e TRUSTED

Conditions of Use GDPR Protection

These conditions, together with the individual user agreement, entered into via the Online order form, regulate the provision of the Trusted Shops **GDPR Manager** and the use of the list of processing activities that has been compiled for that purpose, the provision of the **Trusted Shops legal-text generator** and the use of the privacy statement drawn up for that purpose, the update service, the assumption of liability by Trusted Shops GmbH (hereinafter referred to as "**Trusted Shops**") and the user's obligations regarding the systems, texts and information provided. This offer is aimed exclusively at entrepreneurs within the meaning of § 14 of the German Civil Code (BGB). At the same time, the Parties will sign an **agreement on the processing of personal data by a processor**, which is attached as an appendix to the user agreement.

Definitions

"**GDPR Manager**": The online system provided by Trusted Shops for the purpose of creating (1) a list of processing activities in conformity with the GDPR requirements.

"**Legal-Text Generator**": The online system provided by Trusted Shops for the purpose of creating legal texts.

"**Sessions**": The total number of sessions on all domains within a month, as recorded by Analytics. A single session is the whole duration of a user's active of the website or the application. If a user remains inactive for more than 30 minutes, any subsequent activity is usually considered a new session. If a user quits the website and returns within 30 minutes, the original session will be resumed instead of a new one.

A. Services of the GDPR Protection Package

1. The exact services provided by the various GDPR protection packages are determined by the performance specification.

B. Online System

1. Throughout the term of the agreement, Trusted Shops will provide the user with an online system in order to use the GDPR Manager and the Trusted Shops Legal-Text Generator (also referred to jointly as "application program(s)") in German and exclusively earmarked for the user's own operational business under the conditions of this agreement. The user shall not receive any additional rights, particularly those concerning the software or any infrastructure services provided in the computer centre in question. Any further use requires the prior written consent of Trusted Shops.

2. Trusted Shops is not obligated to physically deliver the application program or to physically provide the services thereof. The customer is aware that access to and use of the Trusted Shops application program is exclusively internet-based.

3. The user acknowledges that it is not purchasing any licence or right to the application programs itself and that these programs may only be used to provide the services.

4. The creation of texts and lists using the application program is based on information provided by the supplier/ service provider (e.g. hosters, tracking tools and social plugins, payment service providers) and is based on legal conditions and mandatory requirements. Trusted Shops shall assume that the information provided by the supplier/ service provider is correct and accepts no liability for misinformation supplied by said third-party providers.

C. Partner Law Firm / Services of the Partner Law Firm

1. The user simultaneously concludes a legal consultation contract with FÖHLISCH Rechtsanwälte (hereinafter "the partner law firm") which includes the Membership Terms.

2. The legal tech products Legal text Generator and Record of Processing Activities Generator (a.k.a. GDPR-Manager) are services provided by the partner law firm in the context of the legal consultation contract, whereas Trusted Shops provides the infrastructure necessary for their performance.

D. Use of Trusted Shops Trademarks

1. With regard to trademarks, the online system and all other services and licensed content delivered, Trusted Shops holds all intellectual property rights (particularly copyrights, trademark rights, patent rights, design rights, rights to or related to confidential information.

2. The user is prohibited from using the Trusted Shops word/ figurative marks (logo) or from giving the impression that its online presence has been tested by Trusted Shops, unless it is entitled to do so because of a user licence granted by Trusted Shops.

E. User Templates

1. The GDPR Manager gives the user the option of using both existing standard templates and of creating his/her own, new templates.

2. Trusted Shops is entitled to use such user templates as the basis for new standard templates and to permanently integrate the same into the GDPR Manager.

F. Use of Generated Content

1. The list and texts generated are subject to copyright protection. Any use thereof without a licence having been previously issued is excluded.

2. Trusted Shops grants the user the non-exclusive, non-transferrable right, limited to the term of the agreement, to use the list created exclusively for its own personal use and only for the company indicated at the time of registration; texts created may also be used exclusively by the online presence indicated at the time of registration. The linked copyright notice may not be removed.

3. Use for other companies/ other online presences, use other than the intended use or any disclosure of the list to third parties, unless this takes place within the context of the intended use, is prohibited.

4. The right of use pursuant to point 2 does not apply if and so long as the conditions of use and user rights according to sections F to H are not met.

