# Terms & Conditions

*Last modified: October 2020*

The retraced Terms and Conditions form the legal agreement between you, either an individual or legal entity (“You” or “Your”), and retraced GmbH (“retraced”) for use of the retraced platform (“retraced” or “platform” or “we” or “our”). These Terms and Conditions serve to govern your use of the retraced platform, including any updates and accompanying written documentation. The platform is aimed at entrepreneurs.

These Terms and Conditions are subject to change at any time due to technical and legal adaptations. Use of this site forms your consent and legally binding agreement to adhere to these terms. Retraced may occasionally contact you via email.

**What is retraced?**

Retraced is a software solution that enables fashion companies to move towards a more sustainable, resilient and compliant supply chain. With retraced, brands can map their supply chains, collect supply chain data, trace productions and monitor and engage with their suppliers. Besides that, it gives the end-consumer the possibility to trace the individual supply chain of his purchased product. In addition to transparency and fairness on the market, this should in particular strengthen the end consumer's confidence in the brands.

Within the framework of the transparency solution offered by retraced, the data and documents relevant to the characteristics of sustainability and fairness are collected and evaluated from the supply chains of the respective company. At the brand’s option, the collected and evaluated supply chain data can be accessed via app and/or via a widget in the online shop on the brand’s website.

You must be at least 18 years old to use retraced. The acceptance of terms constitutes your confirmation of the same.

**Performance of retraced**

Retraced provides the services to ensure the operational usability of the transparency solution. The scope of our performance depends on your individual requirements and usage of the retraced platform. Therefore, we will determine the scope of our performance individually with you, adapted to your needs.

**Accounts, Passwords and Security**

You must be a registered user to access the platform. Users must register using their email address. You are responsible for keeping your password private and secure and are prohibited from sharing your login and password with others. All activity occurring under your email address is your sole responsibility.

If you recognize that your account is used by unauthorized third parties, you are obliged to immediately report the misuse to retraced. We will then block your account and provide you with new login data.

**Duration and Termination of your account**

These Terms and Conditions run for an indefinite period and apply with you agreeing to them, by loging into the platform for the first time. You are entitled to use the retraced platform according to these Terms and Conditions. Any major break of these Terms and Conditions, will result in your account being terminated.

Each party is entitled to terminate the contract by informing the other party anytime with a one months notice period starting from the end of the month.

The right of both parties to terminate the terms without notice for good cause remains unaffected.

Any termination must be in writing (an email to contact@retraced.co is sufficient).

## Duty to cooperate

The implementation and maintenance of the transparency solution requires cooperation between you, retraced and all participants in the supply chain.

The scope of your duties depends on your individual requirements and usage of the retraced platform. Therefore, we will determine the scope of duties individually with you, adapted to your needs.

## Changes of Products and Terms

retraced reserves the right to amend these terms of use from time to time, especially if this is necessary for technical or legal reasons. In this case retraced will inform you about the change at least four weeks before the actual change of these terms of use.

If you don’t agree with the upcoming change of terms of use, you have the right, to withdraw the change of terms and to terminate the agreement within four weeks after the received information of the planned change of terms of use.

This clause does not affect the billing, agreed between you and retraced.

## Billing

retraced will charge you at the end of each month. The charged amount is based on the usage of the retraced system. If not otherwise agreed with us, there are no fixed expenses, connected to owning and opening up an account.

The first month of usage is always for free. Afterwards, we will negotiate with you the amount of fee, adapted to your individual requirements. The monthly fee depends on your platform requirements. Please contact us in order to discuss your requirements and the respective platform fees.

As payment methods, we accept: bank transfer, Visa or MasterCard. All Credit Card payments are being processed by Stripe Payments Europe Limited.

The fee is due within fifteen days after receipt of the invoice. If any fee is not paid in a timely manner, or retraced is unable to process your transaction using the information provided, retraced reserves the right to deny access to your retraced account until the amount is balanced.

