Data Processing Agreement pursuant to Art. 28 (3) GDPR and other applicable law

1. General

1.1. Essentry Inc. (hereinafter referred to as the "Contractor") operates systems for the digital administration of access management processes and concludes contracts with Clients for the use of the "essentry" system (hereinafter referred to as "system contracts" or "system contract").

1.2. This agreement (together with its annexes described in more detail below) on data processing in accordance with Art. 28 GDPR and other applicable law (hereinafter also referred to as the "Agreement") specifies the legal rights and obligations arising for the Contractor and the Client from the General Data Protection Regulation (Regulation (EU) 2016/679, hereinafter also referred to as the "GDPR") and other privacy and data protection laws (such as the California Consumer Privacy Act, as amended, and its regulations (hereinafter also collectively referred to as the “CCPA”)) if the Contractor processes personal data for the Client within the scope of the system contracts or carries out commissioned maintenance (hereinafter also referred to as "data processing").

1.3. The Contractor acknowledges that the GDPR and other applicable laws protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and that these principles also apply to the Contractor.

2. Definitions

2.1. The definitions in Art. 4 and Art. 9 GDPR and the following additional definitions apply:

2.2. "Commissioned maintenance" means services provided by the Contractor (e.g. care, maintenance or other services on computer programs or technical objects for information processing), during the performance of which it cannot be ruled out that the Contractor will gain access to personal data for which the Client is responsible.

2.3. "System Contract" means the respective legal relationship between the Client and the Contractor based on which the Contractor carries out data processing or commissioned maintenance for the Client as intended.

2.4. "Subcontractor" means third parties within the meaning of Art. 4 No. 10 GDPR, which the Contractor uses with the written consent of the Client to provide services under the system contract.

2.5. Further definitions can be made contextually in the respective clause of this agreement.

3. Components of the agreement

3.1. Data processing or commissioned maintenance by the Contractor shall always be carried out based on a system contract between the Contractor and the Client. The system contract is decisive for the subject matter, duration, type, and purpose of the data processing, as well as for determining the type of personal data and the categories of data subjects (hereinafter also referred to as "subject matter of the order"). To determine the subject matter of the order, the Contractor and the Client shall use the **Annex 1: Subject-matter of the data processing** and add it to the corresponding system contract in a legally binding manner.

3.2. This agreement contains provisions on data processing and commissioned maintenance that apply to all system contracts concluded between the Client and the Contractor. Binding components of this agreement are

- **Annex 1: Subject-matter of the data processing**
- **Annex 2: Security of processing**
- **Annex 3: Contact persons**
- **Annex 4: Subcontractors**
- **Annex 5: Notification form for data protection breaches**

3.3. The provisions of this agreement, including its annexes, shall take precedence over any contradictory provisions of a system contract.

4. Principles for data processing

The Contractor processes personal data exclusively in accordance with the system contract, in accordance with this agreement and within the scope of the Client's instructions. Without limiting the foregoing restrictions on Contractor’s processing of the personal data, the Contractor:

- shall not “sell” the personal data, as such term is defined in the CCPA and similar U.S. state privacy laws;
- shall not “share” the personal data, as such term is defined in the CCPA (regardless of whether the CCPA applies) or otherwise disclose it for targeted advertising purposes;
- shall not retain, use, or disclose any such data outside of the direct business relationship between the Client and the Contractor, or for any purpose (including any commercial purpose) other than the limited business purposes specified in this agreement and as permitted by applicable law;
- shall comply with any restrictions under applicable law on combining the personal data that Contractor receives from, or on behalf of, Client with personal data that Contractor receives from, or on behalf of, another person or persons, or that Contractor collects from any other interaction between Contractor and a data subject;
- shall provide the same level of protection for any personal data subject to the CCPA as is required of businesses under the CCPA, and shall promptly inform the Client if the Contractor determines that it can no longer meet its obligations under the CCPA;
- hereby certifies that it understands the restrictions and obligations set forth in this agreement and that it will comply with them.

5. Duration of the data processing

5.1. The term of this agreement depends on the duration of the system contracts.

5.2. The agreement ends automatically and without the need for termination if the Contractor no longer carries out any data processing or commissioned maintenance for the Client.

