CONTRACT

DATA PROCESSING AGREEMENT

between

_____
(Corporate name)

_____
(Address)

_____
(Postal Code Town)

_____
(Country)

("**Data Controller**")

and

FINDOLOGIC GmbH
Jakob-Haringer-Str. 5a
5020 Salzburg
Austria

("**Data Processor**")

1. PREAMBLE

The Data Processor shall provide the Data Controller with various search, navigation, personalisation and merchandising services within the scope of a separate contract and/or based on separate individual orders (hereinafter collectively referred to as "Principal Contract") in the context of the website of the Data Controller (hereinafter collectively referred to as "Services"). The Services are described in more detail in the Principal Contract and the respective service specifications.

2. OBJECT

2.1. Processing of personal data

This agreement ("Contract") regulates the processing of personal data, which the Data Processor processes within the scope of the provision of the services for the data controller ("Data") and is to be understood as a supplementation to the main contract between the Data Controller and the Data Processor.

Personal data is any information, which refers to an identified or identifiable natural person. The data in particular comprises the IP address and browser identification of the users of the website of the Data Controller and thus linked behavioural data relating to the provided services such as search enquiries, visited categories, selected filters as well as viewed and purchased products.

The following categories of data subjects are subject to processing:

- Visitors of the Data Controller's website

The processing of the personal data shall be carried out by the entry, storage, processing and erasure.

The personal data (IP address), which becomes known over the course of the data processing, will be processed for settlement purposes for the duration of 6 (six) months, this will be anonymised after this period of time. Insofar as necessary, however, in accordance with statutory storage and documentation obligations, respectively until the ending of a possible lawsuit, etc., the personal data will be processed beyond this time.

2.2. Contents of the order processing

The object, duration, type and purpose of the processing of the data can be derived from the Principal Contract and the respective service specifications.

3. OBLIGATIONS OF THE DATA CONTROLLER

3.1. Instructions

Insofar as the data processing is carried out by the Data Processor within the scope of standard software made available to the Data Controller for online use, the Data Controller shall exercise its right to give instructions (see Subclause 4.1) as a rule by its own use of the online interface of this software. Incidentally, instructions of the Data Controller are either to be issued via the web interface made available to the Data Controller by the Data Processor or in text form; oral instructions are to be confirmed in text form without delay. The Data Controller reserves the right to issue such instructions at all times. If the contents of instructions of the Data Controller exceed that which the Data Processor owes the Data Controller according to the Principal Contract, the Data Controller has to remunerate the Data Processor for the corresponding services separately. If an instruction can only be implemented with a disproportionately large amount of work, the Data Processor shall be entitled to an extraordinary termination of the Principal Contract and this contract.

3.2. Reporting obligation

The Data Controller will inform the Data Processor without delay in the event that an unauthorised third party gains unplanned knowledge of the data of the Data Controller that is processed by the Data Processor according to this agreement, in the area of responsibilities of the Data Controller.

3.3. Liability and damages

The Data Controller and Data Processor shall principally be liable to the data subjects in line with the regulations set forth in Article 82 GDPR. The liability restriction contained in the General Business Terms and Conditions will have their effect in the internal relationship.

4. OBLIGATIONS OF THE DATA PROCESSOR

4.1. Obligation to comply with instructions

The Data Processor shall exclusively process the data within the scope and for the purpose of providing the Services for the Data Controller and according to its documented instructions. The Data Processor shall not process the personal data in any other manner and for no other purposes insofar as it is not obligated in this respect by the law of the EU or the EU member states, which the Data Processor is subject to; in such a case the Data Processor shall inform the Data Controller of these legal

requirements before the processing if the relevant law does not forbid such a notification owing to an important public interest.

4.2. Notification obligation

The Data Processor will point out to the Data Controller without delay if an instruction issued by the Data Controller, in its opinion, breaches applicable regulations regarding data protection. The Data Processor is entitled to suspend the execution of the corresponding instruction until this is confirmed or changed by the Data Controller. The Data Processor has no obligation for the legal examination of instructions.

