Contract for order processing

Between

the [company, adress, authorized representative]

as responsible person

(here referred to as **"client"**)

and

of **Ryte GmbH**, Paul-Heyse-Strasse 27, 80336 Munich

as contract processor

(referred to here as **"Contractor"**)

Preamble

The client wishes to commission the contractor with the services mentioned in § 3. Part of the contract implementation is the processing of personal data. In particular Art. 28 DSGVO makes certain demands on such contract processing. In order to comply with these requirements, the parties conclude the following agreement, the performance of which will not be remunerated separately, unless this has been expressly agreed.

§ 1 Definitions

(1) In accordance with Art. 4 Paragraph 7 of the DSGVO, the controller is the body which alone or jointly with other controllers decides on the purposes and means of processing personal data.

(2) According to Art. 4 Paragraph 8 DSGVO, a processor is a natural or legal person, authority, institution or other body which processes personal data on behalf of the controller.

(3) Pursuant to Art. 4 (1) DPA, personal data is defined as any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(4) Particularly sensitive personal data are personal data in accordance with Art. 9 DSGVO, from which the racial or ethnic origin, political opinions, religious or ideological beliefs or trade union membership of data subjects are evident, personal data in accordance with Art. 10 DSGVO on criminal convictions and offences or related security measures as well as genetic data in accordance with Art. 4 (13) DSGVO, biometric data in accordance with Art. 4 (14) DSGVO, health data in accordance with Art. 4 (15) DSGVO and data concerning the sexual life or sexual orientation of a natural person.

(5) According to Art. 4 Para. 2 DSGVO, processing is any operation or set of operations, whether or not automated, which is performed upon personal data, such as collection, recording, organisation, organisation, sorting, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction.

(6) Pursuant to Art. 4 para. 21 DSGVO, a supervisory authority is an independent state body established by a Member State pursuant to Art. 51 DSGVO.

§ 2 Information on the competent data protection supervisory authority

(1) The competent supervisory authority for the contracting entity is [name, insert contact details]

(2) The competent supervisory authority for the Contractor is the Bavarian State Office for Data Protection Supervision (BayLDA), Promenade 18, 91522 Ansbach, Germany, telephone: +49 (0) 981 180093-0, fax: +49 (0) 981 180093-800, e-mail: poststelle@lda.bayern.de

(3) The customer and the contractor and, if applicable, their representatives shall cooperate with the supervisory authority upon request in the performance of their duties.

§ 3 Subject matter of the contract

(1) The contractor provides services for the customer in the area of "web services". In doing so, the contractor receives access to personal data and processes them exclusively on behalf of and according to the instructions of the customer. The scope and purpose of the data processing by the Contractor are specified in the main contract. The main contract is referred to in its entirety. It is the responsibility of the Customer to assess the permissibility of the data processing.

(2) The parties conclude the present agreement in order to specify the mutual rights and obligations under data protection law. In case of doubt, the provisions of the present agreement shall take precedence over the provisions of the main contract.

(3) The provisions of this Agreement shall apply to all activities in connection with the main contract in which the Contractor and its employees or persons commissioned by the Contractor come into contact with personal data originating from the Customer or collected for the Customer.

(4) The term of this contract is based on the term of the main contract, unless the following provisions impose obligations or rights of termination that go beyond this.

§ 4 Right to issue instructions

(1) The contractor may only collect, process or use data within the scope of the main contract and in accordance with the instructions of the customer; this applies in particular with regard to the transfer of personal data to a third country or to an international organization. If the law of the European Union or of the Member States to which the contractor is subject obliges him to carry out further processing, he shall notify the customer of these legal requirements prior to processing.

(2) The customer's instructions are initially set out in this contract and may subsequently be amended, supplemented or replaced by individual instructions in writing or in text form (individual instructions). The client is entitled to issue corresponding instructions at any time. This includes instructions regarding the correction, deletion and blocking of data. The person authorized to issue instructions on the part of the client is [name, insert contact details]
In the event of a change or long-term inability of the persons named, the successor or representative must be named to the contractual partner in text form without delay.

