support the Processor by providing necessary information. The Processor shall assist the Controller in responding to such requests within a reasonable timeframe.

4.4. The Processor agrees that the Controller may take reasonable and appropriate steps to (a) ensure that the Processor uses the Customer Data in a manner consistent with the Controller’s obligations under Data Protection Law and (b) upon notice to the Processor, require the processor to stop and remediate unauthorized or unlawful Processing of the Customer Data.

4.5. The Parties shall be able to demonstrate compliance with Data Protection Laws.

(a) The data Processor shall deal promptly and adequately with inquiries from the controller about the processing of data.

(b) The Data Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA. At the Controller’s request, the Processor shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the processor.

(c) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice.

(d) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

5. REMEDIATION

5.1 The Processor shall immediately notify the Controller if for any reason it cannot comply or has not complied with any portion of the Agreement, this DPA or Data Protection Law, or if it becomes aware or has reason to believe that its Processing may cause Controller to breach any of its responsibilities under Data Protection Law.

5.2 Upon notice given pursuant to Clause 4.2 or 5.1, the Processor shall promptly endeavor to remediate any Processing of Customer Data that violates the Agreement, this DPA or Data Protection Laws, and cooperate with and keep Controller informed in respect of such remediation activities (without prejudice to Controller's right pursuant to Clause 4.2 to require Processor to stop any non-compliant Processing).

6. CONFIDENTIALITY, LIMITED USE AND DISCLOSURE

6.1. The Processor will keep and maintain all Customer Data in strict confidence, subject to its confidentiality obligations under the Agreement.

6.2. The Processor will be responsible for the actions and omissions of the Processor's employees, agents, or subcontractors.

7. INFORMATION SECURITY

The Processor shall implement appropriate technical and organizational measures (TOMs) to protect Customer Data against internal and external risks to the security, confidentiality, availability, and integrity of CustomerData, and against Security Incidents. Detailed TOMs are provided in Annex 3 and include regular reviews and updates to adapt to evolving security threats.

8. SECURITY INCIDENT NOTICE

8.1. The Processor will notify the Controller in the event of a Security Incident without undue delay by e-mail to ______________________________ with a copy to the Processor's primary business contact within the Controller. The notification shall contain:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

8.2. Subsequent updates shall be provided as further information becomes available.

9. RESTRICTED PROCESSING

The Parties acknowledge and agree that the provisions set out in Annex 1 shall apply to any Restricted Processing pursuant to this DPA.

10. SUBPROCESSORS

10.1. The Processor may appoint subprocessors to process Customer Data provided that such subprocessors:

(a) Process Customer Data solely for the Permitted Purpose and in accordance with the Controller's documented instructions;

(b) Implement appropriate technical and organizational security measures to protect Customer Data against Security Incidents;

(c) Provide sufficient guarantees that they will process Customer Data in compliance with Data Protection Law.

10.2. Processor shall notify the Controller of any intended changes to subprocessors, giving the Controller an opportunity to object to such changes. The Processor remains fully liable for the performance of its subprocessors' obligations.

10.3. For the avoidance of doubt, **Remerge GmbH** serves as a Subprocessor for all Partner entities and complies with the aforementioned requirements. For transparency purposes, the list of subprocessors of Remerge GmbH can be found at https://www.remerge.io/service-privacy-policy

11. DATA RETENTION AND TERMINATION

Following the termination or expiry of the Agreement, the Processor shall continue to comply with the provisions of this DPA in respect of any Customer Data still in its possession or under its control and will only Process Customer Data to the extent and for as long as necessary to fulfill the Permitted Purpose or as required under Data Protection Laws (following which, it shall promptly delete or destroy such Customer Data and instruct any third party processors it has appointed to do the same).

12. GENERAL

12.1. Material Breach. Party's failure to comply with any of the provisions of this DPA is a material breach of this DPA and the Agreement. In such an event, the other party may terminate the Agreement effective immediately upon written notice.

12.2. Indemnification. The Processor shall be liable to the Controller for any and all loss or damage culpably caused in the performance of the services under the Main Agreement or by a breach of applicable statutory data protection obligations on the part of the Processor, its employees or parties commissioned by it to implement the Principal Agreement. The Processor shall not be obliged to pay compensation if the Processor proves that it has processed the data provided by the Controller solely in accordance with the instructions of the Controller and that it has complied with its obligations arising from the Data Protection Law and Regulations directed to processors. (2) The Controller shall indemnify the Processor against any and all claims for damages asserted against the Processor based on the Controller's culpable breach of its own obligations under this Agreement or under applicable data protection and security regulations.