## Intellectual Property Rights

Subject to the Terms and Conditions of this Agreement, retraced grants you a non-exclusive, non-transferable, limited and revocable license to use the Product. The Product and their structure, organization, source code, and documentation belong solely to retraced and its licensors. Accordingly, you agree to not allow third parties to sublicense, transfer, or distribute any part of the retraced service to any third party. You are not allowed to modify, adapt or translate any part of this service, or in any way act to derive source code from the Product.

## Responsibility for Contents

You are solely responsible for the content and data which you upload to the platform and make available to the consumers via the retraced Consumer App or the retraced Shop Plug-in. You assure that you are the owner of the rights to all content and data, including images, which you make available to the public via the retraced Consumer App or the retraced Shop Plug-in.

Retraced does not examine these contents and therefore has no influence on the selection and content of the uploaded data and information.

## Indemnity

In the event that claims by third parties are asserted against retraced, due to an infringement of intellectual property rights caused by you, you are obliged to reimburse retraced for the reasonable costs of a defense against the alleged infringement of intellectual property rights.

## Limitation of Liability

The liability of both parties is unlimited in the case of intent, gross negligence and injury to life, body or health as well as in the case of intentional or negligent violation of essential contractual obligations (cardinal obligations) of the parties, their legal representatives or accomplices.

Essential to the Terms are such obligations whose fulfilment enables the proper execution of the Terms. Additionally, both parties are liable without limitation under the Product Liability Act.

Apart from the unlimited liability mentioned in paragraph 1, the liability of retraced is limited to the typical damage foreseeable in connection with the Terms. In this case, however, the liability is limited to the amount of the annual remuneration, which the parties have agreed upon. Any further liability of retraced is excluded.

The liability of retraced is also excluded if you change the software products or the retraced environment and you cannot prove that these changes did not cause the damage.

## Confidential Information

The parties commit to treat all confidential information, which they become aware of during the contract, strictly confidential and to use such information only for the contractually agreed purposes. The parties shall not disclose any confidential information, whether in writing, orally or in any other form, to third parties.

"Confidential Information" shall mean all information, documents, details and data that are marked as confidential or which, by their nature, are considered confidential. Each party commits to make every effort to protect such Confidential Information from disclosure to third parties. Companies affiliated with a party (§§ 15 ff. AktG) are not considered third parties within the meaning of this contract. Disclosure of the Confidential Information shall be limited to employees of the parties who are directly involved in the activities covered by this contract, who need to know such Confidential Information and who are bound by the provisions of this paragraph.

The parties commit to use all information exclusively for the fulfilment of their obligations under this contract. This shall not include:

(a) Information which is or becomes generally known without either party breaching its confidentiality obligation,

(b) Information which is disclosed by third parties without breach of confidentiality obligations towards a party,

(c) Information already known to a party at the time of conclusion of the contract, or

(d) Information required to be disclosed by law or court order. If one party suffers damage as a result of the other party deliberately or negligently disclosing confidential information in breach of its duty of confidentiality, it may demand compensation for the same within the scope of these Terms.

The rights and obligations arising from this paragraph shall remain unaffected by the termination of the contract and shall continue to apply for a period of 2 [two] years after the termination of this contract.

**Data protection**

When you use retraced, you agree that retraced may duplicate and store your data, information, files and folders in accordance with retraced policies and these Terms.

The transparency solution offered by retraced is blockchain powered. The encryption means that only anonymized data is stored on it. The parties are aware, that data once stored in the blockchain, can always be viewed and cannot be permanently deleted. Retraced can only perform an update of the data in order to delete them. After an update of the data, the previous data can still be viewed in the history of the blockchain. By making the data anonymous, the data cannot be used by third parties without further information and in particular cannot be assigned to your account.

Each element stored in the system of retraced is randomly assigned an unique ID. The stored element can be a created product, created supply chain or created manufacturer. Therefore,no conclusions about the origin of the data can be drawn solely based on the blockchain and the ID. This ID cannot be used to draw any conclusions about the origin of the data based solely on the blockchain.

At your request, your own data can be deleted from the retraced system. Optionally, a company or single employee or product data sets can be deleted. If a company shall be deleted as a whole, the company and all employees and products are deleted from the retraced system, except for the respective employee or product IDs. If only one employee or product shall be deleted, the employee or product is deleted from the retraced system except for its ID.

