Data Processing Agreement Pursuant to Art. 28 GDPR

between

CLIENT

– referred to in the following as "Client" –

and Infopark AG, Kitzingstraße 15, 12277 Berlin

– referred to in the following as "Contractor" –

§ 1 Preamble, scope, definitions

(1) This Agreement details the rights and obligations of the Client and Contractor within the framework of contract data processing.

(2) This Agreement applies to all activities in which the employees of the Contractor or companies commissioned by the Contractor (subcontractors) process personal data on behalf of the Client.

(3) The terms used in this Agreement must be interpreted as defined in the EU General Data Protection Regulation (GDPR). Where statements are required "in writing" in the following, the written form shall be as defined in Section 126 German Civil Code (BGB). Statements can also take place in an alternative form, provided appropriate verifiability is guaranteed.

§ 2 Object and duration of processing

(1) Object
The Contractor accepts processing as follows:

- Storage of customer data (exact data are determined in the specific project and are subject to change)
- Storage of contacts for authentication and authorization in Scrivito (and on the website)
- Processes explicitly commissioned by the Client

Processing shall take place according to the Infopark quotation 201xxxxxx dated 201x-xx-xx (referred to in the following as the "Main Contract").

(2) Duration
Duration of processing shall be based on the term of the Main Contract.

§ 3 Nature and purpose of data collection, processing or use

(1) Nature and purpose of processing
Processing shall be as follows: collection, organization, storage, contractual use, erasure of data.

Processing takes place for the following purpose:

- Content editing and delivery
- Troubleshooting
- Availability monitoring
- Performance Analysis
- Analysis of customer visits and website optimization (integration of the code only - evaluation by the Client)
- Providing maps for driving directions and location search

(2) Types of data
The processing of personal data refers to the following types/categories of data

□ Personal master data
□ Communication data (e.g. telephone, email)
□ Contract master data (contractual relationship, pertaining to products or contracts)
□ Customer history
□ Contractual remuneration and payment data
□ Planning and control data
□ Informational data (from third parties, e.g. credit agencies or from public directories)
□ Recipients and senders of messages addressed to or sent by the Client

(3) Categories of data subjects
The group of data subjects affected by the processing of personal data within the framework of this Agreement includes:

□ Customers
□ Interested persons
□ Subscribers
□ Employees
□ Suppliers
□ Contact persons
□ Recipients and senders of messages addressed to or sent by the Client

§ 4 Scope of application and responsibilities

(1) The Contractor shall process data on behalf of the Client. This shall include all activities detailed in the Agreement and the statement of work. Within the framework of this Agreement, the Client shall be solely responsible for compliance with the applicable statutory requirements and

data protection, including, but not limited to, the lawfulness of disclosing data to the Contractor and the lawfulness of data processing (»Controller« in the meaning of Art. 4. paragraph 7 GDPR).

(2) The individual instructions on contract processing shall, initially, be as detailed in the Agreement. The Client shall subsequently be entitled to, in writing or in a machine-readable format (in text form), modify, amend or replace such individual instructions by issuing such instructions to the point of contact designated by the Contractor. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. Instructions issued orally shall be confirmed in writing or in text form without undue delay.

(3) Where additional costs are incurred due to individual instructions, especially such as exceed the contractually agreed statement of work, the Contractor shall receive remuneration.

§ 5 Contractor’s obligations

(1) Except where expressly permitted by Article 28 paragraph 3 point (a), the Contractor shall process data subjects’ data only within the scope of the statement of work or on the instructions issued by the Client. Where the Contractor believes that an instruction would be in breach of applicable law, the Contractor shall notify the Client of such belief without undue delay. The Contractor shall be entitled to suspend performance on such instruction until the Client confirms or modifies such instruction.

(2) The Contractor shall, within its scope of responsibility, arrange its internal organization so that it satisfies the specific requirements of data protection. It shall implement technical and organizational measures to ensure the adequate protection of the Client’s data, which measures shall fulfil the requirements of the General Data Protection Regulation (Art. 32 GDPR). The Contractor shall implement technical and organizational measures and safeguards to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services used in connection with the processing. The Client is familiar with these technical and organizational measures, and it shall be the Client’s responsibility that such measures ensure a level of security appropriate to the risk (Annex 1).
The Contractor reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

(3) The Contractor shall support the Client, insofar as agreed upon by the parties, and where possible for the Contractor, in fulfilling data subjects’ requests and claims, as detailed in Chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR. The Contractor is entitled to demand remuneration for support services not included in the statement of work or that are due to misconduct on the part of the Client.