(3) All instructions issued must be documented by both the customer and the contractor. Instructions that go beyond the performance agreed in the main contract shall be treated as a request for a change in performance.

(4) If the Contractor is of the opinion that an instruction from the Client violates data protection regulations, he must inform the Client of this immediately. The contractor shall be entitled to suspend the execution of the instruction in question until it is confirmed or amended by the customer. Contractor may refuse to carry out an obviously illegal instruction.

§ 5 Nature of the processed data, group of persons concerned

(1) In the course of the execution of the main contract, the contractor shall be granted access to the personal data specified in more detail below. These data include:

- First and last name(s)
- IP addresses
- Address
- Phone number
- email address
- Company of the employer

- Professional activity

(2) The group of persons affected by the data processing

- includes employees of the client

§ 6 Protective measures of the contractor

(1) The contractor is obliged to observe the legal provisions on data protection and not to pass on to third parties or suspend access to information obtained from the customer's area. Documents and data shall be secured against unauthorized access, taking into account the state of the art.

(2) The contractor shall design the internal organization within his area of responsibility in such a way that it meets the special requirements of data protection. He shall take all necessary technical and organizational measures for the appropriate protection of the customer's data in accordance with Art. 32 DS-GVO

The contractor reserves the right to change the security measures taken, whereby he shall ensure that the level of protection does not fall below the contractually agreed level.

(3) The contractor has been appointed as external data protection officer for data protection: ECOVIS L+C, Dr. Larissa von Paulgerg. Christoph-Rapparini-Bogen 25, 80639 Munich, dsb-muenchen(at)ecovis.de, +4989217516-700. The contractor has published the contact data of the data protection officer on his website.

(4) The persons employed by the Contractor for data processing are prohibited from collecting, processing or using personal data without authorization. The Contractor shall impose a corresponding obligation (obligation of confidentiality, Art. 28 para. 3 lit. b DS-GVO) on all persons entrusted by him with the processing and fulfilment of this contract (hereinafter referred to as employees) and shall ensure compliance with this obligation with due care. These obligations must be formulated in such a way that they remain in force after the termination of this contract or the employment relationship between the employee and the contractor. The customer must be provided with appropriate evidence of the obligations on request.

§ 7 Contractor's duty to inform

(1) In the event of malfunctions, suspicion of data protection violations or breaches of contractual obligations on the part of the contractor, suspicion of security-related incidents or other irregularities in the processing of personal data by the contractor, persons employed by him within the scope of the order or by third parties, the contractor shall inform the customer immediately in writing or in text form. The same applies to audits of the contractor by the data protection supervisory authority. The notification of a violation of the protection of personal data shall contain at least the following information:

> (a) a description of the nature of the personal data breach, specifying, where possible, the categories and number of persons concerned, the categories and number of personal data sets concerned
>
> (b) a description of the measures taken or proposed by the contractor to remedy the breach and, where appropriate, measures to mitigate its possible adverse effects.

(2) Contractor shall immediately take the necessary measures to secure the data and to mitigate the possible adverse effects on the data subjects, shall inform Customer thereof and request further instructions.

(3) In addition, the Contractor shall be obliged to provide the Customer with information at any time if his data are affected by a violation pursuant to paragraph 1.

(4) If the data of the Customer are endangered at the Contractor's premises by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Customer immediately, unless this is prohibited by court or official order. In this context, the contractor shall inform all competent authorities without delay that the authority to decide on the data lies exclusively with the customer as the "responsible party" within the meaning of the DS-GVO.

(5) The contractor shall inform the customer without delay of any significant change in the security measures pursuant to § 6 (2).

(6) The Customer shall be informed immediately of any change in the person of the external data protection officer for data protection.

