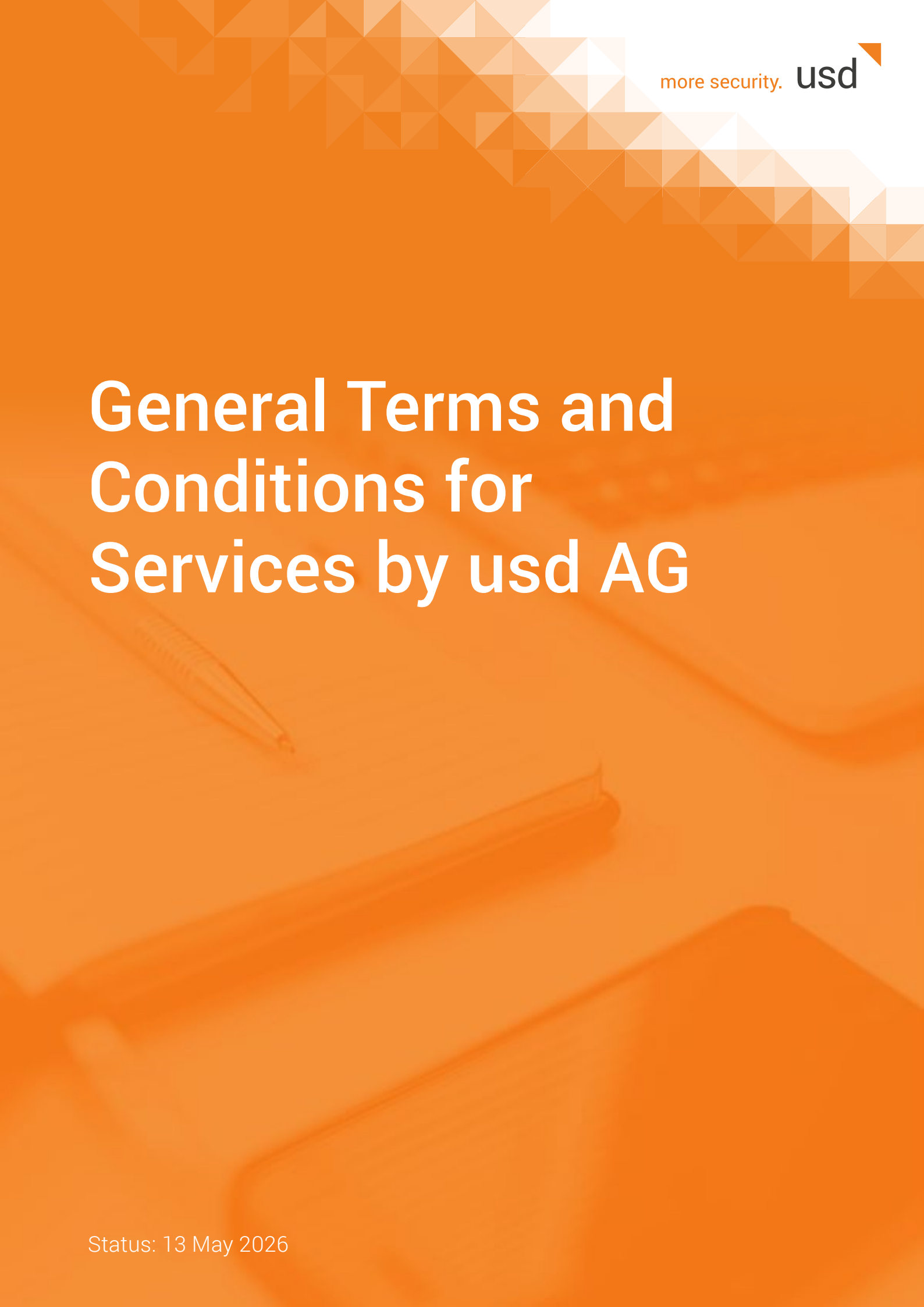
more security. usd

General Terms and Conditions for Services by usd AG



Status: 13 May 2026

General Terms and Conditions for Services by usd AG (13 May 2026)

Section A: General Terms

All contracts concluded with usd AG (hereinafter referred to as "usd" or "Supplier") in the context of consulting services shall be concluded and executed exclusively in accordance with these General Terms and Conditions. Conflicting conditions of the Client shall not be valid unless and until they have been accepted in writing by the Supplier.