4.3. Rectification, erasure and blocking

If personal data is to be rectified, erased or blocked, the Data Controller will carry this out itself by using the corresponding functions of the provided software. If this is not possible, the Data Processor will take over the rectification, erasure or blocking according to the instructions of the Data Controller. Subclause 7.2 will apply to the erasure of the data at the end of the contractual term.

4.4. Location of the data processing

Data processing activities are partly also carried out outside of the EU or the EEA, i.e. in the USA. The adequate level of data protection can be derived from

- an appropriateness resolution of the European Commission (EU-US Privacy Shield) pursuant to Article 45 GDPR as well as
- Standard data protection clauses pursuant to Article 46 GDPR

The involved Sub-Data Processors and their countries of origin are listed in Annex 2. The provisions in Paragraph 6 will furthermore apply for Sub-Data Processors.

4.5. Data protection coordinator

The data protection coordinator can be contacted under privacy@findologic.com.

4.6. Data secrecy

The Data Processor will ensure that its employees who are entrusted with the processing of personal data are familiar with the decisive provisions of data protection and obligate them, in writing, to confidentiality and data secrecy. This non-disclosure obligation shall in particular apply to the persons entrusted with the processing of the data, also for the data of legal entities or associations of persons and shall also continue to exist after the termination of their activity for the Data Processor.

4.7. Reporting obligation

In the case of a breach of the protection of personal data in line with Art. 4 Para. 12 GDPR, the Data Processor will inform the Data Controller hereof without delay.

Reports pursuant to Article 33 or 34 GDPR may only be carried out by the Data Processor for the Data Controller after obtaining prior instruction from the Data Controller.

4.8. Obligation to provide support

Insofar as the Data Controller can only fulfil its obligations towards the data subjects (in particular the obligation to provide a data subject information about the processing of their personal data) with the help of the Data Processor, the Data Processor will reasonably support the Data Controller hereby at its request. If a corresponding enquiry for information is directed towards the Data Processor and if this indicates that the applicant has mistakenly considered it to be the Data Controller of the data application the applicant objected to, the Data Processor has to forward the application to the Data Controller without delay and to inform the applicant of this.

The Data Processor will also support the Data Controller, upon request, by showing consideration for the type of processing and the information available to it, with the compliance with its obligations with regard to the security of personal data (security of the processing, report of breaches of the protection of personal data to the supervisory authority, notification of the person affected by a breach of the protection of personal data) as well as a necessary data protection impact assessment and the prior consultation if applicable. The Data Controller has to remunerate the Data Processor separately for the required work.

4.9. Technical and organisational measures

By showing consideration for the status of technology, the implementation costs, the type or the extent, the circumstances and the purposes of the processing as well as the different probabilities of occurrence and severity of the risk for the rights and freedoms of natural persons, the Data Processor will take all necessary technical and organisational measures, which are suitable for guaranteeing a level of protection that is appropriate for the risk. In its area of responsibility, the Data Processor shall in particular take the technical and organisational measures stated in Annex 1 to this contract for the protection of the data. The Data Processor will also take steps in order to ensure that the natural persons subordinate to it have access to personal data and only process these at the instruction of the Data Controller, unless they are obligated to the processing according to the law of the EU or the EU member states.

Owing to the constant further development of the technical and organisational measures the Data Processor is permitted to implement alternative adequate measures, whereby the level of security of the already stipulated measures may not be

fallen short of. Essential changes are to be documented and will be communicated to the Data Controller directly after the change has been carried out.

Pursuant to Art. 32 Para. 1 lit. d GDPR, the Data Processor has, with due reason but at least once a year, to carry out a check, assessment and evaluation of the efficacy of the technical and organisational measures in order to guarantee the security of the processing.

4.10. List of processing activities

The Data Processor has to set up a list of processing activities pursuant to Article 30 GDPR for this contract processing.