5.3. The right to ordinary termination is - subject to the termination option under **section 5.4** - is excluded. The right to extraordinary termination for good cause in accordance with § 314 BGB remains unaffected.

5.4. The Client may terminate a system contract, irrespective of any conflicting provisions in the system contract, if the Contractor breaches a statutory data protection provision or an obligation under this agreement or breaches a guarantee. In this case, the notice period shall be three (3) months to the end of the month. Claims of the Contractor due to premature termination of the contract, in particular claims for damages, are excluded.

6. Place of data processing

6.1. Subject to the following provisions, the data processing may only take place in a member state of the European Union or in another state party to the Agreement on the European Economic Area.

6.2. Any data processing outside a member state of the European Union or outside another state party to the Agreement on the European Economic Area (hereinafter referred to as "third country") requires the prior written consent of the Client.

6.3. Consent to data processing in a third country will not be granted in particular if the special requirements of Art. 44 f. GDPR are not permanently fulfilled, in particular if there is no adequate level of protection in the third country or if there are no suitable guarantees to ensure an adequate level of protection.

6.4. The Contractor shall ensure at its own expense that an appropriate level of protection is ensured in the third country and shall provide evidence of this to the Client when obtaining approval, in particular by:

- an adequacy decision by the EU Commission (Art. 45 (3) GDPR);
- binding internal data protection rules (Art. 46 section 2 lit. b. in conjunction with Art. 47 GDPR);
- Standard data protection clauses (Art. 46 section 2 lit. c and lit. d GDPR);
- approved codes of conduct (Art. 46 section 2 lit. e in conjunction with Art. 40 GDPR);
- approved certification mechanisms (Art. 46 section 2 lit. f. in conjunction with Art. 42 GDPR); or
- other measures (Art. 46 section 2 lit. a., section 3 lit. a and lit. b GDPR).

7. Instructions from the Client

7.1. Notwithstanding binding stipulations within the meaning of **section 3.1** of this Agreement, the Contractor acknowledges that the Client alone determines the purposes of the data processing and may also order this by means of individual instructions, and that any processing by the Contractor outside the intended purpose or an instruction is unlawful. Art. 28 section 3 lit. a GDPR is decisive for exceptions to this.

7.2. Every instruction from the Client obliges the Contractor to carry out, tolerate or refrain from ("actions") every process specified in the instruction (e.g. collection, storage, transmission, deletion or destruction of personal data) in accordance with the instructions. The Client's right to issue instructions includes, in particular, that the Client may lawfully determine vis-à-vis the Contractor how the system contract is to be implemented in terms of data protection law, as well as to request order-related information and to request actions that may serve to fulfill a legal, sovereign or official requirement to which the Client is subject.

7.3. Instructions must always be issued in writing (Section 126 BGB) or in text form (Section 126b BGB). Verbal instructions are only permissible in exceptional cases; they must be documented by the Contractor in writing (Section 126 BGB) or text form (Section 126b BGB). The Contractor must inform the Client immediately if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Client.

8. Adjustments and further development

8.1. When processing personal data, interpreting the requirements of the GDPR and interpreting this Agreement, the applicable recommendations of the Art. 29 Working Party or its successor organization (European Data Protection Board) must be taken into account appropriately.

8.2. The Client and the Contractor agree to adapt and amend this Agreement, including annexes, by mutual agreement and free of charge for the Client in the event of changes, adaptations and/or additions to data protection regulations - in particular the GDPR and/or the applicable national implementation laws, the CCPA, or similar laws.

9. Duty of confidentiality

9.1. The Contractor guarantees that it has obligated the persons employed by it for processing to maintain confidentiality and that it will also comply with this obligation through organizational precautions, in particular that personal data will not be processed without authorization, only in accordance with the order or in accordance with instructions, and that this obligation will continue to apply even after the end of their activities (Art. 28 section 3 lit. b); Art. 29; Art. 32 section 4 GDPR). The same applies to other confidentiality and/or protection provisions under data protection law, insofar as these are relevant to the processing.

9.2. Upon request, the Client shall be provided with corresponding evidence free of charge. The Contractor is at liberty to provide evidence by complying with approved rules of conduct (Art. 40 GDPR) or by complying with an approved certification procedure (Art. 42 GDPR), provided that this shows that the persons involved in the processing in accordance with **section 9.1** are obliged to maintain confidentiality.

