

AGREEMENT CONCERNING ORDER PROCESSING

between

**John Smith Services
represented by John Smith
203 East 50th St., Suite 1157
NY 10022 New York
United States of America**

ProvenExpert customer number: 123

- hereinafter referred as "**Customer**" -

and

**Expert Systems AG
Represented by the Management Board Remo Fyda
Quedlinburger Str. 1
10589 Berlin**

- hereinafter referred to as "**Contractor**" -

The Customer and Contractor are jointly referred to below as "**Parties**" or individually as "**Party**".

PREAMBLE

The Contractor offers the provenexpert.com service that the Customer uses. For this purpose, a User Agreement (the "User Agreement") exists between the Parties that regulates the basic obligations of the Parties. This Agreement shall be concluded to take into account the data privacy requirements, in particular, the European General Data Protection Regulation (GDPR) [*Europäischen Datenschutzgrundverordnung (DS-GVO)*]. The User Agreement represents an order processing relationship according to Art. 28 DS-GVO. In order to specify the rights and obligations arising from the order processing relationship according to the legal obligation, the Contractual Parties shall conclude the following Agreement. The Contractual Parties shall also agree that the similar regulations of the German Federal Data Protection Act [*Bundesdatenschutzgesetz (BDSG)*] shall apply to this Agreement until the DS-GVO and any supplementary national laws in Germany take effect.

1. SUBJECT MATTER, TERM

- 1.1 The subject matter, type and purpose of the data processing are set forth in the User Agreement, which is referred to here.
- 1.2 The subject matter of the collection, processing and / or use of personal data includes the following data types / categories:
 - Personal master data (e.g. first name, last name)
 - Communication data (e.g. telephone, e-mail)
- 1.3 The group of people affected by the handling of the personal data within the scope of this order:
 - The customers, users, clients of the Customer
- 1.4 The term of this Agreement (duration) corresponds to the term negotiated in the User Agreement. This Agreement shall, in all cases, end automatically with the termination of the User Agreement. The right of both Parties to termination without notice for good cause shall remain unaffected.

2. TECHNICAL AND ORGANIZATIONAL MEASURES

- 2.1 The Contractor shall document the implementation of the required technical and organizational measures and submit the documentation to the Customer on request for examination. Upon acceptance by the Customer, the documented measures shall become the basis of the order. If

the examination/an audit of the Customer determines the need for adaptation, it must be implemented by mutual agreement.

- 2.2 The Contractor shall provide the security according to Art. 28, Section 3 lit. c, 32 DS-GVO, in particular in conjunction with Art. 5, Section 1 and Section 2 of DS-GVO. Overall, the measures to be taken include measures for ensuring data protection and ensuring a level of protection, which is suitable to the risk involved, with regard to the confidentiality, the integrity, the availability and the resilience of the systems. Here, the state-of-the-art, implementation costs and the type and scope as well as the purpose of the processing and the various probabilities of occurrence and severity of the risk for the rights and freedoms of individuals must be taken into consideration according to Art. 32, Section 1 of the DS-GVO. The particulars are stated in **Annex 1**.

- 2.3 The technical and organizational measures shall be subject to technical progress and further development. In this respect, the Contractor shall be permitted to implement alternative adequate measures. In this case, the security level of the defined measures must be satisfied or exceeded, but may not fall short of the defined the security level. Significant changes must be documented.

3. CORRECTION, LIMITATION AND DELETION OF DATA

- 3.1 The Contractor may not correct, delete or limit the processing of the data processed in the order without authorization. In fact, the Contractor may only do so according to the documented instruction of the Customer.
- 3.2 Provided this is included in the scope of services, the deletion concept, right to be forgotten, correction, data portability and information must be ensured by the Contractor immediately after the documented instruction of the Customer.

4. QUALITY ASSURANCE AND OTHER OBLIGATIONS OF THE CONTRACTOR

- 4.1 In addition to the compliance with the regulations of this order, the Contractor has legal obligations according to Art. 28 through 33 of the DS-GVO; in this respect, he shall ensure compliance with the following regulations, in particular:
- 4.1.1 Contact for data protection - The contact of the Contractor for all issues surrounding data protection is:

The Contractor shall inform the Customer of any changes regarding this person and/or contact details.