5. CONTROL RIGHTS OF THE DATA CONTROLLER

5.1. Controls

The Data Controller is entitled to control the compliance a) with the statutory regulations regarding data protection, b) with the contractual agreements of the parties and c) the instructions of the Data Controller to the necessary extent at the Data Processor or to have these controlled by an auditor commissioned by the Data Controller. The Data Processor will contribute to such controls and make all necessary information available for proof of the compliance. Controls in the permanent establishments of the Data Processor must be announced to the Data Controller at least 2 (two) weeks in advance in writing.

The Data Processor shall permit and enable the Data Controller and auditors commissioned by it to carry out corresponding examinations – including inspections – principally 2 (two) times a year within the scope of the normal business hours and without a substantial impairment to the business operation of the Data Processor and will contribute to this to a useful extent.

5.2. Costs

Costs incurred by controls of the Data Controller will be borne by the Data Controller. This shall also comprise compensation for expenses for the working hours of the personnel used by the Data Processor.

5.3. Interests of the Data Processor that are worthy of protection

Insofar as business and trade secrets of the Data Processor can be disclosed or intellectual property of the Data Processor is jeopardised by controls, the Data Controller has to have the controls carried out at its own costs by a competent and independent third party which has entered into a non-disclosure agreement towards the Data Processor.

6. Sub-Data Processors

6.1 Approved Sub-Data Processors

The Data Processor is authorised to involve the Sub-Data Processors named in Annex 2. The Data Processor has already concluded the necessary contracts with the Sub-Data Processors within the meaning of Art. 28 Para. 4 GDPR, whose level of protection at least corresponds with that of this contract and which impose the same obligations on the Sub-Data Processors, for which the Data Processor is responsible owing to this contract. The Data Controller explicitly agrees hereto.

6.2. Information about intended changes

The Data Processor is moreover authorised to involve further Sub-Data Processors. The Data Processor has to notify the Data Controller of the intended involvement of a further Sub-Data Processor. In this case, the Data Controller can file justified objections in written form within 4 weeks. If it does not do this the consent of the Data Controller shall be deemed as granted.

The Data Processor shall conclude a necessary contract within the meaning of Art. 28 Para. 4 GDPR with the Sub-Data Processor. The Data Processor shall ensure that the Sub-Data Processor enters into the same obligations, for which the Data Processor is responsible based on this contract.

6.3. Sub-Data Processors in third countries

A commission of subcontractors in third countries may only be carried out if the special prerequisites of Article 44 et seqq. GDPR are fulfilled (e.g. appropriateness decision of the Commission, approved rules of conduct).

The provisions in Paragraph 4.4 shall furthermore apply for Sub-Data Processors.

7. TERM

7.1. Term

The term of this contract corresponds with the term of the Principal Contract. The right to termination for good cause shall remain unaffected.

7.2. Data at the end of the contract

Until 6 (six) months after the expiry / the termination of the main contract at the longest – through which this contract will also be deemed as expired / terminated – the Data

Processor will erase the personal data processed within the scope of the provision of its services for the Data Controller at its order from its data carriers and destroy corresponding documents in its company, insofar as the Data Processor is not obligated to further storage by law. The Data Controller is personally responsible for exporting data in time before the expiry of this deadline and to secure it for its further own use. Handing over or exporting data, which is not possible via the standard functions contained within the scope of the services (e.g. download of files), has to be commissioned separately by the Data Controller in time and has to be remunerated.

7.3. Backup copies

The aforementioned erasure obligations shall not apply to data copies, which are contained in regularly created backup copies of comprehensive data stocks of the Data Processor, the isolated erasure of which would mean a substantial amount of work for the Data Processor and which will be erased or replaced automatically within the scope of the backup cycle applied by the Data Processor no later than after 6 (six) months. The recovery and any other use of such copies until their automatic erasure or overwriting is inadmissible after the termination of the contract.

The Data Controller can also request the immediate erasure of such backup copies from the Data Processor if the Data Controller reimburses the Data Processor the costs caused hereby; this shall also comprise compensation for expenses for the working hours of the personnel used by the Data Processor.