G. Use of the Consent Manager

1. The use of the Consent Manager is subject to certain limitations. Trusted Shops reserves its right to limit the use of the service or to authorise it under new conditions for use of the tool on a larger scale in case it records a use of more than 30,000 sessions per month.

2. The service is provided by a Trusted Shops partner. By starting use of the service, the user accepts the partner's terms of use and concludes a sub processing agreement with them.

H. Obligations relating to the Online System/ Application Program

1. The user is obligated to treat their username and password in the strictest confidence, not to pass on their login information to other individuals and is not entitled

    a. to allow interfaces not provided by Trusted Shops (e.g. scripts, robots or web crawlers) access to the Trusted Shops online systems;

    b. to leverage or bypass technical measures in order to gain unauthorised access to the Trusted Shops systems or to allow third parties access to the same;

    c. to download or decompile the Trusted Shops application program or to analyse it as part of reverse engineering.

2. The user is obligated to correctly answer the questions posed in the application programs and bears the responsibility for answering correctly. All questions and advice must be read and complied with carefully. If the user has the option of entering information in free text fields, then only those entries permitted therein are allowed and only those which do not contradict the questions asked and the advice present on the system. The user bears sole responsibility for entries made in free text fields. Manual changes made to the generated list are not permitted. Supplements or deletions represent a subset of changes.

3. The user is obligated to carefully read the protocols created after running the application program and to check these for plausibility.

4. The user is obliged to immediately update the list and texts created if there is a change to or if there are relevant changes to its company and/or online presence which concern the facts being queried.

I. Additional Obligations relating to Use of the GDPR Manager

Trusted Shops continuously updates the GDPR Manager templates where required. The online version of the templates provided is always valid. In the case of an export taking place prior to use of the exported document, the user is obligated to check that said document is up to date.

J. Additional Obligations relating to the Use of the Legal-Text Generator

1. The user must ensure that the following usage requirements are met for its online presence for as long as the Legal-Text Generator is used:

    a. Providing that the online presence is an online shop the user is running independently or in a marketplace, goods may only be offered to customers who have their usual place of residence in the target markets specified in the respective service description or in the online system. The sale of medicine or the offer of services requiring a prescription is strictly prohibited.

    b. Providing that the user chooses the option "website" in the generator, the target website must not allow visitors to submit or express any form of legally binding declarations (of intent), e.g. paid orders of goods or services, paid reservations and subscriptions, and the like.

    c. Regardless of the type of online presence (online shop or website), the contract must not be concluded outside the online presence (e.g. via phone, fax, or email).

    d. That no cease-and-desist declarations have been made which the member would breach were it to use the created texts.

    e. Processing of personal data that is not specified in the generated privacy policy or lacks legal basis must not take place.

    f. Processing of special categories of personal data in the sense of art. 9 para. 1 GDPR must not take place.

    g. The user is obligated to adhere to the applicable law and comply with the Trusted Shops Exclusion catalogue (TS-ASK).

2. The user is responsible for the correct use of the texts in its online presence. It must particularly ensure that no contradictions arise between the created and other pages used on its online presence (e.g. "FAQ", "Customer Information"). The user accepts no liability for entries made by the member in free text fields, Changes to the created texts are not permitted. Supplements or deletions represent a subset of changes.

3. Trusted Shops shall advise the customer via e-mail of any changes to the legal situation that are relevant to the created texts and provide the user with instructions with which the user must immediately comply. The user is obligated to ensure that these messages are received, in particular by regularly checking its spam folder. When absent, the user must ensure that changes and notifications relating thereto can be received and implemented.

K. Confidentiality

1. In this user agreement, "confidential information" means all information disclosed between the contracting parties with the aim of processing the user agreement, whether in writing, verbally or otherwise (e.g. technically or via a visual display) which is marked as confidential or which, under the circumstances in question, is necessarily confidential.

2. Trusted Shops undertakes to keep secret the confidential information, particularly undertaking not to disclose it or parts thereof to third parties, treating it with the same confidentiality as it would its own business secrets. Confidential information may only be disclosed to third parties after the express written approval of the affected party.

3. Notwithstanding the provision in no. 2 above, Trusted Shops is entitled to disclose the confidential information to those of its own bodies and employees as well as to those of its tax advisors, statutory auditors and lawyers who require it in order to process the user agreement, provided that the aforementioned individuals are contractually and/or professionally sworn to secrecy.