10. Safety of processing

10.1. The Contractor confirms that it has taken the measures required in its area of responsibility in accordance with Art. 32 GDPR. The Contractor undertakes to design and update its internal organization accordingly, taking into account the respective state of the art, the implementation costs and the nature, scope and circumstances and purposes of the processing and the different probability of occurrence and severity of the risk to the rights and freedoms of the data subjects, so that they comply with the special requirements of data protection under the GDPR and ensure the protection of the rights of the data subjects. In general, the technical and organizational measures (TOM) to be taken include in particular

10.1.1. protecting the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing of the data;

10.1.2. as appropriate, the encryption of personal data and, where possible, its pseudonymization;

10.1.3. the ability to quickly restore the availability of personal data and access to it in the event of a physical or technical incident;

10.1.4. the implementation and maintenance of procedures to regularly review, assess and evaluate the effectiveness of the technical and organizational measures to ensure the security of the processing at intervals of no longer than twenty-four (24) calendar months.

10.2. The Contractor shall present the measures to which it commits to the Client correctly, completely, and clearly in advance of the award of the contract, document them with regard to the specific execution of the contract and submit them to the Client for review. If accepted by the Client, the documented measures will form the basis of the respective data processing and will be used as **Annex 2: Security of processing** to this agreement.

10.3. The Contractor is free to prove the suitability of the technical and organizational measures to be taken - in particular in accordance with Art. 32 GDPR - by complying with approved rules of conduct in accordance with Art. 40 GDPR or by complying with an approved certification procedure in accordance with Art. 42 GDPR. Proof can only be provided (and only for as long as) the Contractor presents the Client with a valid certificate issued by an accredited certification body in accordance with Art. 43 GDPR for those processing procedures and locations that are relevant for the processing operations under this Agreement or the corresponding system contract. The Contractor must notify the Client immediately of any changes to the certificate or its expiry.

10.4. The submission of the aforementioned certification does not diminish the Contractor's responsibility and does not replace the Contractor's obligation to guarantee that the **requirements** under this **section 10** and the **Annex 2: Security of processing** within the meaning of Art. 32 GDPR are in place as well as maintained and updated.

10.5. To increase the security and further development of the essentry app, the Contractor evaluates anonymized usage data. This information cannot be assigned to any person and the Contractor does not merge this data with other data sources. For this purpose, the Contractor performs the anonymization on behalf of the Client.

10.6. The Contractor is permitted to take and implement a technical measure other than one expressly described if the security level of the processing is thereby maintained or increased, and the measure is documented and communicated to the Client.

10.7. The Client shall be entitled at any time to demand compliance with the obligations and guarantees entered in this Clause in accordance with **section 16** to check. Any breaches of duty identified shall be remedied by the Contractor without delay.

11. Subcontractor

11.1. The subcontracting of processing by the Contractor to a subcontractor is not permitted unless the following conditions are met:

11.1.1. The Client has expressly consented to the subcontracting in writing (in this agreement or in a system contract).

11.1.2. The Contractor has carefully selected the subcontractor and has given the Client a guarantee that the subcontractor will perform all subcontracted services in accordance with all relevant provisions of this Agreement and the relevant statutory provisions, including, where applicable, the GDPR.

11.1.3. The Contractor has ensured through appropriate agreements with the subcontractor and demonstrated to the Client that the Client can also exercise all rights to which it is entitled vis-à-vis the Contractor vis-à-vis the subcontractor during the term of the subcontracting; this also includes rights of inspection of documents and contracts relevant to data protection and information about processes relevant to data protection law.

11.2. The processing, and in particular the transfer of personal data to or by the subcontractor, is only permitted (and only for as long as) the conditions set out in **section 11.1** are demonstrably fulfilled and the Client has not withdrawn its consent in accordance with **section 11.4** has revoked its consent.

11.3. Subcontractors approved at the time of conclusion of this agreement between the Client and the Contractor are listed in **Annex 4: Subcontractors** and any addenda thereto shall be made in writing. The right to authorize subcontractors in the system contract remains unaffected.

11.4. The Client may revoke its consent to the use of a subcontractor in justified cases - in particular in the event of a breach of law or other breach of duty. The Contractor shall immediately cease the subcontracting.