8. FINAL PROVISIONS

8.1. Applicable law

Insofar as no other choice of law can be seen from the Principal Contract, Austrian law shall apply exclusively to this contract (without possible referrals to other legal systems and under the exclusion of the UN Convention on Contracts for the International Sale of Goods).

8.2. Place of jurisdiction

Insofar as no other place of jurisdiction can be derived from the Principal Contract, the exclusive place of jurisdiction for disputes from or in connection with this contract is Salzburg, Austria.

8.3. Partial invalidity

Should individual provisions of this contract be or become invalid this shall have no effect on the validity of the other provisions. Instead of the invalid provision, the provision shall apply which the parties would have fairly agreed according to the

originally intended purpose under a commercial approach. The same shall apply in the event of a loophole in the contract.

8.4. Written form

All amendments and addendums to this contract, including possible assurances of the order processor shall require a written form in order to be valid, which may also be carried out in an electronic format; this shall also apply in the event of a deviation from this form requirement.

For the **Data Controller**:

_____
Name (in block capitals)

_____
Position / Function

_____
Place, date

_____
Signature

For the **Data Processor**:

Matthias Heimbeck
_____
Name (in block capitals)

CEO
_____
Position / Function

Salzburg, 16 September 2020
_____
Place, date

_____
Signature

ANNEX 1: TECHNICAL AND ORGANISATIONAL MEASURES

1. ADMISSION CONTROL

Measures in order to refuse unauthorised persons access to data processing systems, with which personal data is processed or used:

The processing of personal data on the premises of the Data Processor will only take place in exceptional cases such as maintenance or inspections. During this time the data processing systems are in constant use. Extended measures for admission control are therefore not envisaged.

Further data processing systems, with which personal data is processed or used, will be exclusively operated by the Sub-Data Processors named in Annex 2. The responsibility to implement adequate admission controls lies with the respective Sub-Data Processor.

2. ENTRY CONTROL

Measures in order to prevent those data processing systems being used by unauthorised persons (including encryption processes):

- Access protection (authentication):
  - There is access protection to all data processing systems by user authentication.
  - The passwords must comply with the guidelines in the 9th edition of the IT Security Manual of the Austrian Federal Economic Chamber.
- Secured transmission of authentication secrets (credentials) in the network:
  - The transmission of the authentication secrets via the network is encrypted.
- Stipulation of authorised persons:
  - There is a role concept – insofar as supported by the respective data processing system – (pre-defined user profiles).
  - Entry authorisations will – insofar as supported by the respective data processing system – be allocated individually (person-based).
  - The group of authorised persons is to be reduced to the necessary minimum for the operation.
- Administration and documentation of personal entry authorisation:
  - A process for the application for, approval of, allocation and withdrawal of entry authorisations is set up, described and applied.
  - A responsible person has been appointed for the allocation of entry authorisations.
  - There are regulations on representation.

- Manual entry block:
    - There is a policy to protect work stations and terminals against unauthorised use in case of temporary absence from the workplace, e.g. by automatic or manual update of the password-protected screensaver.

The users are instructed about these stipulations.

3. ACCESS CONTROL

Measures in order to guarantee that the persons authorised to use a data processing system can exclusively access the data subject to their access authorisation and that personal data cannot be read, copied, changed or removed without authorisation during the processing, use and after the storage (including encryption processes):

- Authorisation concept / implementation of access restrictions:
    - There are regulations regarding the creation, alteration and erasure of authorisation profiles.
    - Each person with access authorisation can only access the data which he concretely requires for the processing according to the order of the respective current transaction and which has been set up in the individual authorisation profile.
- Administration and documentation of personal access authorisations:
    - A process for the application for, approval, allocation and withdrawal of access authorisations has been implemented.
    - Authorisations are – insofar as supported by the respective data processing system – linked to a personal user ID and to an account.
    - If the basis for an authorisation ceases to exist (e.g. by a change in function), this will be withdrawn promptly.
- Recording of the data access:
    - All reading, input, change and erasure transactions will – insofar as supported by the data processing system – be recorded.
    - Evaluations will be carried out at random if required in order to identify misuse.