4. Trusted Shops undertakes to take the precautions necessary to ensure that persons other than those referred to in no. 3 above have no knowledge of the confidential information. Trusted Shops shall make those persons involved with the confidential information aware of this agreement and make them expressly aware of their duty of confidentiality.

5. Copies, duplicates and recordings made on electronic or other media or other reproductions of confidential infor-

mation may only be made with the prior written consent of the affected party, unless such are required to process the user agreement.

6. Trusted Shops undertakes, at the first request to do so, to publish all confidential information disclosed on a physical medium as well as all reproductions of such information found on a physical medium. If the confidential information is transmitted or reproduced in another manner, then Trusted Shops undertakes to delete it or to ensure that it is deleted. The following are exceptions to the obligations undertaken in the two previous sentences: Secured archiving of copies kept in order to comply with mandatory legal requirements, judicial or official orders for the time periods set out therein and those copies that are contained in encrypted automatic backups.

7. Trusted Shops undertakes to use the confidential information for the exclusive purpose of processing the user agreement and, in particular, not to use it for competition purposes.

8. The obligations stemming from this confidentiality agreement do not apply to information that must be disclosed to third parties due to mandatory legal, judicial or official orders.

L. Data Protection and Data Security

1. If Trusted Shops processes personal data of the user or which falls within such scope, it must only do so for the purpose of executing the agreement. Its data processing activities are regulated by Appendix 1. This agreement forms an integral component of the user agreement.

2. It is agreed that the user, both in the general contractual relationship and within the meaning of data protection law shall remain the "owner of the data". Trusted Shops, as well as all those participants involved on its side in the execution of the contract, shall have no control over the legal admissibility of the data saved on the user's behalf unless otherwise agreed in this contract.

M. Maturity of User Fees

1. For the first year, the user fee is payable when the contract is entered into, subsequently being payable at the beginning of a contract year in advance.

2. The parties may agree to an instalment contract. Trusted Shops is entitled to terminate the instalment contract if the user is at least 30 days in arrears with payment of an instalment.

3. In the event of such termination, the outstanding user fee for the contract year in question shall be payable immediately.

4. So long as the user, despite a dunning notice, remains 30 days in arrears with the payment of amounts due, Trusted Shops is entitled not to render the agreed services for the duration of the default period.

5. A user based in another EU Member State shall confirm the accuracy of the VAT ID no. provided and shall authorise Trusted Shops to settle bills according to the reverse charge procedure.

6. The user agrees to the transmission of all bills via e-mail. It may withdraw its consent at any time.

N. Availability of the Online Systems

1. Trusted Shops does not guarantee that the online systems provided will be reachable, available and error-free at all times. Access and transmission delays or failures may occur as a result of technical difficulties that are beyond the control of Trusted Shops.

O. Term of Contract

1. The minimum term of the user agreement is 12 months. The agreement shall be extended by one year if it is not terminated 3 months prior to the expiry of the respective 12-month period.

2. The right to notice-free, extraordinary termination of the agreement for good cause remains unaffected.

3. Good cause for notice-free, extraordinary termination by Trusted Shops is where, in particular, the user, despite a dunning notice, is more than 30 days in arrears with payment of its annual user fee.

P. Contractual Amendments

Amendments to the General Conditions of Use (TS-ANB-DSGVO-Schutz) shall be notified to the user in text format (§ 126b BGB). Such amendments shall be deemed to have been accepted if the user does not disagree with them in text format. Trusted Shops shall specifically inform the user of this in its notification letter. Any disagreement must be received within four weeks of the notification being received.

Q. Final Provisions

1. Those declarations concerning the members shall only be applicable if they are received in text format. Terminations must be made in writing.

2. German law shall apply exclusively to these conditions and to any and all disputes resulting therefrom or relating thereto.

3. The language of the agreement is German.

4. If the user is a businessperson, a legal person under public law or a public-law special fund, then the place of jurisdiction is Cologne, unless another exclusive jurisdiction is named. The same shall apply if the user has no general jurisdiction in Germany or its base or usual residence are unknown at the time the action is brought.