11.5. If the Client does not agree to the use of a new subcontractor or revokes its consent to an already approved subcontractor, both parties have a special right to terminate the contract and this data processing agreement with one month's notice.

12. Rights of the data subjects

12.1. The Client is responsible for safeguarding the rights of data subjects in accordance with Chapter 3 of the GDPR and other applicable law. The Contractor is only permitted to implement the rights of data subjects in accordance with the instructions of the Client. However, the Contractor is obliged to fully support the Client in fulfilling requests and claims of data subjects in accordance with Chapter 3 of the GDPR and other applicable law.

12.2. If data subject rights are asserted directly against the Contractor, the Contractor must forward the request to the Client without delay. If it is not possible for the Contractor to identify the personal data of the individual making the request, the Contractor shall prove the lack of identifiability to the Client (including, where applicable, in accordance with Art. 11 section 2 GDPR). If requests are not forwarded immediately, the Contractor shall be liable to the Client for any delays in processing requests from data subjects, considering the processing periods specified in Art. 12 section 3 GDPR or other applicable law, unless the Contractor is not responsible for the delay.

13. Reporting of data protection incidents

13.1. The Contractor shall notify the Client in any case in which it becomes aware of (i) a breach of the protection of personal data by it or the persons employed by it, (ii) a breach of regulations on the protection of personal data or (iii) a breach of the provisions made in this Agreement (hereinafter "Data Protection Incident").

13.2. The notification must be made immediately, at the latest within forty-eight (48) hours of becoming aware of it.

13.3. Upon becoming aware of a data protection incident, the Contractor shall immediately take the necessary measures to secure the data and mitigate any adverse effects for the data subjects and the Client.

13.4. The notification of a data protection incident must - as far as possible - contain all information required by the Client to fulfill its obligations under Art. 33 and Art. 34 GDPR; in particular

13.4.1. a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, the categories concerned and the approximate number of personal data records concerned;

13.4.2. the name and contact details of the Contractor's data protection officer or a person of the Contractor who can provide information on the matter;

13.4.3. a description of the likely consequences of the personal data breach;

13.4.4. a description of the measures already taken and those proposed by the Contractor to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

13.5. For reports, please use the form in attached hereto.**Annex 5: Notification form for data protection breaches** The Contractor is obliged to document data protection incidents in detail, including their effects and the remedial measures taken. The documentation must be made available to the Client without delay.

14. Obligations of the Contractor to cooperate

14.1. With regard to its area of responsibility, the Contractor is obliged to keep detailed documentation on the processing of personal data and to make this available to the Client immediately upon first request. Based on the documentation, the Client must be able to prove the correctness of the data processing in accordance with Art. 24 section 1 GDPR in a suitable manner at any time.

14.2. With regard to its area of responsibility, the Contractor is obliged to provide the data and information required for the Client's process register in accordance with Art. 30 (1) GDPR.

14.3. The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR and equivalent requirements in other applicable laws. in particular, those relating to the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. For this purpose, the Contractor shall provide the Client with all documents, records and evidence required for Art. 32 - 36 GDPR and such other applicable laws.

14.4. The Client must be informed immediately of any inspections and measures taken by the supervisory authority or other government authority in relation to the Client of the Client’s personal data, including in accordance with Art. 58 GDPR. This also applies if a competent authority investigates the Contractor.

14.5. The Contractor is obliged to regularly check the performance of the processing itself for conformity with this agreement. If errors or irregularities are discovered during the inspection, the Client must be informed immediately.

14.6. Where required by law, the Contractor is obliged to appoint a data protection officer who can carry out their activities in accordance with Art. 37, 38 GDPR. The contact details of the data protection officer or another contact person for data protection issues - insofar as a data protection officer is not to be appointed - shall be provided to the Client for the purpose of direct contact.

15. Release of personal data

15.1. The Contractor acknowledges that the Client must be entitled to demand the surrender of personal data from the Contractor at any time as a result of its role as controller. The Contractor therefore guarantees the Client that it has taken technical and organizational measures to be able to fulfill the claim for surrender without delay and waives any objections and defenses against the claim for surrender.

15.2. The right to disclosure includes all personal data processed by the Contractor under the responsibility of the Client, in particular personal data transmitted by the Client and personal data that has been changed, created, or generated in the course of the performance of a system contract.