(7) The contractor and, if applicable, his representative shall keep a register of all categories of processing activities carried out on behalf of the customer, which contains all the information required under Article 30(2) DS-GVO. The list shall be made available to the customer on request.

(8) The contractor shall participate to an appropriate extent in the preparation of the list of procedures by the customer. He must provide the customer with the necessary information in a suitable manner.

§ 8 Rights of control of the customer

(1) The customer has the right to carry out inspections in consultation with the contractor or to have them carried out by inspectors to be appointed in individual cases. He shall have the right to convince himself of the contractor's compliance with this agreement in his business operations by means of spot checks, which as a rule must be notified in good time.

(2) The contractor shall ensure that the customer can satisfy himself of the contractor's compliance with his obligations under Art. 28 DSGVO. The contractor undertakes to provide the customer with the necessary information on request and in particular to provide evidence of the implementation of the technical and organisational measures.

(3) The proof of such measures, which do not only concern the specific order, can also be provided by

- compliance with approved rules of conduct pursuant to Art. 40 DSGVO; and/or
- certification in accordance with a certification procedure pursuant to Art. 42 DSGVO; and/or
- current certificates, reports or report extracts from independent bodies (e.g. auditors, auditors, data protection officers, IT security department, data protection auditors, quality auditors); and/or
- a suitable certification through IT security or data protection audit (e.g. according to BSI basic protection).

(4) The effort of an inspection at the contractor's premises is generally limited to one day per calendar year. For additional checks which are not based on a concrete reason or a well-founded suspicion of a violation of personal data, the contractor can demand an appropriate remuneration.

§ 9 Use of subcontractors

(1) The contractor is only permitted to commission subcontractors to process the customer's data with the approval of the customer, cf. Art. 28 para. 2 DSGVO.

(2) Approval shall be granted to the contractor if the contractor informs the customer of the name and address as well as the intended activity of the subcontractor and if the subcontractor fulfils the requirements of § 9 para. 3 and para. 4 of this contract.

(3) The contractor undertakes to select the subcontractor carefully and in particular to check the effectiveness of his technical and organisational measures in accordance with Art. 32 DSGVO in advance and to document this.

The result of the documentation and the essential contents must be presented to the customer on his request.

(4) The commissioning of subcontractors who are based in third countries shall only be subject to the separate provisions of Art. 44 et seq. DSGVO. In this respect, the Contractor must provide the Customer with appropriate evidence upon request. This shall be done with the help of the EU standard contract clauses. It should be noted purely declaratory that these contracts must be drawn up in writing or, in accordance with the DSGVO, in electronic format pursuant to Art. 28 para. 4 and para. 9.

(5) The Contractor undertakes, within the scope of his possible duties, to check the compliance of his subcontractor with the data protection obligations, to document this and, if requested by the Customer, to hand over the essential parts of the documentation.

(6) According to the preceding preamble in conjunction with § 3 of the contract, the Customer is aware of the large number of subcontractors on the side of the Contractor. Due to the special field of business of the contractor, these are also necessary for the complete fulfilment of the contract. At the time of the conclusion of the GCU, the subcontractors are known to the contractor. These are managed according

to the following pattern: "Supplier", "Address", "DPA Status" and "Content". By signing the present contract, the Customer fully approves the subcontractors indicated in the list.

(7) Furthermore, the contractor undertakes to notify the customer of any significant change with regard to a possible extension, replacement or deletion of individual subcontractors. The customer is granted the right to make an objection (Art. 28 para. 2 sentence 2 DSGVO), which explicitly refers to the extension, i.e. the addition of a completely new subcontractor for a service that is sometimes not provided, and the replacement of an existing subcontractor. This does not affect the entrepreneurial decision-making authority of the contractor.

(8) The customer shall notify the contractor within three weeks after notification of the contractor whether he will make use of his right of objection. For this purpose, at least text form and, if the contractor exercises his right, the indication of an important reason for the objection is required. If the client - for whatever reason - does not exercise his right in time against the contractor, the subcontractor notified is deemed to be approved and added to the list of subcontractors at the end of the third working day.