Appendix 1

Agreement on the processing of personal data by a data processor between the user designated in the Main Agreement, the responsible party, hereinafter also referred to as **the Principal** and **Trusted Shops GmbH, Subbelrather Str. 15C, 50823 Cologne**, the processor, hereinafter also referred to as the **Contractor,** collectively referred to hereinafter as **the Parties**

This Appendix defines the obligations of the Parties with regard to the processing of personal data by a data processor deriving from the Main Agreement. They shall apply to the following activities (not exhaustive) that are covered by the Main Agreement and by which the Principal's personal data shall be processed by employees or agents of the Contractor (hereinafter referred to as **Data**):

- Upload of documents which are designated for combination with the records of processing activities generated via the **GDPR Manager**, e.g. sub processing agreements

The Appendices to this Appendix can be retrieved at http://support.trustedshops.com/lp/en/legal_order_processing_appendices. The user shall be informed of the relevant specifications regarding modifications. Trusted Shops may amend this Appendix and its Appendices by giving notice in writing to Principal. Such amendments will be deemed to be approved by Principal unless Principal objects to the amendments in writing within thirty 30 days following receipt of such notice.

Definitions

For all terms mentioned hereunder, for which Art. 4 General Data Protection Regulation (hereinafter referred to as the **GDPR**) provides a definition, such statutory definition shall also apply to this Agreement.

A Object and duration of the order

A1 The object and duration of the order as well as the type and purpose of processing derive from the Main Agreement, including all Appendices and amendments.

A2 The categories of data to be processed as well as the categories of the data subjects concerned are set out in **Appendix 1** attached hereto.

A3 The term of this Appendix depends on the term of the Main Agreement, notwithstanding any additional obligations under the provisions of this Appendix.

B Obligations of the Contractor

B1 The Contractor and any Person under its authority with access to personal data may process Data on data subjects solely within the scope of the Agreement and on the documented instructions of the Principal, unless an exception within the meaning of Article 28(3)(a) of the GDPR is applicable.

B1.1 The Contractor shall inform the Principal immediately if it considers that an instruction violates applicable law. In such a case, the Contractor may suspend implementation of the instruction until confirmed or amended by the Principal.

B1.2 The instructions shall be initially set out in the Main Agreement and can be confirmed subsequently by the Principal in writing or in an electronic format (text form) and must be immediately transmitted to a location designated by the Contractor by way of special verbal instructions.

B1.3 Instructions that go beyond the contractually agreed services shall be treated as a request for a modification of service. Costs arising therefrom shall be borne by the Principal.

B2 The Contractor shall design the in-house organisation in its area of responsibility in such way that the specific data protection requirements are satisfied. It shall meet the technical and organisational measures for adequate protection of the Principal's Data, which satisfy the requirements General Data Protection Regulation (Art. 32 GDPR). The Contractor shall take such technical and organisational measures that ensure the permanent confidentiality, integrity, availability and resilience of the system and services related to the processing.

B2.1 The Contractor shall document the implementation of its technical and organisational measures before the start of processing, especially with regard to the precise execution of the order and submit it to the Principal for review.

B2.2 The documented and agreed technical and organisational measures are attached hereto as **Appendix 2** and are part of this Agreement. The Principal is familiar with

these technical and organisational measures and shall be responsible for ensuring an appropriate level of protection for the risks to the data to be processed.

B2.3 The technical and organisational measures underlie technical progress and further development. Insofar as the Contractor is allowed to do so, it shall implement adequate alternative measures. In doing so, the security level must not fall short of the measures set out. Significant changes must be documented.

B3 The Contractor is solely authorised to correct, delete or limit the processing of Data processed by subcontractors in strict observance of the Principal's documented instructions.

B3.1 Excepted from this is the case of a data subject who makes a direct request regarding their rights to the Contractor. In this case the Contractor will contact the Principal to clarify whether the request of the affected party shall be processed by him or the Principal himself. After approval by the Principal, the Contractor is entitled to take all measures necessary to protect the rights of the persons concerned within the scope of his possibilities

B3.2 The Contractor shall provide support to the Principal in processing and responding to requests from data subjects whenever possible with the proper technical and organisational measures. Costs justified in this regard shall be borne by the Principal.

B3.3 Provided they fall within the scope of services, the concept of data deletion, the right to be forgotten, rectification, data portability and information in accordance with the instructions of the Principal must be immediately ensured by the Contractor.

B4 In addition to compliance with the provisions of this assignment, the Contractor shall also ensure compliance with legal obligations pursuant to Art. 28-33 of the GDPR. In this particular regard, it shall ensure compliance with the following conditions:

B4.1 The Contractor shall provide to the Principal the contact details of the in-house data protection officer, insofar as one must be appointed pursuant to Art. 37 of the GDPR. The internal data protection officer exercises his/her activity pursuant to Art. 38 f. of the GDPR.