(4) The Contractor warrants that all employees involved in contract processing of the Client’s data and other such persons as may be involved in contract processing within the Contractor’s scope of responsibility shall be prohibited from processing data outside the scope of instructions. Furthermore, the Contractor warrants that any person entitled to process personal data has

undertaken a commitment to secrecy or is subject to an appropriate statutory obligation of secrecy. All such secrecy/confidentiality obligations shall survive the end of the contract processing.

(5) The Contractor shall notify the Client, without undue delay, if the Contractor becomes aware of breaches of the protection of the Client's personal data.
The Contractor shall implement the measures necessary for securing the data and for mitigating potential negative consequences for the data subject; the Contractor shall coordinate such efforts with the Client without undue delay.

(6) The Contractor shall notify the Client of the contact person for data protection issues arising in the context of the Agreement.
The following person is appointed data protection officer for the Contractor:

Mr Stephan Hartinger
Coseco GmbH
Telephone: +49 (0)8232 80988-70
Email: datenschutz@coseco.de

The Client must be informed without undue delay of any change in the data protection officer.

(7) The Contractor warrants that it will fulfil its obligations under Art. 32 paragraph 1 point (d) to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.

(8) The Contractor shall rectify or erase data if instructed to do so by the Client and where covered by the scope of instructions. Where erasure that is consistent with data protection requirements or a corresponding restriction of processing is impossible, the Contractor shall, based on the Client's individual instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material, or return the same to the Client.
In specific cases designated by the Client, such data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.

(9) The Contractor shall, upon termination of contract processing and upon the Client's instructions, return all data, carrier media and other materials to the Client or delete the same.
In case of testing and discarded material, no instruction shall be required.
The Client shall bear any extra costs caused by deviating requirements in returning or erasing data.

(10) Where a data subject asserts a claim against the Client in accordance with Art. 82 GDPR, the Contractor shall support the Client in defending against such claims, where possible.

§ 6 Client’s obligations

(1) The Client shall notify the Contractor, without undue delay and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by the Client in the results of the Contractor’s work.

(2) Section 3 para. 10 shall apply accordingly to claims asserted by data subjects against the Contractor in accordance with Article 82 GDPR.

(3) The Client shall inform the Contractor of the contact person for any issues related to data protection arising out of or in connection with the Agreement.

§ 7 Enquiries by data subjects

(1) Where a data subject asserts claim for rectification, erasure or access against the Contractor, and where the Contractor is able to correlate the data subject to the Client based on information provided by the data subject, the Contractor shall refer such data subject to the Client. The Contractor shall forward the data subject’s claim to the Client without undue delay. The Contractor shall support the Client, where possible, and based upon the Client’s instruction, insofar as agreed upon. The Contractor shall not be liable in cases where the Client fails to respond to the data subject’s request in total, correctly, or in a timely manner.

(2) The Client must reimburse the Contractor for verified costs incurred by the Contractor in the provision of support services according to paragraph 1.

§ 8 Options for documentation

(1) The Contractor shall document and prove to the Client by appropriate means its compliance with the obligations agreed upon in this Data Processing Agreement.

(2) Where inspections and audits by the Client or an auditor appointed by the Client are necessary in individual cases, such audits and inspections will be conducted during regular business hours, and without interfering with the Contractor’s operations, upon prior notice, and with observation of an appropriate notice period. The Contractor may also determine that such audits and inspections shall be subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organizational measures and safeguards that are implemented. The Contractor shall be entitled to object to the appointment of auditors, insofar as they are competitors of the Contractor.
The Contractor shall be entitled to request remuneration for its support in conducting inspections, provided such remuneration has been agreed upon in the Agreement. As a rule, the Contractor’s time and effort for such inspections shall be limited to one day per calendar year.

(3) Where a data protection supervisory authority or another supervisory authority with statutory competence for the Client conducts an inspection, paragraph 2 above shall apply accordingly. The

execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the German Criminal Code (StGB).

§ 9 Subcontractors

(1) The Contractor shall use subcontractors as further processors only where approved in advance by the Client.