§ 1 Services provided by the Supplier

(1) Unless otherwise agreed in individual cases, the activity of the Supplier shall consist in providing independent and advice free from instructions to the Client as a service.

(2) If the Supplier acts as a processor in the sense of the European General Data Protection Regulation (EU-GDPR) for the Client, it undertakes to take appropriate technical and organizational measures to ensure that the processing is carried out in accordance with the EU-GDPR.

(3) The specific content and scope of the work to be performed is described in the Supplier's service offer and confirmed by the Client by means of a written acceptance of the offer or placing an order.

(4) Should the necessity for additional or supplementary activities arise, the Supplier shall draw the Client's attention to this fact. In this case, the Supplier shall also extend the scope of the order if the Client requests or accepts the additional or supplementary work.

(5) The provision of legal counsel or tax advice is excluded as part of the contract.

(6) The service shall be provided within a period of one year from acceptance of the offer or order. If the performance period of one year is exceeded, the Supplier reserves the right to terminate the project prematurely. For the provision of further services, a separate offer acceptance or order is then required.

(7) The Client shall be solely responsible for deciding on the type, scope and timing of implementation of the measures recommended by or agreed upon with the Supplier. This applies even if the Supplier assists the Client in implementing coordinated plans or measures.

(8) The forwarding or presentation of written work or results of the Supplier to third parties by the Client shall require the prior consent of the Supplier and shall be carried out solely in the interest and on behalf of the Supplier. The third party is not included in the scope of protection of the contract between the Client and the Supplier. This shall also apply if the third party bears or takes over, in whole or in part, the remuneration for the Supplier's work for the Client.

(9) Unused services expire one year after receipt of the order.

§ 2 Obligations of the Client to cooperate

(1) The Client shall appoint a competent contact person who can answer all necessary questions and make all related decisions. In addition, the Client shall provide the Supplier with the information and documents required for the execution of the order in full and accurate form.

(2) The Client confirms to the Supplier that the information and documents provided by the Client are complete and correct and that no indications exist or are known which are suitable to call their completeness and correctness into question. The Supplier is not obliged to verify the accuracy, completeness or correctness or to carry out its own research. This shall also apply if the Supplier is required to carry out plausibility checks as part of the order placed, which are based solely on the information, details or documents provided by the Client and do not involve their verification.

(3) If the Client does not perform or does not perform in full the acts of cooperation to which it is obliged after being requested to do so by the Supplier, the Supplier shall be entitled, but not obliged, to terminate the concluded contract without period of grace after prior written notice. In this case, the Supplier may invoice the Client either for the services actually rendered up to the time of termination or, instead, for the agreed or forecast total remuneration reduced by the expenses saved by the premature termination of the contract.

(4) All communication with the Client is in English or German. Furthermore, the Client is obliged to provide necessary documentation in one of these two languages. Should employee interviews be necessary within the scope of the services offered, the Client ensures that these can be conducted in English or German. The support of additional languages shall be requested by the Client prior to the placing of the order and confirmed by usd if possible.

(5) Performance-specific obligations to cooperate may deviate from the general obligations to cooperate and are regulated in sub-documents B and C or in the respective service offer.

(6) The Client undertakes to provide the Supplier (or its authorized representative), at the Supplier's request, with a list of the items outstanding against the Supplier on a key date specified by the Supplier for the purpose of a balance reconciliation within a reasonable period of time. The list must contain at least all outstanding invoices, credit notes, unreconciled payments, overpayments, items on the suspense account and all other items relating to the Supplier.

§ 3 Project Termination and Lead Time in the Event of Termination by the Client

(1) The Client may not terminate individual projects or project components immediately or without notice, unless there is a legally mandatory reason for termination resulting from a material breach of duty for which the Contractor is responsible.