If the Contractor is not obliged to appoint a data protection officer, it shall designate for the Principal a contact person for matters related to the processing of personal data.

B4.2 To preserve confidentiality during the execution of the tasks pursuant to Art. 28(3), p.2, b, 29, 32(4) of the GDPR, the Contractor shall use solely employees who are bound by an obligation of confidentiality and who have been familiarised beforehand with the relevant provisions on data protection. The Contractor shall ensure that it is prohibited for personnel assigned to the

processing of the Principal's Data and other persons acting on behalf of the Contractor to process the Data outside the scope of the instruction.

B4.3 The Contractor shall provide support to the Principal to the extent feasible for satisfying requests by the supervisory authorities or the queries and claims by data subjects pursuant to Chapter III of the GDPR, Art. 82 of the GDPR, as well as for compliance with the obligations set out in Art. 32 to 36 of the GDPR. Costs arising therefrom shall be borne by the Principal, unless the Contractor is responsible for the assertion of such claims, inquiries and the occurrence of reporting obligations. Furthermore, the obligation to bear costs does not apply to the provision of information for the fulfilment of transparency obligations

B4.4 The Contractor shall immediately inform the Principal of any serious disruption to operations or any serious breaches by the Contractor or its personnel of the provisions for the protection of personal data for the Principal's assignment, the specifications hereunder or any other anomalies related to processing of the Principal's Data. It shall take the required measures for securing Data and mitigating possibly more harmful consequences for the parties concerned.

B4.5 The Contractor shall immediately inform the Principal of control procedures and measures by the supervisory authority that are relevant to this assignment. This shall also apply to the extent that a competent authority investigates the Contractor's order processing as part of a regulatory or criminal offence related to the processing of personal data.

B4.6 Insofar as the Principal, for its part, is exposed to inspection by the supervisory authority, for an offence or criminal proceedings, for the liability claim of a data subject or third party or any other claim related to the Contractor's order processing, the Contractor shall support it to the best of its ability. Costs justified in this regard shall be borne by the Principal.

B4.7 The Contractor shall regularly inspect the internal processes as well as the technical and organisational measures to ensure that processing in its area of responsibility is consistent with the current requirements of data protection law and ensuring the protection of the data subject's rights.

C **Obligations of the Principal**

C1 As part of this Agreement, the Principal shall be solely responsible ("Responsible Party" within the meaning of Art. 4(7) of the DSGVO))for regulatory compliance with the statutory provisions of data protection laws, in particular for the legality of the Data transfer to the Contractor as well as for the legality of the data processing. In particular, the Principal is responsible for effectively obtaining all necessary consents from the concerned parties as part of the execution of the order.

C2 The Principal shall fully and immediately inform the Contractor of any errors or anomalies it detects from job results related to data protection provisions.

C3 The Principal shall provide the Contractor with the name of a contact person for any data protection issues arising under the Agreement.

D **Subcontractor**

D1 Subcontracting conditions in the context of this regulation means the provision of services by the Contractor to other Contractors commissioned in whole or in part for a service covered by the Agreement.

D1.1 Ancillary services that the Contractor uses e.g. as telecommunication services, post/transport services, maintenance and user service or the disposal of data carriers, as well as other measures aimed at ensuring the confidentiality, availability, integrity and resilience of hardware and software of data processing Appendices, do not belong to this group, unless the Subcontractor can gain access to personal data. In order to ensure the privacy and protection of the Principal's data, the Contractor is also obliged to make the appropriate and legal contractual arrangements regarding ancillary services,

even such which do not allow access to personal data and to take control measures.

D2 The Contractor may only commission subcontractors (additional processors) after express prior written or documented consent by the Principal.

D2.1 The Principal agrees to the commissioning of the subcontractor designated in **Appendix 3,** provided that a contractual agreement has been concluded between the Contractor and the Subcontractor for the processing of personal data on behalf of the Contractor, which imposes on this further subcontractor, by means of a contract or other legal instrument under Union law or the law of the Member State concerned, the same data protection obligations as those laid down in this Agreement or other legal instrument between the controller and the processor in accordance with Article 28 (3) GDPR.

D2.2 Outsourcing to other subcontractors or changing the existing subcontractor is allowed, provided that:

- the Contractor shall notify the Principal of such outsourcing to subcontractors in writing or electronically with 30 days' prior notice.
- the Principal raises no objection in writing or electronically against the planned outsourcing until the moment of transfer of data to the Contractor; **and**
- a contractual agreement is prepared pursuant to Art. 28 Para. 2-4 of the DSGVO.