You allow all products tracked by retraced to be displayed in the retraced Map. In the retraced Map, products are shown randomly, if a user enters the website without scanning a product before.

**Data Protection Clause**

The Compliance with the legal requirements for data protection is subject of a separate agreement between the parties (AVV) in Appendix 1 at the bottom of these Terms.

## Closure of Terms

At your request, the data collected until the termination of the Terms as well as the account on the retraced platform, remain preserved for 24 months after termination of the Terms. In this case of a request, the data will also be displayed in the retraced frontends for 24 months after the end of the Terms.

## References

Both parties are entitled to refer to the cooperation with the other party and in particular to mention the other party as a reference, including on their website and in advertising. As part of that, each party is also entitled to use the trademark of the other party for the purpose of reference.

## Final Provisions

These Terms, including the annexes as part of the Terms, contain the complete agreement between the parties. No oral agreements have been made.

Amendments or additions to the Terms must be made in writing and signed by both parties. This shall also apply to any amendments to the written form requirement contained in this clause. E-mails do not fulfil this written form requirement.

You are not entitled to assign rights from these Terms.

These Terms and all disputes arising out of or in connection with it, including its creation, shall be governed exclusively by the law of the Federal Republic of Germany, excluding the UN Convention on Contracts for the International Sale of Goods of 11 April 1980 [CISG].

If no exclusive place of jurisdiction applies, the parties shall determine Düsseldorf as place of jurisdiction.

Should one of the above provisions be or become invalid, the validity of the remaining provisions of these Terms shall remain unaffected. In such case, the parties shall replace the invalid provision by a provision which comes as close as possible to the legal and economic purpose of the provision to be replaced. The same applies to regulatory gaps.

# Appendix 1: Contract for data processing

## Preamble

The principal wishes to commission the agent with the services mentioned in Terms and Conditions. Part of the execution of the contract is the processing of personal data. In particular Article 28 GDPR places certain requirements on such data processing. In order to comply with these requirements, the parties conclude the following agreement, the performance is not remunerated separately, unless this has been expressly agreed.

## Definitions

(1) According to Article 4 (7) GDPR, the **responsible person** is the body which alone or jointly with other responsible persons decides on the purposes and means of processing personal data.

(2) According to Article 4 (8) GDPR, a **processor** is a natural or legal person, authority, institution or other body which processes personal data on behalf of the responsible person.

(3) Pursuant to Article 4 (1) GDPR, **personal data** is any information relating to an identified or identifiable natural person (hereinafter "data subject"); a natural person is deemed identifiable if he or she 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 special characteristics which are an expression of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

(4) **Particularly sensitive personal data** are personal data in accordance with Article 9 GDPR, from which the racial or ethnic origin, political opinions, religious or ideological

beliefs or trade union membership of those concerned can be deduced, personal data in accordance with Article 10 GDPR on criminal convictions and offences or related security measures as well as genetic data in accordance with Article 4 (13) GDPR, biometric data in accordance with Article 4 (14) GDPR, health data in accordance with Article 4 (15) GDPR and data concerning the sexual life or sexual orientation of a natural person.

(5) According to Article 4 (2) GDPR, **processing** is defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, arrangement, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) Pursuant to Article 4 (21) GDPR, a **supervisory authority** is an independent state body established by a Member State pursuant to Article 51 GDPR.

**Indication of the competent data protection supervisory authority**

(1) The competent supervisory authority for the principal is the State Commissioner for Data Protection of the Federal State of the principal.

(2) The competent supervisory authority for the agent is the State Commissioner for Data Protection and Freedom of Information, North Rhine-Westphalia.

(3) The principal and the agent and, where appropriate, their representatives shall cooperate with the supervisory authority in the performance of their duties upon request.

## Subject of the contract

(1) The agent shall provide services to the principal in the field of collecting and evaluating data from the principal's value chain based on the above-mentioned Terms and Conditions. In doing so, the Agent shall be granted access to personal data and process them exclusively on behalf of and according to the instructions of the principal. The scope and purpose of the data processing by the Agent are set out in the above-mentioned Terms and Conditions (and the appendices thereto). The principal shall be responsible for assessing 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 Terms and Conditions.