(2) Upon termination of a project, the Client must provide reasonable notice to allow for the orderly completion of the work. The required notice period is determined in particular by the scope, duration, and complexity of the project, as well as its total economic volume, and shall be at least six (6) weeks.

(3) The purpose of this notice period is to enable the contractor to properly wind up the project, finalize documentation, hand over work results, and carry out proper resource planning. Services that are provided in accordance with the contract prior to the termination taking effect, or that are necessary as a result of the termination process, must be paid for in full.

§ 4 Remuneration

(1) Unless otherwise agreed in individual cases, the Supplier's services shall be invoiced on a time and effort basis in accordance with the daily rates agreed in the service offer (one day equals eight hours), plus travel costs and expenses. Travel costs incurred in connection with a flight may include the payment of CO2 compensation (max. 200 euros/flight or max. 20 % of the flight price).

(2) Time and remuneration forecasts of the Supplier in relation to the execution of an order represent a non-binding estimate. Deviations from the estimate cannot be ruled out by the Supplier, as the time required may depend on factors which cannot be influenced by the Supplier.

(3) If the exceeding of the predicted time or remuneration volume is due to circumstances for which the Client is responsible (e.g. insufficient cooperation on the part of the Client), the resulting additional expenditure shall be remunerated according to the agreed daily rates.

(4) If the actual processing time is more than 30 % higher than the forecast time or remuneration, the Client has the right to choose, after being informed by the Supplier, either to terminate the contract and remunerate the services rendered up to that point on the agreed terms, or to continue the contract and additionally pay the excess working time on a daily rate basis.

(5) In the event of cancellation of agreed service contents by the Client, the Client shall pay 100 % of the agreed fee as a cancellation fee for cancellations with a shorter lead time than 10 working days prior to the date of performance, provided that the Supplier cannot use the time freed up by the cancellation of the appointment for other economic purposes. The same applies in the event of a short-term postponement of the date by the Client. Cancellations or postponements must always be made in text form by email, fax

or letter. Travel expenses (hotel, train rides, flights, etc.) that can no longer be reimbursed at this point will be charged to the Client in full.

(6) For assignments that are carried out at the Client's request on weekdays (Monday - Friday) between 8:00 p.m. and 6:00 a.m. (CET/CEST), the booked and billable expenses shall be multiplied by a factor of 1.5. On Saturdays, Sundays and German public holidays, these are multiplied by a factor of 2.0. Support by usd outside of regular working hours shall be requested by the Client prior to the placing of the order and confirmed by usd.

(7) It is possible to invoice the services at a fixed price, provided that the service to be provided is a deliverable that can be checked and approved by the Supplier. If a service is provided at a fixed price, the Supplier is not obliged to estimate or document the expenses. Unless otherwise agreed in writing in individual cases, travel costs and expenses are included in the fixed price.

(8) The project costs may be increased by general expenses for bank charges, office supplies or communication, for example. These will not exceed 2 % of the fee volume without consultation with the Client.

§ 5 Terms of payment

Invoices are issued in ZUGFeRD format. Routing IDs must be communicated to the Supplier in advance as part of the order. Invoices are sent exclusively electronically by email. Invoices are due for payment without deductions upon receipt by the Client. Invoices are to be transferred to the account specified by the Supplier at the latest on the 14th calendar day after the invoice date.

§ 6 Tax conditions

(1) The remuneration agreed with the Supplier is a net price which is payable plus the applicable statutory national value added tax.

(2) The Client is obligated to inform usd about the respective billing address as well as the respective place where the service should be performed with the placement of the order. If the place where the service should be performed is at a permanent establishment of the Client, it is to be considered as the place of performance and the correct statutory value added tax regulation for the respective place of performance has to be applied during the invoicing process. If no additional information is provided by the Client usd assumes that the address declared in the offer is to be considered both the billing address and the place of performance.