(2) A subcontractor relationship shall be subject to consent where the Contractor commissions further contractors with all or part of the performance agreed upon in the Agreement. The Contractor will, to the extent that is necessary, enter into agreements with these third parties to ensure appropriate data protection and information security. The Contractor shall not require consent for the commissioning of subcontractors that merely provide ancillary services to support the services provided in accordance with the Main Contract, even where it is not possible to exclude access to the Client’s data. The Contractor shall conclude industry-standard confidentiality undertakings with these subcontractors.

(3) The Client is only entitled to refuse consent for good cause that must be demonstrated to the Contractor.

(4) In accordance with Art. 28 paragraphs 2–4 GDPR, the Client hereby agrees to the commissioning of the subcontractors listed in Annex 2 as a “general written authorisation”.

(5) Where the Contractor commissions work from subcontractors, it shall be the responsibility of the Contractor to transfer its obligations under data protection laws to the subcontractors as set forth in this Agreement.

(6) The Contractor will notify the Client in advance of any intended addition of new subcontractors or replacement of current subcontractors, whereby the Client shall have a right of objection to these changes (Art. 28 paragraph 2 GDPR). Consent will be deemed to have been provided insofar as an objection is not raised within 14 days of announcement.

§ 10 Obligations to inform, mandatory written form, choice of law

(1) Where the data become subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in the Contractor’s control, the Contractor shall notify the Client of such action without undue delay. The Contractor shall, without undue delay, notify all pertinent parties in such action that any data affected thereby is the Client’s sole property and area of responsibility, the data is at the Client’s sole disposition, and that the Client is the » controller« in the meaning of the General Data Protection Regulation.

(2) No modification of this annex and/or any of its components – including, but not limited to, the Contractor’s representations and warranties, if any – shall be valid and binding unless made in

writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that it is a modification or addition to these provisions. This shall apply also to the waiver of this mandatory written form.

(3) In case of any conflict, the provisions of this annex on data protection shall take precedence over the provisions of the Agreement. Where individual provisions of this annex are invalid, the validity of the other provisions of this annex shall not be affected.

(4) German law applies.

Client	Contractor
	Berlin,
Place, date, signature	Place, date, signature

Annex 1

General description of the technical and organizational measures

1. Confidentiality (Art. 32 paragraph 1 point (b) GDPR)

The risk of physical, tangible or intangible damage, i.e. the risk of impairing the rights and freedoms of data subjects, must be mitigated.

Admission control

Technical and organizational measures:

- Admission control to the server rooms is guaranteed by the layout of the individual data centres and the control systems installed by the operator.
- A personalised electronic key (transponder) secures admission to the premises of Infopark AG in Berlin during working hours.
- External service providers (security services) ensure permanent monitoring (locking of doors and motion alarms) outside of working hours.
- Moreover, the outer doors of the building are locked mechanically outside of working hours.
- Staff in the reception area are responsible for admission control during working hours.
- An optical surveillance system (CCTV) permanently monitors the entrance areas to the IT areas.

Entry control

Technical and organizational measures:

- Unauthorised use of the IT systems is prevented by:
  - Password issue
  - Logging of incorrect password entries.
- Each employee has a personal password that only they know. Disclosing this password is prohibited. Any passwords that have become known must be changed immediately.
- All relevant activities on the IT systems are logged automatically.
- The system administrator analyses random samples of the logs on a regular basis, also in the event of anomalies (e.g. particularly high activity).
- In regard to critical activities (e.g. system maintenance, software updates, backups), the following measures are in place to protect data transmission to and from the IT system against unauthorised use:
  - Review of known public keys when contact is made;
  - Encrypted data transmission (SSL/SSH);
  - Logging of system use and log analysis.

Access control

Technical and organizational measures:

- Unauthorised reading, copying, modification or erasure of data carriers is prevented by:
  - Software-based exclusion mechanisms (permissions concept);
  - Software-based monitoring of implausible use (monitoring);
  - Secure interfaces;
  - Other control mechanisms in the datacentre.
- Mobile data storage media are prohibited. Mobile backup media are not used.
- No data storage media are kept at the workplaces. Developers only have access to fictitious test data. Staff assigned to troubleshooting are able to access real data where necessary for troubleshooting.
- Persons entitled to use an IT system are restricted in their access to data and only have access to the data that falls under their personal permissions by means of the following mechanisms:
  - Automatic checking of access permissions by password;
  - Menu navigation based exclusively on permissions;
  - Differentiated access permissions for application programs;
  - Differentiated processing capabilities (read/edit/delete).