- 4.1.2 The safeguarding of confidentiality according to Art. 28, Section 3 page 2 lit. b, 29, 32, Section 4 of the DS-GVO. When performing the work, the Contractor shall only engage employees who are obligated to maintain confidentiality and who have been made aware of the data protection provisions that are relevant for them. The Contractor and all the Contractor's personnel who have access to personal data may only process this data according to the instruction of the Customer, including the authorizations granted in this Agreement; unless they are legally required for processing.
- 4.1.3 The cooperation with the supervisory authorities. On request, the Customer and Contractor shall work together with the supervisory authorities for fulfilling their tasks.
- 4.1.4 The immediate information of the Customer about control procedures and measures of the supervisory authorities provided they refer to this order. This shall also apply if a responsible authority is conducting an investigation within the scope of a regulatory or criminal proceeding with regard to the processing of personal data during the order processing at the Contractor's location.
- 4.1.5 The support of the Customer. If the Customer in his part is subject to an audit by the supervisory authorities, a regulatory or criminal proceeding, the liability claim of an affected person or a third party or another claim in conjunction with the order processing at the Contractor's location, the Contractor must support him to the best of his ability.
- 4.1.6 The control of the internal processes. The Contractor shall regularly control the internal processes as well as the technical and organizational measures to ensure that the processing takes place in his area of responsibility according to the requirements of the application data protection law and to ensure the protection of the rights of the affected person.

4.1.7 The traceability of the technical and organizational measures taken for the Customer within the scope of his audit authorizations according to Section 5 of this Agreement.

5. AUDIT RIGHTS OF THE CUSTOMER

5.1 The Customer has the right to carry out inspections in consultation with the Contractor or have them carried out by auditors appointed by him in individual cases. He has the right to carry out random checks, which must be announced at least 14 days in advance, in order to audit the compliance of this Agreement by the Contractor at his business during normal business hours (weekdays except for Saturdays between 9 a.m. and 6 p.m.). The Customer shall bear the costs for this.

5.2 The Contractor shall ensure that the Customer can audit the compliance of the Contractor's obligations according to Art. 28 of the DS-GVO. On request of the Customer, the Contractor undertakes to provide the necessary information and in particular, verify the implementation of the technical and organizational measures.

6. DISCLOSURE IN CASE OF VIOLATIONS ON BEHALF OF THE CONTRACTOR

6.1 The Contractor shall support the Customer in ensuring compliance with the obligations specified in Art. 32 through 36 of the DS-GVO for the protection of personal data, reporting obligations in case of data breaches, data protection impact assessments and previous consultations. Among other things, this includes:

- Ensuring a suitable level of protection through technical and organizational measures that take into consideration the circumstances and purpose of the processing as well as the predicted probability and severity of a potential legal violation due to security gaps and allow for the immediate detection of relevant violation incidents;
- The obligation of immediately reporting infringements concerning personal data to the Customer;
- The obligation of supporting the Customer within the scope of his obligation to furnish information to affected parties and to immediately provide him with the information relevant within this context;

- The support of the Customer for his data protection impact assessment.

7. CUSTOMER'S AUTHORITY TO ISSUE INSTRUCTIONS

- 7.1 The handling of data shall be performed exclusively according to Section 1 of this Agreement and according to the instruction on the part of the Customer.
- 7.2 If the Contractor is of the opinion that an Instruction violates statutory data protection regulations, the Contractor shall promptly inform the Customer. In this case, the Contractor shall be authorized to suspend the implementation of the corresponding instruction until the Customer has confirmed or modified the instruction.

8. LOCATION OF THE DATA PROCESSING AND USAGE

- 8.1 The data is processed and used by the Contractor in the territory of the Federal Republic of Germany, in a member state of the European Union or in another Contracting State of the Agreement on the European Economic Area.
- 8.2 Any outsourcing in a third country requires the prior consent of the Customer and may only take place if the special prerequisites of article 44 ff. of the DS-GVO are met.

9. SUBCONTRACTUAL RELATIONSHIPS, ARTICLE 28, SECTION 4 OF THE DS-GVO

- 9.1 The Contractor may only include the Subcontractor in the processing or uses of personal data of the Customer with the prior written consent of the Customer.
- 9.2 The Customer has already issued this consent for the following Subcontractors in advance on conclusion of this Agreement:

Name and address of the Subcontractor	Description of the partial services:
Telekom Deutschland GmbH P.O. Box 30 04 64 53184 Bonn, Germany	Hosting services

MessageBird B.V. Baarsjesweg 285-H 1058 AE Amsterdam, The Netherlands	SMS Service Provider
--	----------------------

- 9.3 The engagement of Subcontractors requires a written order by the Customer. The Contractor must design the contractual Agreements with the Subcontractor so that they satisfy the data protection provisions of this Agreement.
- 9.4 If the Subcontractor would like to engage additional Subcontractors, the provisions according to Clause 9 apply.
- 9.5 Services that the Contractor uses with third parties as an auxiliary service for supporting the execution of the order shall not be considered as Subcontractor relationships according to this regulation. This includes, e.g. telecommunication services, cleaning personnel. The Contractor, however, undertakes to make suitable and lawful contractual Agreements and take control measures to ensure the protection and the security of the Customer's data, also for auxiliary services assigned to third parties.
- 9.6 If the Subcontractor performed the negotiated service outside the EU/ and the European Economic Region, the Contractor shall ensure the compliance with the data protection regulations by taking suitable measures according to Clause 8.2 of this Agreement.

