Remerge

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.	The 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 the 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).	The 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.	The 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 revoked on demand at any time without access to the token. Lock access is centrally logged. The processor's data center, which provides sub-processors, protects the Processor's servers against any physical access besides sub-processor 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.	The 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 who 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 and 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.