(3) In case of one or several places of performances outside of Germany, the Client is obligated to provide the following information to usd with the order placement:

a) Place of performance outside of Germany but inside of EU: Declaration of the valid VAT-ID for all places of performances communicated to usd according to paragraph 2.

b) Place of performance outside of Germany and outside of the EU: Provision of a "Certificate of registration as a taxable person (entrepreneur)" issued by the designated foreign tax office for all places of performances communicated to usd according to paragraph 2.

(4) If the place of performance is situated outside of Germany and the Client provides usd with the required information mentioned in paragraph 3a) and 3b) in a timely manner before the preparation of the first invoice, usd will issue its invoice with no value added tax. If the necessary documents were not transmitted in a timely manner, usd is authorized to issue the invoice including the statutory value added tax applicable at that time (according to present law 19 %) in order to transfer the tax to the responsible German tax office.

(5) Invoicing is carried out in accordance with the German Value Added Tax Act (UStG) and, if applicable, the European VAT Directive. Accordingly, the provision of another service to an entrepreneur resident in a third country is not taxable in Germany. The invoice will therefore be issued without showing VAT (net).

The Parties agree that the Client (economically) owes any taxes and duties that may be due under laws other than German law and is responsible for a proper declaration to the local tax authorities. This Agreement includes all types of taxes, in particular also VAT and all withholding taxes. Alternatively, the price for the services rendered shall be increased by these taxes and duties. The Supplier is entitled to claim these taxes and duties from the Client even after the conclusion of the exchange of services.

§ 7 Liability

(1) Information, explanations, advice or recommendations given in person or by telephone are given to the best of our knowledge and belief. However, they are only binding if they are confirmed in writing.

(2) Any liability or warranty for the success of the services provided by the Supplier and recommended measures is excluded. This also applies if the Supplier assists in the implementation of agreed or recommended plans or measures.

(3) The Supplier shall have unlimited liability in the event of intent or gross negligence. In the case of slight negligence, liability is limited to the typical foreseeable damage, up to a maximum of EUR 25,000.00.

(4) The Supplier shall not be liable if the damage incurred is due to incorrect or incomplete information or documents provided by the Client or was caused by intent or gross negligence on the part of the Client. The same shall apply if the Client fails to notify the

Supplier in writing within 14 calendar days of becoming aware of circumstances giving rise to liability.

(5) The above provisions shall also apply in favor of the Supplier's employees and other vicarious agents.

(6) The aforementioned limitations of liability and exclusions do not affect the Client's claims based on injury to life, body and health. Also excluded from the exclusion of liability is product liability.

(7) The Supplier is entitled to the objection of contributory negligence of the Client.

(8) Should the Supplier not be able to provide the agreed services over a certain period of time, the Client will be informed immediately. The Supplier undertakes to provide appropriate compensation.

(9) The Supplier shall not be liable for a lack of economic success of the Client.

(10) If force majeure (e.g. natural disasters, war, terrorist attacks, epidemics) renders the performance of services permanently impossible, the Supplier shall not be obliged to perform; in this case, any fees already paid to the Supplier for services not yet performed shall be refunded.

§ 8 Secrecy

(1) “Confidential Information" shall refer to all information (whether written, electronic, oral, digital or otherwise) exchanged between the Parties for the previously mentioned purpose, whether or not explicitly designated as "Confidential". Confidential Information in this sense shall mean in particular:

- Offer and contract documents, project contents and results, specifications, drawings, software materials, data, know-how or trade secrets;
- Any documents and information of the holder that are subject to technical and organizational secrecy measures and are marked as confidential or are to be considered confidential according to the nature and information or the circumstances of the transmission;
- The existence of this Agreement and its contents.

No Confidential Information is such information for which the Party that received the Confidential Information in question can prove that the Confidential Information:

- is a matter of public record at the time of disclosure and that circumstance is not due to their misconduct; or
- at the time of disclosure to the receiving Party, was already known to that Party without restriction, i.e., lawfully and without a duty of confidentiality, with written evidence to that effect in that Party's possession; or

- was developed independently of the disclosed information by the receiving Party itself, as evidenced by inspection of the written records; or
- was handed over or made accessible to the receiving Party by an authorized Third Party without breach of a confidentiality obligation; or
- is exempt from such restrictions upon written consent by the disclosing Party.