15.3. Once the Client has confirmed the successful release of the personal data in writing or text form, it must be deleted immediately from the Contractor's storage media in such a way that it can no longer be reproduced. The Contractor shall guarantee the corresponding deletion of this personal data on the storage media of any subcontractors. Upon request, the Contractor shall provide the Client with evidence that this deletion has been carried out by means of suitable documents or appropriate insurance. The above shall apply accordingly if the processing of personal data by the Contractor ends, but the Client expressly waives the surrender to the Contractor and no agreement to the contrary has been made.

15.4. The Contractor may store certain personal data in blocked form instead of deleting it, as long as and to the extent that the Contractor is subject to mandatory statutory provisions that oblige it to retain it. The lawfulness of access to blocked data is assessed according to the legal provision on the basis of which the personal data had to be blocked.

15.5. In the event of the removal or seizure of a storage medium by a third party on which the Client's personal data is stored, or in the event of foreclosure of such a storage medium by a third party, the Contractor shall immediately inform both the third party of the fact that the Client's personal data is located on the data carrier concerned and the Client of the corresponding measure. Any legal remedies of the Client against the measures of the third party shall remain unaffected.

16. Control rights of the Client

16.1. The Client has the right to take reasonable and appropriate steps to (a) ensure that Contractor is using the personal data consistent with Client’s obligations under applicable law and (b) stop and remediate unauthorized use of the personal data. During the term of this agreement and until the general limitation period for claims arising from this agreement has expired, the Client shall have the right to carry out inspections or, in individual cases, to have them carried out by third parties or auditors who are obliged to maintain confidentiality. In particular, the Client shall have the right to satisfy itself of the Contractor's compliance with this Agreement by means of random checks in its business operations during normal business hours. The Contractor may assert a claim for remuneration for enabling the Client to carry out inspections.

16.2. In deviation from **section 16.1** the rights of control referred to in this clause shall continue to exist beyond the term of this Agreement and the general limitation period to the extent that and for as long as the Contractor processes personal data in accordance with **section 15.4** stores personal data.

16.3. This includes the right to enter the property, the business premises and the locations of the Contractor's information technology systems and to carry out inspections and tests there or have them carried out, as well as to inspect business documents and stored data and data processing programs, insofar as this is necessary for order control.

16.4. As a rule, inspections must be announced with a lead time of fourteen (14) days. In urgent cases, the Client may shorten the notice period to 24 hours. An urgent case exists in particular in the case of inspections by data protection supervisory authorities, other sovereign supervisory authorities or in the case of any reportable incidents.

16.5. The Contractor shall ensure that the Client or the auditors commissioned by the Client can satisfy themselves that the Contractor is complying with its obligations under Art. 28 GDPR.

17. Obligations of the Client

17.1. The Client shall be responsible for compliance with the statutory provisions applicable to it regarding the protection of personal data.

17.2. The Client shall inform the Contractor immediately and in full if it discovers errors or irregularities with regard to data protection regulations when checking the processing results.

17.3. If the Client is subject to the GDPR, the Client is obliged to keep a record of processing activities in accordance with Art. 30 GDPR. The Contractor's obligation to keep its own record of processing activities in accordance with Art. 30 (2) GDPR remains unaffected by this.

17.4. The Client shall designate a contact person responsible for data protection issues arising within the scope of the contract and provide their contact details for the purpose of direct contact.

18. Other obligations and provisions

18.1. The Contractor shall inform the Client as soon as a change of ownership, as defined below, is likely to occur. Insofar as the change of ownership requires an adjustment to this Agreement under the law of the European Union or the Federal Republic of Germany applicable to the Client, the Contractor shall agree the adjustment with the Client to the extent necessary. If the adjustment is refused by the Contractor or its conclusion is delayed, the Client may terminate the contract extraordinarily or withhold payments to the Contractor, regardless of the legal relationship, until the necessary adjustment agreement has been concluded. "Change of ownership" means any change in control of the Contractor, whether as a result of the acquisition of voting rights, conversions or agreements. The above shall apply accordingly to subcontractors of the Contractor.

18.2. The partial or complete assignment or transfer of claims, rights and obligations arising from this agreement by the Contractor is not permitted unless the Client has given its prior written consent. § Section 354a HGB remains unaffected.

18.3. Any amendment to this agreement must be made in writing to be effective. This also applies to any waiver of the written form requirement itself.