Separation control

Technical and organizational measures:

- Personal data may only be used for the purpose for which it was originally collected.
- The separate storage of data that is collected for different purposes is guaranteed by:
  - Software-based exclusion (Client separation; multitenancy architecture);
  - The database principle; separation by access policy;
  - Separation of test and productive data;
  - Separation of development and productive programs.

Pseudonymisation (Art. 32 paragraph 1 point (a) GDPR; Art. 25 Paragraph 1 GDPR)

Technical and organizational measures:

- As processor, Infopark AG does not take any measures for pseudonymisation beyond the measures taken by the controller within the framework of contracting.

2. Integrity (Art. 32 paragraph 1 point (b) GDPR)

Transfer control

Technical and organizational measures:

- The policy does not include physical dispatch of data storage media.

- Private data storage media must not be used in the datacentre (datacentre policy).
- Magnetic data storage media that are no longer needed are destroyed by multiple overwrites (datacentre policy).
- Unauthorised reading, copying, modification or removal of data during data transmission is prevented by:
  - SSL, i.e. SSH encryption during data transmission;
  - Completeness checks, where relevant;
  - Establishment of transport connections only between defined systems secured by certificates.
- The transport procedures automatically confirm receipt of data in the software.
- All sensitive data intended for transport is encrypted.
- Personal data is only transmitted using the following services:
  - Routinely WWW (HTTPS);
  - Other services and transport procedures that satisfy the intended purposes and are equivalent to or better than the current state-of-the-art in security technology.
- The documentation of transmission points and pathways provides information on the points at which data transmission systems are used to transmit data.

Input control

Technical and organizational measures:

- It is possible to conduct retroactive checks and to identify whether and by whom data is entered, changed or removed in the IT system, namely by means of:
  - User identification;
  - Logging of data input (processing logs).

3. Availability and resilience (Art. 32 paragraph 1 point (b) GDPR)

The risk of physical, tangible or intangible damage, i.e. the risk of impairing the rights and freedoms of data subjects, also through illegal or negligent actions, due to non-availability of data processed under a Data Processing Agreement must be mitigated.

Availability control

Technical and organizational measures:

- The protection of data against coincidental destruction or loss is guaranteed by:
  - The use of RAID volumes;
  - Software-based exclusion: distribution of the servers for independent and autonomous fulfilment of tasks (shared nothing architecture);
  - Redundant incremental database and system backups;
  - A backup schedule that adequately reflects changes in data based on use;
  - Redundant, separate storage of backup data;

    - Additional measures in the datacentre.
- There is a plan in place for disaster recovery.
- The system is operated at geographically separate datacentres (availability zones).

Resilience of the systems

Technical and organizational measures:

- The following security measures are in place:
    - Hardware and software firewall;
    - Intrusion detection system;
    - Programs to prevent, i.e. to detect, the penetration of viruses.

4. Process for regular testing, assessment and evaluation (Art. 32 paragraph 1 point d GDPR; Art. 25 paragraph 1 GDPR)

Processes must be put in place for the regular testing, assessment and evaluation of the effectiveness of technical and organizational measures designed to guarantee the security of processing.

Order control

Technical and organizational measures:

- Contract processing in the meaning of Art. 28 GDPR is not performed without suitable instruction by the Client, e.g. clear contractual wording, formal order management, strict selection of service provider, duty of pre-evaluation, performance of follow-up checks.
- No processing of personal data without corresponding instructions from the Client is guaranteed by written agreements on data protection between the Contractor and the Client, i.e. the datacentre.
- The Contractor informs the Client of serious changes in procedures.
- Securing of remote maintenance is irrelevant, as remote maintenance for the Client is not included.

Internal organization

Technical and organizational measures:

(a) Data protection management

- Employees may only process data in their areas of responsibility once an undertaking has been executed for adherence to data protection requirements.
- Internal codes of conduct and a data protection manual are in place.
- All employees complete e-learning courses in regular intervals as training measures and to raise awareness.

- Responsibilities and authorisations are defined for individual staff members in an organization flowchart, which is publicised in the company. It is reviewed by senior management in regular intervals within the framework of ISO 9001 certification.

(b) Incident management

- The data protection officer reviews and modifies when necessary adherence to the technical and organizational measures on an annual basis (audit).

(c) Technology design to ensure data protection

- Selection of data protection-friendly technology during procurement.

Annex 2

Subcontractors

The following subcontractors are commissioned with the provision of part services:

- Subcontractor 1 (company, contact details)
- Subcontractor 2 (company, contact details)