(2) The Parties each undertake to:

a) treat Confidential Information as confidential with at least the same degree of care that they ordinarily use to protect their own confidential or proprietary information;

b) use Confidential Information only for the purpose contemplated by this Agreement;

c) limit the disclosure of such information to those employees who have a need to know for the purpose for which it is intended and to inform eligible employees of the commitments made in this Agreement. The Parties shall ensure that all eligible employees are aware of the material content of this Agreement;

d) insofar as the Parties enter into contracts with Third Parties within the scope of the business relationship between the Parties, to conclude agreements with such Third Parties which correspond to the content of this Agreement and to ensure compliance therewith;

e) not to disclose to Third Parties under any circumstances information about offered, negotiated or changed amounts of fees, transfer prices, commissions or other payments agreed within the framework of a contractual relationship and to ensure that only those of its employees gain knowledge of this information for whom it is absolutely necessary in order to decide whether to enter into a contractual relationship or to execute a concluded contract;

f) additionally secure Confidential Information against unauthorized access by Third Parties by means of appropriate confidentiality measures and to comply with the statutory and contractual provisions on data protection when processing the Confidential Information. This also includes technical security measures adapted to the current state of the art (Art. 32 GDPR) and the obligation of employees to maintain the confidentiality of personal data and to comply with data protection as defined in Art. 28 para. 3 lit. b GDPR.

Each Party shall be entitled to disclose Confidential Information if it is required to do so by law or governmental order, has notified the other Party in writing (to the extent legally possible and practicable) of the intended disclosure, and has taken reasonable precautions required by law to minimize the extent of the disclosure.

§ 9 Data protection

(1) Within the scope of the provision of services, it is possible that the Supplier's consultants may inspect personal data stored by the Client. The inspection is classified as a transmission process under data protection law.

(2) By signing the service agreement or the offer, which is part of the intended contract, the Client assures that he is entitled to the possible transfer of personal data. Otherwise, the Client excludes the inspection of personal data by means of suitable measures (e.g. pseudonymization or anonymization).

(3) The Supplier has obliged all employees entrusted with the performance of the contract to strictly comply with the applicable data protection regulations. The Supplier shall not store any personal data viewed in the course of the performance of the services or shall only store, use or process such data to the extent and for as long as this is absolutely necessary for the performance of the respective contract.

(4) In all other respects, any further processing of personal data by the Supplier shall be carried out exclusively on the instructions of the Client. The Supplier may only process or use the Client's data within the scope of these instructions. In Section D the Parties shall conclude a commissioned data processing agreement.

§ 10 Loyalty commitment

Client and Supplier are committed to mutual loyalty. In particular, the enticement of employees who have been active in connection with the execution of the order before the expiry of two years after the end of the cooperation is to be refrained from.

§ 11 Other activities

The Supplier is free to work for other clients. The prior consent of the Client is not required for this.

§ 12 Copyright, rights of use and exploitation

The Client is entitled to use the contractual services for the contractually stipulated purpose without local, personal or quantitative restrictions. For this purpose the Supplier grants the Client the irrevocable, worldwide, unlimited and non-exclusive right of use. The transferred rights are not subject to any restrictions on disposal.

§ 13 Feedback on the performance of the Supplier

In order to continuously improve the services and adapt them to the needs of the Client, the Supplier shall ask the Client to provide feedback on satisfaction after the performance of the services offered.

§ 14 Designation as reference customer

The Contractor shall be entitled to designate the Client as a reference customer upon successful completion of the project and to use the Client's company logo in reference lists (print, website, social media, presentations, proposals, and tenders). Such use shall be made solely as a factual indication of the existing or completed cooperation and in compliance with the Client's brand guidelines.

The publication of any further information (such as press releases, case studies, testimonials, or a detailed description of the project) shall take place only following prior agreement with the Client.

Confidential information and securityrelevant details shall not be disclosed; Section 8 (Secrecy) remains unaffected.