18.4. The law of the Federal Republic of Germany shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

18.5. The place of jurisdiction for all disputes arising from or in connection with this agreement and data protection-related disputes arising from system contracts is Frankfurt am Main. The Client shall also be free to assert any claims arising from this agreement at the court with subject-matter and local jurisdiction for the Contractor's registered office. Statutory regulations on exclusive jurisdiction remain unaffected

Annex 1: Subject-matter of the data processing

1. Subject-matter of the data processing

1.1. **Digital access management:** programming, customization, provision,

1.2. and operation of the software for digital access management. Hosting, support, and maintenance of the software. Project management and training.

2. Nature and purpose of processing

2.1. Purpose of processing: Digital access management including identity verification of authorized persons and other persons with temporary access authorization.

2.2. Type of processing:

- Recording the names and identification features of individuals who wish to enter a site, building or part of a building of the Client
- Verification of government issued photo ID documents
- Capture a photograph of the person for comparison with the ID document
- Recording information on the issue of access media issued to these persons and assigned access profiles
- Storage of this data for a period specified by the Client

2.3. The Contractor shall anonymize and evaluate data from the essentry platform for the purpose of providing statistical overviews to the Client. This data is anonymized in accordance with the anonymization method of k-anonymity. The k=7 anonymization method is used. This means that 7 different data records of each category of data are required for them to be included in the statistical analysis.

3. Type of personal data

3.1.1. List of those affected

The following groups of persons are affected by data processing:

- Employees of the Client
- Authorized persons, interested parties, customers, suppliers and service providers of the Client

3.1.2. Data categories

The following types or categories of data are subject to collection, processing and/or use by the Contractor:

No.	Data field name	Group of people	Data type according to deletion concept
001	First name	Authorized persons	Master data of the authorized persons
002	Surname	Authorized persons	Master data of the authorized persons
003	Company	Authorized persons	Master data of the authorized persons
004	Email address	Authorized persons	Master data of the authorized persons
005	Date of birth (optional, can be deactivated)	Authorized persons	Master data of the authorized persons
006	ID number (optional, can be deactivated)	Authorized persons	Master data of the authorized persons
007	Cut-out photograph of the authorized person from the identification document	Authorized persons	Cut-out photograph of the authorized person from the identification document
008	Photo of the authorized person taken by the self-service kiosk	Authorized persons	Photo of the authorized person taken by the self-service kiosk
009	First name	Users / employees / access managers	Employee data
010	Surname	Users / employees / access managers	Employee data

No.	Data field name	Group of people	Data type according to deletion concept
011	Email address	Users / employees / access managers	Employee data
012	Password	Users / employees / access managers	Employee data
013	Start time of the appointment	Authorized persons / persons responsible for access	Access data
014	End time of the appointment	Authorized persons / persons responsible for access	Access data
015	Check-in time	Authorized persons / persons responsible for access	Access data
016	Check-out time	Authorized persons / persons responsible for access	Access data
017	Name of the person responsible for access	Authorized persons / persons responsible for access	Access data
018	Location of the appointment	Authorized persons / persons responsible for access	Access data

If necessary, further user-defined data fields can be collected, processed and stored as part of the "master data of authorized persons" if the customer's administrator activates further data in the essentry SaaS platform for querying at the self-service kiosk or the reception dashboard.

Annex 2: Security of processing

1. Pseudonymization and encryption of personal data (Art. 32 section 1 lit. a GDPR)

1.1. **Pseudonymization:** Processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to technical and organizational measures.

Description of the measures taken:

- No direct pseudonymization of personal data can take place in order to fulfill the purpose of the order.
- Evaluations and queries for statistical purposes, are carried out anonymously.
- The application collects pseudonymized usage and traffic data on the server side. This information is not merged with the bearer (user) of the pseudonym except for provision of the service features that require this.