12.3. Order of Precedence. In the event of any inconsistency between the terms and/or definitions of this DPA and those of the Main Agreement or IO, the terms and/or definitions of this DPA shall prevail to the extent of that inconsistency.

12.4. Counterparts. This DPA may be signed in counterparts, using an electronic or handwritten signature, which constitute one copy and are of equal effect, whether on original or electronic copies.

By signing below, each Party agrees to be bound by the terms of this DPA.

Controller: (please complete)

Signature: ________________________

Name: ___________________________

Title: ____________________________

Date: ____________________________

Processor: remerge (please complete)

Signature: ________________________

Name: ___________________________

Title: ____________________________

Date: ____________________________

Annexes as part of this document:

ANNEX 1 - Restricted Processing and Data Processing Description

ANNEX 2 - Data Processing Description

ANNEX 3 - Security Annex

ANNEX 1 - Restricted Processing and Data Processing Description

1. This Annex 1 forms part of the DPA and describes the measures that the Parties will implement in the event of Restricted Processing.

2. **Restricted Processing**

2.1. If the Processing of Customer Data by Processor entails Restricted Processing, the appropriate Standard Contractual Clauses described below shall be deemed incorporated into this DPA and will apply between Customer (the Controller acting as "**data exporter**") and Processor (the Processor acting as "**data importer**") as follows (with module, clause, option, and annex references being references to the modules, clauses, options, and annexes of the Standard Contractual Clauses unless otherwise stated):

a. in relation to Customer Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

i. Module Two (Controller to Processor) will apply;

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 11, the optional language will not apply;

iv. in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by the German law;

v. in Clause 18(b), disputes shall be resolved before the courts of Germany;

vi. Annex I of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex 2 to this DPA; and

vii. Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex 3 to the DPA; and

b. In relation to Customer Data that is protected by the UK GDPR, the EU SCCs as modified by the UK Addendum will apply as follows:

i. the EU SCCs shall be deemed completed as set out above in sub-clause 2.1(a) of this Annex 1 and shall be modified by the UK Addendum (completed as set out in sub-clause ii below);

ii. Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out in sub-clause 2.1(a) of this Schedule 1, the options "Exporter" shall be deemed checked in Table 4, and the start date of the UK Addendum (as set out in Table 1 of the UK Addendum) shall be the date of this Agreement; and

c. In relation to Customer Data that is protected by the Swiss DPA, the EU SCCs will apply as set out in sub-clause 2.1(a) of this Annex 1 with the following amendments:

i. references to ‘Regulation (EU) 2016/679’ in the EU SCCs will be deemed to refer to the Swiss DPA;

ii. references to specific articles of ‘Regulation (EU) 2016/679’ will be deemed replaced with the equivalent article or section of the Swiss DPA;

iii. references to ‘EU’, ‘Union’ and ‘Member State’ will be deemed replaced with ‘Switzerland’,

iv. references to the ‘competent supervisory authority’ and ‘competent courts’ are replaced with the ‘Swiss Federal Data Protection Information Commissioner’ and ‘applicable courts of Switzerland’ (as applicable),

v. in Clause 17, the EU SCCs will be governed by the laws of Switzerland, and (vii) in Clause 18(b), disputes shall be resolved before the competent courts of Switzerland.

d. In relation to Customer Data that is protected by another Data Protection Law, the Data Exporter and the Data Importer agree that such Standard Contractual Clauses shall automatically apply to the transfer of Customer Data from the Data Exporter to the Data Importer and, where applicable shall be deemed completed on a mutatis mutandis basis to the completion of the Standard Contractual Clauses as described above.

e. In the event that any provision of this Annex 1 of the DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

f. If the Parties' compliance with GDPR requirements relating to international transfers of Personal Data is affected by circumstances outside of the Parties' control, including if the Standard Contractual Clauses or any other legal instrument for international transfers of Customer Data is invalidated, amended or replaced, then the Parties will work together in good faith to reasonably resolve such non-compliance.

ANNEX 2 - Data Processing Description

This Annex 2 forms part of the DPA and describes the Processing that the Processor will perform on behalf of the Controller.