D2.3 If no objection is raised within the time limit, consent to modify shall be deemed granted. Where an objection is raised and it proves impossible to find an amicable solution between the Parties, the Parties shall grant an exceptional right to termination with regard to the Main Agreement, until the time of transfer of the data to Subcontractor.

D2.4 The transmission of the Principal's personal data to the subcontractor and when it first takes action, are only allowed if all subcontracting conditions are met.

D3 If the Subcontractor performs the agreed services outside of the European Union/ European Economic Areas, the requirements of Section E shall also apply. The same shall also apply if service providers must be used pursuant to para. D1.1(2).

E **Processing location**

E1 The Contractor shall gather, process or use Data exclusively in a Member State of the European Union or of another State party to the European Economic Area Treaty.

E2 In special cases, the Contractor may derogate therefrom, provided the Contractor has ensured the permission to transmit to third countries under data protection law by the measures set out in Art. 44 et seq. of the DSGVO. Paragraphs D2.1 and D2.2 shall apply mutatis mutandis.

F **The Principal's monitoring rights**

F1 The Contractor shall prove, by appropriate means compliance with the obligations set out hereunder, to the Principal.

F2 Proof of such measures that do not solely concern a definite order can be provided at the Contractors' discretion by:

F2.1 conducting a self-assessment;

F2.2 intragroup rules of conduct including external certification of compliance;

F2.3 compliance with authorised rules of conduct pursuant to Art. 40 of the DSGVO;

F2.4 certification in accordance with an approved certification process pursuant to Art. 42 of the DSGVO;

F2.5 current certificates, reports or report extracts from independent bodies (e.g. auditors, data protection officers, IT Security Department, revision, data protection auditors, quality auditors);

F2.6 an appropriate certification by means of an IT data security or privacy audit (e.g. according to the Federal Office for Information Security - Basic level of security (*BSI-Grundschutz*).

F3   If, in individual cases, inspections by Principal or an inspector commissioned by Principal should be necessary, because the proof specified in paragraphs F1and F2 is not sufficient, inspections shall be carried out during normal business hours without disrupting the course of operations after registration, taking into account a reasonable notice time. If the inspector commissioned by Principal is in a competitive relationship with Contractor, Contractor has a right of objection against this.

G   **The deletion and return of personal data**

G1   Data copies or duplicates shall not be created without the Principal's knowledge. Exceptions are backups required for ensuring proper data processing and Data required for compliance with statutory obligations.

G2   Following completion of the contractually agreed work or earlier if so requested by the Principal – and no later than termination of the performance agreement – the Contractor shall return all documents, processing and user results compiled as well as Data files related to the contractual relationship in its possession, and hand them over to the Principal or destroy them according to the latter's choice, pursuant to data protection provisions, provided there is no storage obligation for personal data according to European Union law or the applicable law of the relevant Member State. The same shall apply for test and waste material. The deletion log must be presented upon request. Documentation intended for substantiating the order and for proper data processing, must be kept by the Contractor in accordance with the retention periods, beyond the term of the Agreement indicated. It can discharge itself of its liabilities by handing such documentation over to the Principal at the end of the Agreement.

G3   Any additional costs arising as a result of the Principal's deviating requirements for the issuing or deletion of the data shall be borne by the Principal.

H   **Liability and damages**

The Principal and the Contractor shall also be liable vis-à vis data subjects insofar as there is a deviation from the agreed liability regulations in the Main Agreement - in accordance with the rules set out in Art. 82 of the DSGVO.

I   **Information requirements, written form and governing law**

I1   Should the Principal's data with the Contractor be at risk of seizure or confiscation, insolvency or by other events or third party measures, the Contractor shall immediately inform the Principal thereof. the Contractor shall immediately inform all Responsible Parties in this regard thereof that the control and ownership of the Data lie exclusively with the Principal as "Responsible Party", pursuant to the General Data Protection Regulation.

I2   Modifications and amendments to this Appendix and all of its components – including any the Contractor warranties – must be agreed in writing. They may also be made in an electronic format (text form), with the express indication thereon that it is a change or amendment to these conditions. This shall also apply for the waiver to this form requirement.

The regulations of this Appendix on data protection shall prevail over regulations of the Main Agreement in the event of any discrepancies in this regard.