10. LIABILITY

- 10.1 Claims for damages of the Customer due to the breach of obligations and from illegal acts as well as claims to compensation for futile expenses shall be excluded both with regard to the Contractor as well as his respective vicarious agents and assistants.
- 10.2 This limitation of liability shall not apply if the damage was caused through wilful intent or gross negligence or for damage arising from the damage to life, body, or health if the Contractor is responsible for the breach of obligation.
- 10.3 Moreover, the limitation of liability according to Section 10.1 shall not apply for damage that is attributed to the absence of an assured characteristic or for liability designated according to

the German Product Liability Act as well as in case of the violation of essential contractual obligations whose correct performance is essential to making the contract possible at all and whose compliance can be regularly relied upon by the Contractual Parties and whose violation impedes the injured party's ability to fulfil the purpose of the Agreement. In case of the violation of essential contractual obligations, the liability is limited to the damages which must be typically expected.

11. DELETION OF DATA AND THE RETURN OF DATA STORAGE MEDIA

On termination of this Agreement, the Contractor shall, on written request, immediately save all data files managed for the Customer on data storage media and hand over these data storage media to the Customer. Rights of retention of Contractor concerning such files shall be excluded. On written request of the Customer, the Contractor must completely delete the data files managed for the Customer, also including backup copies on the data carrier systems. The documentation verifying the deletion must be submitted on request. The Customer shall bear the costs for this.

12. FINAL PROVISIONS

- 12.1 Changes or additions to this Agreement shall require written form to become effective and must be signed by both parties. Terminations shall require written form to become effective. Changes and additions must be explicitly marked as such.
- 12.2 In the event that a provision of this Agreement should prove to be ineffective, this shall not affect the effectiveness of the remaining provisions. The Parties shall immediately replace the invalid provision with an effective provision that comes as close as possible to the economic meaning of the invalid provision.
- 12.3 This Agreement is subject to the law of the Federal Republic of Germany under exclusion of German International Civil Law.



12.4 The place of jurisdiction for all disputes arising from and in conjunction with this Agreement is Berlin.

New York, May 23, 2018

Berlin, May 22, 2018

Customer

CEO – Remo Fyda

Contractor

ANNEX 1– TECHNICAL AND ORGANIZATIONAL MEASURES**1. Confidentiality (Art. 32, Section 1 lit. b of the DS-GVO)**

- Access control
No unauthorized access to data processing facilities, e.g.: magnet or chip cards, keys, electrical door openers, factory security, doormen or gatekeepers, alarm systems, video systems;
- Access control
No unauthorized system use, e.g.: (secure) passwords, automatic locking mechanisms, two factor authentication, encryption of data storage media;
- Access control
No unauthorized reading, copying, changes or removal within the system, e.g. authorization concepts and access rights, logging of access in line with demands;
- Separation control
Separate processing of data that was collected for different purposes, e.g. multi-client capability, sandboxing;
- Pseudonymization (Art. 32, Section Abs. 1 lit. a of the DS-GVO; Art. 25, Section 1 of the DS-GVO)
The processing of personal data in such a manner that the data can no longer be assigned to a specific person involved without consulting additional information provided this additional information is stored separately and is subject to corresponding technical and organizational measures;

2. Integrity (Art. 32, Section 1 lit. b of the DS-GVO)

- Transfer control
No unauthorized reading, copying, changes or removal during the electronic transfer or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature;

- Data entry control

Determination whether and the details regarding who has entered, changed or deleted personal data in the data processing systems, e.g. logging, document management;

3. Availability and resilience (Art. 32, Section 1 lit. b of the DS-GVO)

- Availability control

Protection against random or intended destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans;

- Rapid recoverability (Art. 32, Section 1 lit. c of the DS-GVO);

4. Procedure for the regular checking, rating and evaluation (Art. 32, section 1 lit. d of the DS-GVO; Art. 25, section 1 of the DS-GVO)

- Privacy policy management
- Incident response management
- Data protection-friendly presets (Art. 25, Section 2 of the DS-GVO)
- Order control

No order data processing according to Art. 28 of the DS-GVO, without a corresponding instruction from the Customer, e.g.: clear design of the Agreement, formalized order management, strict selection of service providers, preliminary audit obligation, subsequent controls