Upon request, the Contractor undertakes to provide information at any time on whether and to what extent such use is taking place; the relevant information shall be provided to the Client free of charge.

The Client may revoke its consent at any time, in whole or in part, without stating any reasons. The Contractor shall implement the revocation within ten (10) working days at the latest.

§ 15 Closing provisions

(1) All annexes to the Service Agreement or the offer form an integral part of the contract between Supplier and Client. The regulations in the Service Agreements replace the General Terms and Conditions in the event of deviations.

(2) Amendments or supplements to the order or these General Terms and Conditions must be made in writing to be effective. Tacit changes to the order or the General Terms and Conditions are excluded.

(3) Should a provision of a Service Agreement or these Terms and Conditions be or become legally ineffective, this shall not affect the legal effectiveness of the remaining provisions of the order and these Terms and Conditions. In this case, a legally effective provision shall be agreed between the contract parties which comes closest to the meaning and purpose as well as the economic objective of the invalid clause. The same procedure shall be followed if the order or these Terms and Conditions contain a loophole that is contrary to the rules, which is to be closed by a contractual amendment.

(4) The law of the Federal Republic of Germany applies exclusively, excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG).

(5) The exclusive place of jurisdiction is Frankfurt am Main, Germany, if the Client is a merchant. In addition, the Supplier is also entitled to bring an action at the Client's general place of jurisdiction.

(6) In case of doubt, the German text of the General Terms and Conditions and their constituent parts as well as the service offers of the Supplier shall take precedence over translations in other languages.

(7) Service-specific GTCs may deviate from the general GTCs and are regulated in the individual agreements, service contents or in the GTC sub-documents B and C.

(8) The Supplier shall keep the elaborations and results produced within the scope of the commissioned activity available for retrieval by the Client for a period of 6 years after completion of the commissioned activity. Prior to the expiry of this period, the Client may request the Supplier to delete the elaborations and results at any time. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data that is required with regard to compliance with statutory retention obligations. Also not included is evidence regarding the orderly and proper performance of the agreed activity. These are stored beyond the end of the contract in accordance with the respective retention periods to be observed.

Section B: Technical Security Analyses & Penetration Tests

§ 1 Liability, limitation of liability, exclusion of liability

(1) The Supplier is not obliged to verify whether the Client has full and unlimited rights to the IT system and/or application to be tested.

(2) The liability for data loss is limited to the typical recovery effort that would have been required if back-up copies had been made regularly and in accordance with the risk. The Supplier shall not be liable for any damages caused by the Client interrupting the technical security analysis during execution.

§ 2 Indemnity obligation of the Client

(1) If a third party (e.g. a customer or service provider of the Client) makes a claim against the Supplier due to possible effects of the technical security analysis on the IT system and/or the application, the Client undertakes to indemnify the Supplier against any claims, provided that

a) the technical security analysis met a generally accepted and appropriate standard (otherwise 'Section A liability' shall apply); or

b) the damage was (partly) caused by a breach of duty by the Client because the Client

- has had an external IT system/application tested without appropriate permission,
- failed to inform affected third parties, or failed to inform them within a reasonable period of time, of the technical security analysis being carried out, or
- has not been granted permission under data protection law to transfer personal data.

(2) The obligation to indemnify refers to all expenses necessarily incurred by the Supplier or its employees and other vicarious agents as a result of the extrajudicial, official and/or judicial claims by a third party. The Client must assume all costs and fees for the necessary legal prosecution, as well as all damages, losses and expenses.

§ 3 Warranty

(1) The Supplier expressly points out to the Client that the technical security analysis may influence the integrity and availability of the tested IT systems and/or applications.

(2) The Supplier shall guarantee and ensure that the methods and tools used for the technical security analysis comply with a generally accepted and appropriate standard.

(3) The Supplier shall have no further obligation or warranty. The Supplier is not subject to any warranty liability in the event of damage due to an impairment of the integrity and/or the availability of the tested IT system and/or the application, which is or was caused by a proper, i.e. by a technical security analysis carried out in accordance with generally accepted and appropriate standards.