(3) The provisions of this agreement shall apply to all activities in connection with the above-mentioned Terms and Conditions, in which the agent and its employees or agents commissioned by the agent come into contact with personal data originating from or collected for the principal.

(4) The term of this agreement shall be based on the above-mentioned Terms and Conditions of retraced, unless the following provisions impose additional obligations or rights of termination.

## Right to issue instructions

1. The agent may collect, process or use data only within the framework of the above-mentioned Terms and Conditions and in accordance with the instructions of the principal; this applies in particular to the transfer of personal data to a third country or to an international organization. If the agent is obliged to carry out further processing based on the law of the European Union or of the Member States, the agent shall notify the principal of these legal requirements before processing.

(2) The instructions of the principal are initially laid down in this contract and may subsequently be amended, supplemented or replaced by individual instructions in writing or in text form (individual instructions). The principal is entitled to issue corresponding instructions at any time. This includes instructions regarding the correction, deletion and blocking of data.

(3) All instructions issued must be documented by both the principal and the agent. Instructions that go beyond the performance agreed in the above-mentioned Terms and Conditions will be considered as request for a change in performance.

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

### Nature of the data processed, circle of persons affected

(1) In the context of the implementation of the above-mentioned terms and conditions, the agent shall be granted access to the personal data specified in Annex 1. These data shall include the special categories of personal data listed and identified as such in Annex 1.

(2) The group of persons affected by the data processing is shown in Annex 1.

### Protective measures of the agent

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

(2) Within his area of responsibility, the agent shall design the internal organization 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 principal's data in accordance with Article 32 GDPR, in particular at least the measures of

a) entry control

b) access control

c) surveillance

d) Passing on control

e) input control

f) Order control

g) Availability control

h) Separation control

The agent reserves the right to change the security measures taken, while ensuring that the level of protection does not fall below the contractually agreed level.

(3) The persons employed in data processing by the agent shall not be permitted to collect, process or use personal data without authorization. The agent shall impose a corresponding obligation on all persons entrusted by it with the processing and fulfilment of this contract (hereinafter referred to as employees) (obligation of confidentiality, Article 28 (3) lit. b GDPR) and shall ensure compliance with this obligation with due care. These obligations must be formulated in such a way that they continue to apply after the termination of this contract or the employment relationship between the employee and the agent.

(4) At the agent, the contact person for data protection can be reached at the following e-mail address: datenschutz@retraced.co.

## Disclosure duty of the agent

(1) In the event of disruptions, suspicion of data protection violations or breaches of contractual obligations on the part of the agent, suspicion of security-related incidents or other irregularities in the processing of personal data by the agent, persons employed by the agent within the scope of the contract or by third parties, the agent shall inform the principal without delay in writing or text form. The same applies to audits of the agent 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, including, 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 agent to remedy the breach and, where appropriate, measures to mitigate its possible adverse effects.

(2) The agent and, where appropriate, his representative shall keep a register of all categories of processing operations carried out on behalf of the principal, containing all the information referred to in Article 30 (2) GDPR. The list shall be made available to the principal on request.

## Rights of control of the principal

(1) Before starting data processing and then at regular intervals at its own discretion, the principal shall satisfy itself of the technical and organizational measures of the agent. For this purpose, he may, for example, obtain information from the agent, have existing attestations from experts, certifications or internal tests presented to him or, after timely coordination during normal business hours, personally check the technical and organizational measures of the agent himself or have them checked by a competent third party, provided that the latter is not in a competitive relationship with the agent.

The principal shall only carry out inspections to the extent necessary and shall not disproportionately disturb the agent's operating procedures.

(2) The agent undertakes to provide the principal at the latter's oral or written request within a reasonable time with all information and evidence required to carry out a check of the agent's technical and organizational measures.

**Requests and rights of data subjects**

(1) The agent shall support the principal as far as possible with suitable technical and organizational measures in the fulfilment of the principal's obligations under Article 12-22 and 32-36 GDPR.

(2) If a data subject asserts rights, such as the right to information, correction or deletion with regard to his data, directly against the agent, the agent does not react independently, but refers the data subject immediately to the principal and awaits his instructions.