(9) For any further outsourcing by a subcontractor, the above procedure shall apply accordingly.

(10) A subcontractor relationship in the sense of this provision shall not exist if the contractor commissions third parties with services which are to be regarded as purely ancillary services. These include, for example, postal, transport, cleaning, telecommunication and shipping services which are not in a concrete exchange relationship with the main service obligation.

§ 10 Inquiries and rights of affected persons,

(1) The contractor supports the customer as far as possible with suitable technical and organizational measures in the fulfillment of his obligations under Art. 12-22 as well as 32 and 36 DS-GVO.

(2) If a data subject asserts rights, such as the right to information, correction or deletion of his data, directly against the contractor, the contractor does not react independently, but refers the data subject to the customer immediately and awaits the customer's instructions.

§ 11 Liability

(1) In the internal relationship with the Contractor, the Customer alone shall be responsible to the affected party for the compensation of damages suffered by the affected party due to an inadmissible or incorrect data processing or use within the scope of the order processing, unless the violation of applicable data protection provisions and laws and/or this Agreement is the responsibility of the Contractor.

(2) The parties shall each release themselves from liability if one party proves that it is in no way responsible in any way for the circumstance by which the damage occurred to a person affected.

§ 12 Extraordinary right of termination

The customer may terminate the main contract in whole or in part without notice if the contractor fails to comply with his obligations under this contract, violates provisions of the DS-GVO intentionally or through gross negligence or is unable or unwilling to carry out an instruction of the customer. In the case of simple - i.e. neither intentional nor grossly negligent - violations, the customer shall set the contractor a reasonable deadline within which the contractor can remedy the violation.

§ 13 Termination of the main contract

(1) The Contractor shall return to the Customer after termination of the main contract or at any time at the Customer's request all documents, data and data carriers provided to him or - at the Customer's request, unless there is an obligation to store personal data under Union law or the law of the Federal Republic of Germany - delete them. This also applies to any data backups at the contractor. The contractor must keep documented proof of the proper deletion of any remaining data. Documents to be disposed of are to be destroyed with a shredder. Data carriers to be disposed of are to be irretrievably destroyed.

(2) The customer has the right to check the complete and contractually correct return or deletion of the data at the contractor in a suitable manner.

(3) The Contractor is obliged to treat the data which have become known to him in connection with the main contract confidentially even after the end of the main contract. The present agreement shall remain valid beyond the end of the main contract as long as the Contractor has personal data at its disposal which was provided to it by the Customer or which it collected for the Customer.

§ 14 Final provisions

(1) The parties agree that the objection of the contractor's right of retention within the meaning of § 273 BGB (German Civil Code) with regard to the data to be processed and the associated data carriers is excluded.

(2) Changes and amendments to this agreement must be made in writing. This also applies to the waiver of this formal requirement. The priority of individual contractual agreements remains unaffected.

(3) Should individual provisions of this agreement be or become invalid or unenforceable in whole or in part, the validity of the remaining provisions shall not be affected.

(4) This agreement is subject to German law. Exclusive place of jurisdiction is Munich, Germany.

(5) This contract for order processiong is a translation of the legally binding German version. In the event of any conflict or ambiguity, the wording of the German version shall prevail as legally binding.

[Place] , the	Munich, the .....
……...	……...
For the [client]	For Ryte GmbH

Documentation of "technical and organizational measures" (TOMs, English version)

This Document contains the English translation of the original legally binding German TOM Document. In the event of any conflict or ambiguity, the wording of the German version shall prevail as legally binding.

Measures for preventing unauthorized access to data processing systems where personal data is processed or used.

Key issue
Logging of on-site visitors
Transponder door lock system
Manual lock system
Secure locks
Careful screening of (cleaning) staff

Measures that are suitable to prevent data processing systems from being used by unauthorized persons.