(4) Otherwise Section B, §1, "Liability, limitation of liability, exclusion of liability" shall apply accordingly.

§ 4 Obligations of the Client to cooperate

(1) By commissioning the Service Agreement, the Client assures that the technical security analysis is carried out or intended to be carried out on the Client's IT systems and/or applications provided in writing by the Client.

(2) Insofar as the technical security analysis is not carried out on the Client's IT systems and/or applications, the Client assures upon commissioning the Service Agreement that it has the full and unrestricted right to carry out the technical security analysis on the IT systems and/or applications.

(3) At the request of the Supplier, the Client must prove that it has the unrestricted right to commission the Supplier to carry out the technical security analysis and the rights to access the IT systems and/or applications.

(4) Prior to the performance of the technical security analysis by the Supplier, the Client undertakes to fully back up all IT systems and/or applications to be tested by the Supplier and the associated data. In addition, the Client must take all necessary security measures, including those that go beyond a backup, before using the service, in order to be able to restore the IT systems and/or applications and data to their original state after the technical security analysis, if necessary.

(5) Depending on the type of technical security analysis, the Client shall provide the Supplier with the information and documents necessary to execute it as safely and securely as possible. Before the technical security analysis is carried out, the Supplier shall inform the Client what information is required. The Client will then provide the Supplier with the necessary complete and correct information in a timely manner.

(6) The Client shall inform any affected third parties about the technical security analysis out within a reasonable period of time before the technical security analysis is carried out, since IT systems and/or applications of third parties, such as the provider's router or the web server of a hoster, are also used in a technical security analysis and, despite sufficient security, an impairment of the proper operation of these IT systems and/or applications cannot be excluded.

(7) The Client is expressly advised that the technical security analysis may cause damage to existing IT systems and/or applications. In particular, the technical security analysis may result in impairments and changes to content and data, such as layout changes on a

website or impairments to the Client's server. These damages can usually only be remedied by installing backups or by - sometimes extensive - post-processing by the Client. Furthermore, the Client is advised that the Client's IT systems and/or applications may not be usable during the technical security analysis.

§ 5 Tools used

(1) The Supplier shall use the best tools available worldwide for technical security analyses. The use of these tools allows the Supplier to render its tests more efficient and therefore much more comprehensive. The Client benefits from very high-quality results. The resulting license costs are already included in the respective offers and are not charged separately.

(2) Technical security analyses carried out from the Supplier's offices via the internet are performed from a dedicated public network with known fixed IP addresses. This ensures that the Supplier's activities can be clearly identified at any time by the Client's operational managers.

§ 6 Responsible Disclosure

(1) Vulnerabilities in standard products not manufactured by the Client shall be reported by the Supplier in a structured process for responsible disclosure of security vulnerabilities.

(2) This shall be done in strict confidence, in writing and in a form that allows the manufacturer to understand and close the vulnerability.

(3) The Supplier reserves the right to publish the vulnerabilities found.

(4) Within a period of 60 days the manufacturer shall provide a solution. If this is not done, publication may still take place after this period.

(5) The Supplier may deviate from this procedure in cases where a different approach would demonstrably reduce the risks to all parties concerned.

(6) By commissioning the Service Agreement, the Client agrees to the described procedure.

Section C: Security Audits

§ 1 Obligations of the Client to cooperate: KRITIS Audit (critical infrastructure)

(1) Since the Supplier proves its qualification as a KRITIS Auditor via a self-declaration of the auditing body ("Selbsterklärung der prüfenden Stelle", see BSI), the Client is obliged to submit the self-declaration together with the official assessment documents to the BSI.

(2) In addition, the Client shall provide the Supplier with its industry-specific security standard (B3S).

§ 2 Obligations of the Client to cooperate: PCI Security Services

(1) The Client has provided the Supplier with information on its audit scope, which was used to determine the price when preparing the offer. If the actual scope deviates from the assumed scope due to incorrect or incomplete information, the Supplier reserves the right to invoice the Client for any additional expenses incurred in the performance of the audit upon consultation.