(A). LIST OF PARTIES

Controller / Data exporter:

Name:	Means the Customer whose details are specified at the outset of this DPA.
Address:	The Controller address as specified at the outset of this DPA
Contact person's name, position and contact details:	(complete)
Activities relevant to the data transferred under these Clauses:	The receipt of services by the Processor pursuant to the Agreement and this DPA.
Signature and date:	This Annex 2 shall be deemed executed upon execution of the DPA.
Role:	Controller

Processor / Data importer:

Name:	Means the Partner whose details are specified at the outset of this DPA.
Address:	The Processor address as specified at the outset of this DPA
Contact person's name, position and contact details:	**EU Data Protection Officer**: Ilan Leonard Selz **Non-EU Data Protection Officer:** Julie Armindo Kremp E-mail: privacy@remerge.io
Activities relevant to the data transferred under these Clauses:	The provision of services on behalf of the Controller pursuant to the Agreement and this DPA.
Signature and date:	This Annex 2 shall be deemed executed upon execution of the DPA.
Role:	Processor

B. DESCRIPTION OF PROCESSING AND TRANSFER

Categories of data subjects whose personal data is processed and transferred:	The Customer Data transferred may concern the following categories of Data Subjects, as further specified in the Agreement: ● Consumers and prospective consumers of Controller products and services
Categories of personal data processed and transferred:	The following types of personal data shall be processed under this Agreement: ● advertising identifier (such as IDFA and AAID), if provided ● IP addresses, Click ID, specified URL, and User Agent From time to time, the Controller may supply the Processor with additional, so-called attribution data which typically relates to the behavior of users inside the apps of the Controller, its affiliates and counterparties. This data may consist of ● installation and first opening of an app on user's mobile device; ● user interactions within an app (e.g. in-app purchases, registration); ● information regarding which advertisements users have seen or clicked on; ● certain metadata, such as timestamp, device type and model, app and app version, country.
Sensitive data processed and transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	The Customer Data transferred concern the following special categories of data (please specify): ● None
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous for the duration of the Agreement
Nature of the processing:	The provision of the mobile advertising services specified in the Agreement. The nature and purpose of the processing of personal data by the Processor is specified in the Principal Agreement. The Principal Agreement (IO or Master Agreement), according to the type of campaign chosen by the Controller, may include some or all of the following activities and purposes:

	● the provision of advertising identifiers (IDFA, AAID) from Controller to Processor (and vice versa for reporting purposes) in encrypted form via a secure interface provided by Processor; ● the creation of a database based on the collected data in order to provide services for the Controller (e.g. user segmentation); ● the recognition of these users on the publisher and supply side platforms; ● the targeting of these users with personalized marketing messages and/or ● targeting of inventory segments based on their contextual similarity with the advertisers' existing user base and/or ● matching of advertising identifiers for the purpose of excluding known users and ● the processing of IP addresses, Click ID, specified URL, and user agent, for purposes of displaying the advertising.
Purpose(s) of the data transfer and further processing:	Processor shall Process the Customer Data set out in this Annex 2, Part B for the following purposes: a. Targeted advertising and optimization of Controller campaigns; b. Analytics and attribution for Controller campaigns; c. Frequency capping, audience verification, system maintenance, fraud detection, tracking and measurement of Controller campaigns; and d. To verify, maintain, or improve the quality of the services provided to the Controller.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	For the duration of the Agreement (or as otherwise specified in the Agreement).
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	To **Remerge GmbH**, the main entity that provides all the infrastructure to the processing.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	Where the EU GDPR applies, the competent supervisory authority shall be the Berlin DPA (Berliner Beauftragte für Datenschutz und Informationsfreiheit) or as otherwise determined by Clause 13 SCCs. Where the UK GDPR applies, the UK Information Commissioner's Office. Where the Swiss DPA applies, the Swiss Federal Data Protection and Information Commissioner.