4. TRANSFER CONTROL

Measures in order to guarantee that personal data cannot be read, copied, changed or removed by unauthorised persons during the electronic transmission or during their transport or their storage on data carriers and that it can be checked and determined to which bodies a transmission of personal data is envisaged by equipment for the data transmission (including encryption processes):

- Secure data transmission between the server and client:
    - The data transmission between clients and servers shall be encrypted (SSL, SSH, SFTP or VPN).

- Transmission in the backend:
  - The connection to the backend systems is protected.
  - Data with a high need for protection will be encrypted.
- Human-machine authentication:
  - Reciprocal authentication by means of cryptographic process.
- Process for the collection and disposal:
  - There are regulations for the destruction of data carriers conforming to data protection.
  - There are regulations for the destruction of documents conforming to data protection.
- Erasure/ destruction processes conforming to data protection:
  - Data carriers are erased in a manner that fulfils data protection standards before they are re-used by other users; recovery of the erased data is not possible at all or only with a disproportionate amount of work.
  - Hardware components or documents are destroyed so that recovery is not possible at all or only with a disproportionate amount of work.

5. INPUT CONTROL

Measures in order to guarantee that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed in data processing systems (input control):

- There is documentation regarding which persons are authorised and responsible, owing to their tasks, for entering, changing and removing personal data in the data processing system.

6. ORDER CONTROL

Measures in order to guarantee that personal data, which is processed by order, can only be processed in line with the instructions of the Data Controller (order control):

- Exercising control obligations:
  - The Data Processor supports the Data Controller with the exercising of its control obligations.
  - Any incidents that occur will be reported to the Data Controller.
  - The Data Processor has informed all employees about the reporting obligation regarding incidents.

7. AVAILABILITY CONTROL

Measures in order to guarantee that personal data is protected against accidental destruction or loss (availability control):

- Backup concept:

    - There is a backup concept.
    - Backups take place regularly.
    - A person responsible for the backup and representatives have been appointed.
    - It is checked regularly whether it is possible to recover a backup.
- Examination of the infrastructure:
    - A permanent monitoring of the operating parameters takes place.

8. ORGANISATION CONTROL

- Process definition /control:
    - Process instructions are available.
    - Processes and work flows have been defined for the processing of data in the company.
    - The implementation and compliance with the processes is controlled.
- Training / obligation:
    - Principles of data protection, including technical-organisational measures.
    - Non-disclosure obligation regarding business and trade secrets including the processes of the Data Controller (Section 11 UWG).
    - Proper and careful handling of data, files, data carriers and other documents.
    - The training is documented.
    - The training courses are repeated regularly but at least every three years.
- Training / obligation of persons not belonging to the company:
    - Persons not belonging to the company only receive access to data processing systems when they have been obligated, in writing, to data secrecy and, if applicable, also the telecommunications secrecy or further non-disclosure obligations and have been trained before they may put into operation and operate the data processing systems.
- Internal allocation of tasks:
    - Segregation between operative and administrative functions has been carried out.
- Representative regulation:
    - A representative regulation has been stipulated for all tasks/functions that are necessary for the operation.

ANNEX 2: Sub-Data Processor

Sub-Data Processor	Services provided by the Sub-Data Processor	Guarantee of the level of data protection
CDN77 / DataCamp Limited 207 Regent Street London UK	Hosting of Web Assets	ADV
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Germany	Hosting of the infrastructure	ADV
OVH 2 Rue Kellermann 59100 Roubaix France	Hosting of Web Assets	ADV
Sentry 132 Hawthorne St San Francisco CA 94107 USA	Real-Time Error Tracking	EU-US-Privacy Shield Standard contractual clauses
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Hosting of the infrastructure in the Google Cloud Platform (GCP)	EU-US-Privacy Shield Standard contractual clauses