**Liability**

(1) In the internal relationship with the agent, the principal alone shall be responsible to the person concerned for compensation for damages suffered by a person concerned as a result of data processing or use within the scope of order processing that is inadmissible or incorrect according to the data protection laws.

(2) The parties shall each release themselves from liability if one party proves that he is not to any extent responsible in any way for the circumstance as a result of which the damage has occurred to a person affected.

## Extraordinary right of termination

The principal may terminate the agreement in whole or in part without notice, if the agent does not fulfil his obligations under this agreement, if he intentionally or grossly negligently breaches the provisions of the GDPR or if he cannot or does not wish to carry out an instruction from the principal. In the case of simple - i.e. neither intentional nor grossly negligent - infringements, the principal shall set the agent a reasonable time within the agent can remedy the infringement.

## Termination of the agreement

(1) The agent shall return to the principal after termination of the l agreement or at any time at the principal's request all documents, data and data carriers made available to him or - at the principal'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 agent. The agent shall keep documented proof of the proper deletion of any remaining data.

(2) The agent is obliged to treat confidentially all data that has become known to him in connection with the agreement even after the end of the agreement. The present agreement shall remain valid beyond the end of the cooperation as long as the agent has personal data at his disposal which have been forwarded to him by the principal or which he has collected for the principal.

## Final provisions

(1) 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.

(2) Should any 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 thereby.

(3) This agreement is subject to German law. Exclusive place of jurisdiction is Düsseldorf.

**Annex 1 of AVV**

| Kind of data | Purpose of the data processing | Affected |
|---|---|---|
| Employee data and user data<br>- First name<br>- Last name<br>- E-mail address<br>- Company | - Administration of access (login, authorizations etc.) | - principal's employees<br>- value chain participants<br>- employees of subcontractors of the principal |
| Data that participants in the value chain can record while using the retraced Business App:<br>- Employee / user data<br>- Signatures<br>- Text input<br>- Photos<br>- Photo descriptions<br>- Numbers, e.g. temperatures, kilos, currency, etc.<br>- Geo data including place and time<br>- Product type<br>- Material specifications for the individual product | Use of the retraced Business App to enter the data of the value chain for the purpose of product tracking and transparency | - principal's employees<br>- value chain participants<br>- employees of subcontractors of the principal |
| Master data of you<br>- Company name / branches<br>- Address<br>- E-mail address<br>- Contact person with name<br>- Phone number | Correspondence with the principal | - Contact person<br>- value chain participants<br>- Authorizing person of the principal |

## Annex 2 of AVV

## Technical and organizational measures of the contractor

### Entry control

The data is stored and processed in a professionally operated computer center. Access control is only permitted to authorized persons of the data center operator.

### Access control

The following measures deny unauthorized persons access to data processing systems with which personal data are processed or used:

User names & passwords, virus protection, firewalls, monitoring, regular security updates of the systems

### Surveillance control

The system has an access rights and access role functionality with which the access to the data of users can be individually adjusted on the side of the contractor as well as on the side of you.

### Passing on control

The server data transfer of the retraced system is exclusively carried out via a 256-bit encrypted SSL connection.

A direct transfer to third parties is only possible by authorized users of you and authorized employees of the contractor.

Support is exclusively provided by employees of retraced.

### Input control

System-side log files for user activities and administrators are recorded.

### Job control

The data collected by you via the Web App or the Mobile Apps is encrypted and transferred to the servers of retraced.

Only your authorized users as well as administrators and authorized support staff of the contractor have access to this data afterwards.

The contractor has concluded corresponding data protection contracts with the computer centers or corresponding order processing agreements in the form of certificates are available.

**Availability control**

The data is primarily stored at the server location in Germany. The processing takes place on Oracle servers in Germany.

They are mirrored several times a day at the server location in Germany.

The server locations are professional data centers which are equipped with fire protection, burglary protection, power backup UPS, gas extinguishing systems and other measures in the area of business IT.

The contractor has an emergency management in place.

**Disconnection control**

The retraced system is multi-client capable.

Your data or project can be extracted on request.