ANNEX 3 - Security Annex

TECHNICAL AND ORGANIZATIONAL MEASURES

INCLUDING MEASURES TO ENSURE THE SECURITY OF THE DATA

The Processor guarantees that the following technical and organizational measures have been taken:

MEASURE	DESCRIPTION
PSEUDONYMIZATION MEASURES Measures that reduce direct references to persons during processing in such a way that it is only possible to associate data with a specific person if additional information is included. The additional information must be kept separately from the pseudonym by appropriate technical and organizational measures.	Processor does not collect, process or store any data that would allow association with a specific person with a pseudonym as further data points are unavailable to Processor. For internal and external aggregated reporting pseudonyms are dropped therefore anonymizing the data.
ENCRYPTION MEASURES Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted, character string (secret text) by means of an encryption method (cryptosystem).	Processor uses TLS (1.2) for all communication that does not use a private channel. Data at rest is encrypted using standard block encryption algorithms.
MEASURES TO ENSURE CONFIDENTIALITY	
1. **Physical access control:** measures that physically deny unauthorized persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data storage media.	Processor’s office is protected by an electronic door lock system. Tokens to open doors are assigned to individual employees on an as needed basis and can be centrally revoked on demand at any time without access to the token. Lock access is centrally logged. Processor’s data center providing sub-processors protects Processor’s servers against any physical access besides sub-processors maintenance staff employing industry standard data center protection techniques.
2. Logical access control: measures to prevent unauthorized persons from processing or using data which is protected by data privacy laws.	Processor uses a centrally managed SSO solution with 2FA support. The system enforces personal and individual login user credentials with strong password rules and regular password changes. Authentication attempts are logged. After a number of unsuccessful attempts credentials are suspended temporarily. Access is granted on a as needed basis using a role based rights management system. A standardized employee on- and offboarding process is in place to ensure access rights are only granted as long as necessary and based on the role of the employee. Production systems are completely separated from

	other company systems and only support public/private key based authentication. Keys are managed centrally and only employees that need to interact with production systems (developers, ops) hold time limited keys. Data at rest is encrypted.
3. Data access control: measures to ensure that persons authorized to use data processing systems can only access personal data according to their access rights, so that data cannot be read, copied, changed or removed without authorization during processing, use and storage.	Processor uses a role-based approach to determine access rights for all user and system combinations. Roles are based on job function and defined responsibilities using the concepts of need-to-know and least privilege. They are assigned during the onboarding process and reviewed if the job function changes or if the employees role changes. Role application, approval, allocation and reset are reviewed and signed off by the responsible manager. Granted roles are tied to a personal identifier and an account. Resource authorization is tied to specific roles. If the foundation for an authorization ceases to apply, the authorization/role is withdrawn immediately. Access to personal data via the Remerge Platform is limited to operational personnel and restricted in the scope of access capabilities to the minimum need to fulfil operational duties. Interaction with Processor’s systems is logged in an immutable log and can be audited afterwards. To ensure that data can not be read or copied by unauthorized personnel, Processor encrypts data in transit (HTTPS) and at rest.
4. Separation rule: measures to ensure that data collected for different purposes are processed separately and separated from other data and systems in such a way as to preclude the unplanned use of such data for other purposes.	The Processor employs different data processing systems for different purposes. These systems are architecturally (logical and physically) separated. All systems require a valid authorization to be accessed. Changes to the structure of Processor’s systems that affect data separation are documented in a revision safe manner and follow a strict review process by the technical operations personnel. To ensure against unintentional amalgamation of data, Processor separates development, testing, staging and production environments. Controller data is logically separated.
5. Authentication and Access Control Enhancements	Processor utilizes SSO tool to enhance authentication and access control mechanisms. This includes enforcing Two-Factor Authentication (2FA) on all assets, further securing access to systems and data against unauthorized use. This measure strengthens Processor's commitment to ensuring the confidentiality and integrity of the data processed.

MEASURES TO ENSURE INTEGRITY	
1. **Data Integrity:** measures to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.	Processor employs an automated testing system for new releases which verifies the correctness of the changed component. Components that fail these tests will not be deployed to a production environment. Changes to Processor’s main database are logged, can be audited and rolled back on a per change basis. To ensure against unintentional data corruption the production system is segregated from other environments.
2. **Transmission control:** measures to ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted or made available using data communication equipment.	Processor offers Controllers the ability to access their own data via several APIs. Access to these APIs is governed by a per Controller authentication and authorization process. Transactions are logged and are available for auditing. Data that is transmitted to the Controller by Processor’s operations personnel is governed by a transport process with individual responsibilities (encryption & signing).
3. **Transport control:** measures to ensure that the confidentiality and integrity of data is protected during transmission of personal data and transport of data carriers.	Personal data that is transmitted (sent and received) to or from Processor over public channels is encrypted (TLS 1.2). If changes to the data are detected during transmission the data is discarded and the channel is considered compromised.
4. **Input control:** measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data have been entered or modified in data processing systems.	Personal data that is submitted by Controller using Processor’s APIs is verified and associated with its source by a Controller specific verification token. All interactions with the Processor’s main database via the Remerge Plattform are verified and logged. This change log includes information about who added, modified or deleted data and what point in time.
MEASURES TO ENSURE AVAILABILITY AND RESILIENCE	
1. **Availability control:** measures to ensure that personal data are protected against accidental destruction or loss.	To ensure against a loss of data all storage systems are multi-way redundant (hardware and logical). In addition data is automatically backed up in regular intervals to physically separated systems and can be restored on demand. Backups are encrypted. Furthermore Processor’s data center sub-processors provide a highly available infrastructure that is secured against major physical risks by providing: alarm systems, fire alarms, air conditioning, waterproof server rooms, uninterrupted power supplies and redundant upstream connectivity.