1.2. **Encryption:** Use of procedures and algorithms that convert the content of personal data into a non-readable form using digital or electronic codes or keys. Symmetric and asymmetric encryption techniques can be used:

Description of the measures taken:

- Encryption of all data "in transit" (during transmission) and "at rest" (stored on the hard disk). Only strong cryptographic methods are used.
- The Cloud KMS (Key Management Service) is used to store the keys of the encrypted databases. This protects the keys on special hardware security modules (HSMs). The keys do not leave these hardware modules and access to them is fully logged.
- TLS encryption
- cloud.google.com/security
- images.apple.com/business/docs/iOS_Security_Guide.pdf
- android.com/intl/en_en/security-center/
- HTTPS is used for the connection from the user's browser to the essentry servers. The specific version of the protocol and the type of encryption depend on the browser used. The essentry servers only accept secure protocols.

2. Measures to protect confidentiality (Art. 32 section 1 lit. b GDPR)

2.1. **Access control:** Technical and organizational measures for access control, in particular for the legitimation of authorized persons:

Description of the measures taken:

- Protection of physical access to data centers through structural measures and a locking system
- Personal reception of customers and authorized persons
- Authorized persons are accompanied or supervised
- Sensitive company areas and rooms in which no employees are working are locked

Organizational measures:

- internal documentation and specifications for contract fulfillment, e.g. internal guidelines and instructions on data security and data protection
- Internal documentation and guidelines on data protection and data security

2.2. **Access control:** Technical (password / password protection) and organizational (user master data record) measures with regard to user identification and authentication:

Description of the measures taken:

- The data processing systems are protected against unauthorized use by log-in and authorization procedures.
- Password security includes personalized and automated login procedures.
- Length and complexity requirements for passwords.

- Access to the essentry SaaS platform via mobile systems and end devices only takes place via secure and encrypted lines and connections.

2.3. **Access control:** Demand-oriented design of the authorization concept and access rights as well as their monitoring and logging:

Description of the measures taken:

- Access authorizations for employees to the IT systems are assigned restrictively.
- Our employees only receive the authorizations that they actually need for their work.
- Employee access authorizations to the servers with customer data are restricted to what is absolutely necessary in accordance with the principles of need-to-know and least privilege. Developers only have access to test systems on which they can test new features. Only tested new features are transferred by an admin to the servers on which essentry is running.
- essentry servers are protected against hacking attacks by several defense mechanisms including a firewall.

2.4. **Separation control:** Measures for separate processing (storage, modification, deletion, transmission) of data with different purposes:

Description of the measures taken:

- Data is stored on Google Cloud IT systems that are logically separate from data of other Google Cloud customers. cloud.google.com/security/

3. Measures to protect integrity (Art. 32 section 1 lit. b GDPR)

3.1. **Transfer control:** Measures during transportation, transfer and transmission or storage on data carriers (manually or electronically) as well as during subsequent verification:

Description of the measures taken:

- Transport encryption (TLS) is implemented for the transfer of personal data from the respective end device to the server.
- A subsequent check of the transfer control can also be carried out by viewing the log files.

3.2. **Input control:** Measures to subsequently check whether and by whom data has been entered, changed or removed (deleted):

Description of the measures taken:

- A subsequent check of the input control can also be carried out by viewing the log files.

4. Availability and resilience of systems and services (Art. 32 lit. b GDPR)

4.1. Availability control

Description of the measures taken:

- The data backups of our IT systems are carried out according to a binding data backup concept. A backup of the databases is made daily between 1:00 am and 3:00 am. It is stored for 30 days and is encrypted with AES256.
- The Client's customer data is processed in the Google Cloud. Reference is made here to Google's availability and resilience measures.
cloud.google.com/compute/
cloud.google.com/storage/
- The files requiring storage are stored redundantly at different locations to prevent loss. In addition, certain critical objects are versioned, which means that the replacement or deletion of a file is logged and the old file is not lost but remains stored. All stored files are encrypted with AES256.
- In the Google Cloud, computing capacity is automatically increased in the event of a sharp increase in requests or users.
- Every change to the configuration is first tested on the test systems and changes are saved in log files for traceability. Regular security scans of the servers are performed. Basic configurations of the communication paths between instances are carried out by defined administrators.