Assignment of User permissions
Password Authentication for user
Disabled external interfaces (e.g. USB)
Key Access / handing over logged
Logging of on-site visitors
Antivirus software
Creation of User Profiles
Assignment of user profiles to internal it-systems
Remote Access via VPN
Secure mechanical locks
Hardware Firewall
Encryption of Hard-Disks (e.g Macbooks)
Software Firewall

Measures to ensure that those authorized to use a data processing system can only access the data subject to their authorization and that personal data cannot be read, copied, changed, or removed without authorization during processing, use, and after storage.

Erstellen eines Berechtigungskonzepts
Number of administrators reduced to the necessary minimum.
Physical erase of storage devices before reuse
Encryption of hard-disks
Permission management by System Administrator
Password-Policy
Secure storage of storage devices
Logging of destruction

Measures to ensure that data collected for different purposes can be processed separately.

Stored on physically different storage devices
Creation of an authorization concept
Providing the data records with purpose attributes / data fields
Logical client separation (software based)
Separation of Testing and Production Envriroment
Database Access-Policies

Measures that reduce the direct personal reference during processing in such a way that an assignment to a specific data subject is only possible with the addition of additional information. The additional information is to be kept separate from the pseudonym by means of suitable technical and organizational measures.

Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of a transfer or after the statutory deletion period has expired

Measures to ensure that personal data cannot be read, copied, changed or removed without authorization during electronic transmission or during their transport or storage on data carriers, as well as measures with which it can be checked and determined to which points a transfer of personal data is intended (i.e. no unauthorized reading, copying, changing or removing in the case of electronic transfer or transport, e.g. encryption, virtual private networks (VPN), electronic signature).

E-Mail transport encryption
Use of VPN
Permission management by system administrator
Documentation of the data recipients and the duration of the planned transfer or the deletion periods
Carefulness in the selection of transport personnel and vehicles

Measures that ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed, or removed in IT systems. (e.g. logging, document management).

Beschreibung des Eingabekontrollvorgangs:

Overview of the programs with which data can be entered, changed or deleted
Clear responsibilities for deletions
Traceability of inputs, changes, and deletions of data through individual user names (not user groups)

Measures to ensure that personal data is protected against accidental destruction or loss.

Uninterrupted power supply (UPS)
Fire and smoke alarm systems
Definition of database access permissions
Protection sockets for servers
Server rooms not under/close to sanitary facilities

Measures to ensure the ability to quickly restore and access to personal data in the event of a physical or technical incident.

Data recovery testing
A backup & recovery concept is in place

Measures that ensure data protection compliant and secure processing.

Central documentation of all procedures and regulations for data protection with access for employees as required (e.g. wiki, intranet)

Employees trained and committed to confidentiality / data secrecy
Internal / external IT security officer
Formal process for processing information requests from clients / user

Assistance in responding to security breaches.

Use of firewall and regular updates
Documentation of security incidents and data breaches
Involvement of the data protection officer in security incidents and data breaches
Specific Software-Developer to support security breach management (#cert team)

Privacy by design / Privacy by default.

Only necessary personal data is collected for the respective purpose.	Simple process for right of withdrawal through technical and organizational measures

Measures to ensure that personal data that is processed on behalf of the customer can only be processed in accordance with the instructions of the client. In addition to data processing, this also includes the implementation of maintenance and system support on-site and via remote maintenance. If the contractor uses service providers in the sense of order processing, the following topics must always be regulated with them.

Review of the security measures taken by the contractor and their documentation prior to commissioning	Selection of the contractor under due diligence aspects, especially with regard to data protection and data security
Conclusion of the necessary agreement for order processing or EU standard contract clauses	Obligation of the Contractor's employees to maintain data security
Written orders to the contractor	Obligation to appoint a data protection officer by the contractor if the obligation to order exists
Agreement on effective control rights towards the contractor	Regulations for the use of further subcontractors