2. Quick recovery: measures to ensure the ability to quickly restore the availability of and access to personal data and used systems in the event of a physical or technical incident.	Due to the redundant storage a quick recovery is ensured.
3. Reliability: measures to ensure that the functions of the system are available and malfunctions are reported.	All systems in the Processor’s infrastructure are monitored with the help of a software based system. An automated alerting system notifies Processor’s personnel 24/7 via SMS, eMail, call or custom notifications in case any systems behave outside of well defined normal conditions. In case of a malfunction Processor’s personnel follow a standardized incident management & communication process which clearly defines steps and responsibilities.
4. Endpoint Protection Measures	To enhance the security of all employee desktops, Processor has implemented an antimalware solution that routinely scans for viruses, ensuring that threats are identified and mitigated promptly. This measure complements the existing access control and data integrity frameworks by providing an additional layer of protection against malicious software.
5. Device Management and Security	Processor has enabled Mobile Device Management to manage and secure company devices effectively. This system provides comprehensive control over devices, ensuring they comply with Processor’s security policies and standards. It also facilitates the deployment of security updates and patches, further securing the devices against vulnerabilities.
MEASURES FOR THE REGULAR TESTING AND EVALUATION OF THE SECURITY OF DATA PROCESSING	
1. Verification process: measures to ensure that the data are processed securely and in compliance with data protection regulations.	The processor employs an external auditing service that regularly verifies compliance with data protection regulations. Furthermore, a regular internal audit by the Processor’s legal department ensures compliance. Processor’s personnel are regularly trained with regard to data protection and security best practices. The Controller is entitled to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties. The Controller shall notify the Processor immediately of any errors or irregularities detected in relation to the processing of personal data by the Processor.
2. Order control: measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.	The Controller is entitled to issue instructions concerning the nature, scale and method of data processing. Upon request by the Controller, the

	Processor shall confirm verbal instructions immediately in writing or in text form (e.g. by email). Instructions received by the Controller are documented and acted upon by the Processor as applicable. This includes data request, retention and deletion policies. Insofar as the Controller deems it necessary, persons authorized to issue instructions to the Processor may be appointed. The Controller is entitled to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties.
ORGANIZATIONAL MEASURES Organizational measures are actions and protocols put in place by the Processor to ensure the effective management and protection of personal data. These measures encompass a range of activities, including but not limited to:	
1. Data Protection Officer (DPO)	The Processor has appointed a DPO for oversight of data protection strategies and compliance as defined in the privacy policy. https://www.remerge.io/service-privacy-policy
2. Privacy Policy	https://www.remerge.io/service-privacy-policy
3. Training and Awareness	The Processor conducts regular training sessions for employees on data protection principles, security, and practices.
4. Data Protection Impact Assessments (DPIAs), RoPAs and assessments with Risk Management	The Processor performs DPIAs for high-risk processing activities to identify and mitigate risks and Maintaining detailed records of all data processing activities, identifying and assessing risks related to data processing activities and implementing measures to mitigate those risks
5. Data Subject Rights	Implemented internal procedures to handle data subject requests to support our Customers efficiently.
6. Incident Response and Breach Notification	The processor established an incident response plan to handle data breaches promptly.
7. Third-Party Management	The Processor ensures that third-party service providers comply with GDPR and relevant Data Processing Laws, including through Data Processing Agreements (DPAs)
8. Regular Internal Audits and Review	Conducting regular internal audits and reviews of data protection and security practices to ensure ongoing compliance.