4.2. Availability of the IT systems used

Description of the measures taken:

- Reasonable measures for fire protection, power supply, air conditioning, data backup, disaster recovery, etc. have been taken for our IT systems as part of an emergency concept.
- The Kubernetes cluster scheduler distributes the instances of the software in such a way that the different instances always run on different servers. A hardware defect therefore generally does not lead to the essentry system becoming unavailable.
- The Client's customer data is processed in the Google Cloud. Reference is made here to Google's availability and resilience measures.
cloud.google.com/compute/
cloud.google.com/storage/

5. Measures to restore the availability of and access to personal data in the event of a technical incident (Art. 32 lit. c GDPR)

5.1. Recovery / backup systems

Description of the measures taken:

- Appropriate measures for fire protection, power supply, air conditioning, data backup, disaster recovery, etc. have been taken for our IT systems as part of an emergency concept. A recovery time of 24 hours is guaranteed.
- The Client's customer data is processed in the Google Cloud. Google guarantees an availability of over 99.99%. In addition, reference is made to the measures taken by Google to restore availability. cloud.google.com/compute/
cloud.google.com/storage/

6. Procedure for the regular review, assessment, and evaluation of technical and organizational measures; data protection by default (Art. 32 section 1 lit. d GDPR; Art. 25 section 1 GDPR)

6.1. Data protection management

Description of the measures taken:

- A data protection management system (DPMS) is in use. The DPMS is provided by the Contractor's data protection officer and operated together with the Contractor. Our procedures are regularly reviewed, assessed, and evaluated as part of resubmissions and regular meetings. Depending on the type of processing, these measures are carried out after 3, 6 or a maximum of 12 months.

6.2. Data protection-friendly default settings (Privacy by Default)

Description of the measures taken:

- Default settings are protective of data. Client-specific development is carried out on the instructions of the Client. Data subjects can obtain information about the use of their data at any time when using the software/app with the help of the data protection declaration.
- The Client specifies the categories of data to be collected.

6.3. **Order control:** Measures (technical / organizational) to delimit the competencies between Client and Contractor:

Description of the measures taken:

- When processing personal data, contracts are concluded with subcontractors in accordance with Art. 28 GDPR / EU Model Clauses.

Annex 3: Contact persons

Responsible and authorized persons of the Client and Contractor. Contractor: Essentry GmbH

Instruction recipient	Name	Email	Phone
CEO	Dr. Dennis Lips	dennis.lips@essentry.com	will be announced separately
CTO	Christian Böhlke	christian.boehlke@essentry.com	will be announced separately

Other functions	Name	Email	Phone
External Data Protection Officer	Philipp Rothmann	privacy@essentry.com	will be announced separately
External Information Security Officer	Philipp Rothmann		

Client shall inform Contractor of the persons responsible and authorized to issue instructions accordingly.

Annex 4: Subcontractors

Overview of all subcontractors working for the Contractor who directly collect, process and/or use the Client's data.

The following subcontractors work with the consent of the Client:

Subcontracting taker	Address	Field of activity
Google Ireland Limited	Gordon House, Barrow Street Dublin, D04 E5W5, Ireland	Hosting of the databases and servers in Germany.
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy 1855, Luxembourg	Sending e-mails and generating name tags for the printer; photo comparison; data processing takes place within the EU
Cubefinity GmbH Product NinjaOne	Stanisla-Kist-Str. 14A 94330 Aiterhofen Deutschland	Management of kiosk devices including the installation of app and system updates, assignment of customer and location-specific profiles and remote monitoring in the event of problems and other support cases. Data processing and storage takes place in the EU.
Twilio Inc.	375 Beale Street Suite 300 San Francisco CA 94105, USA	Sending SMS and (video) telephony service. The subcontractor can only be used if the functionality is explicitly ordered.

Annex 5: Notification form for data protection breaches

Name (Contractor) Address (Contractor)

Name (Client) Address (Client)

More detailed description of the contractual relationship concerned:

Period of the incident (date, time):

Description of the data protection incident:
(personal data breach)

Personal data concerned:
(according to data categories)

Number of persons affected (approximate):

Number of data records affected (approximate):

Affected IT systems:

Responsible department / responsible IT department if applicable:

Name and contact details of the data protection officer or other contact point:

Author and date of the message:

Who has already been informed and by whom:
(e.g. data protection officer, data protection supervisory authority, etc.)

Learn about this through (source):

Description of the likely consequences of the data protection incident:

Description of the immediate measures taken by the Contractor to rectify the problem:

Proposal for measures to be taken:

Measures to mitigate possible adverse effects:

Overall risk:

Legally binding confirmation of the correctness and completeness of the above information:

Place, date Signature Signature (Data Protection Officer)