(2) In the context of PCI SSF and PCI Secure Software Standard (part of PCI SSF) Assessments, the Client shall additionally provide the required test environment (see current "Secure Software Template for Report on Validation", Appendix B).

§ 3 Other PCI DSS services

In order to use the PCI DSS scanning services, the PCI DSS certificate and the PCI DSS Seal of usd, the General Terms of Use for the Security Platforms of usd AG, which apply to these services, must be observed: https://www.usd.de/en/terms-conditions/

§ 4 Feedback on services provided by usd

The PCI Security Standards Council (PCI SSC) gives the Client the opportunity to provide central feedback on the QSA services provided by the Supplier. The Client can access the PCI SSC feedback form under the following link: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback

§ 5 PCI Security Standards Council (PCI SSC)

(1) The PCI SSC reserves the right to review the assessment report, all documents prepared by the Supplier in the course of the assessment as well as documents provided by the Client without obtaining any additional approval in advance. In its role as an accredited assessor, the Supplier is obliged by the PCI SSC to pass on the documents on request. The Client agrees to this procedure.

(2) The Supplier shall fundamentally not bear any costs for listings with payment brands, such as Visa or Mastercard, or with the PCI SSC.

Section D: Data Processing Agreement (DPA)

Commissioned data processing agreement according to Art. 28 GDPR

Agreement

between the

Controller – hereinafter referred to as the Client –

and

usd AG
Frankfurter Str. 233, Forum C1
63263 Neu-Isenburg, Germany

Processor – hereinafter referred to as the Supplier –

Preamble

(1) The Supplier processes personal data for the Client on behalf of the Client. The Client has selected the Supplier as a service provider within the scope of the due diligence requirements of Article 28 of the General Data Protection Regulation (GDPR). A prerequisite for the admissibility of commissioned processing is that the Client gives the Supplier the order in writing. According to the will of the Parties and in particular of the Client, this contract contains the written order for commissioned processing within the meaning of Art. 28 of the GDPR and regulates the rights and obligations of the Parties in connection with the data processing.

(2) Where the term "data processing" or "processing" (of data) is used in this Agreement, it is generally understood to mean the use of personal data. The use of personal data includes in particular the collection, storage, transmission, blocking, deletion as well as the anonymization, pseudonymization, encryption or other use of data.

1. Subject and duration of the contract

(1) The subject of the order is set out in the associated Service Agreement or the associated offer to which reference is made here (hereinafter referred to as Service Agreement).

(2) The duration of this contract (term) is the same as the term of the Service Agreement.

2. Specification of the order content

(1) The nature and purpose of the tasks of the Supplier is the potential processing of personal data in the context of consulting and certification projects as well as technical security and vulnerability analyses in accordance with the Service Agreement.

(2) The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another state that is a party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the Client and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

(3) The data can potentially belong to any category of data processed on the Client's systems. The Supplier cannot foresee in advance of the projects and analyses which information will be processed within the scope of the contract.

(4) All persons whose personal data is processed on the Client's systems can potentially be affected. The Supplier cannot foresee in advance of the projects and analyses which information will be processed within the scope of the contract.

3. Technical and organizational measures

(1) The Supplier shall document the implementation of the technical and organizational measures described and required prior to the award of the contract before processing commences, in particular with regard to the specific execution of the contract and shall hand them over to the Client for review. If accepted by the Client, the documented measures shall become the basis of the order. If a review/audit of the Client reveals a need for adjustment, this shall be implemented by mutual agreement.

(2) The Supplier shall ensure security in accordance with Art. 28 para. 3 lit. c and Art. 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 of the GDPR must be taken into account [details in Section E].

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Supplier is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

4. Rectification, restriction and erasure of data

(1) The Client is solely responsible for safeguarding the rights of data subjects.

(2) The Supplier may not rectify, erase or restrict the processing of data processed under the order on its own authority, but only in accordance with documented instructions from the Client. Insofar as a data subject contacts the Supplier directly in this regard, the Supplier shall forward this request to the Client without delay.

(3) As far as included in the scope of services, the erasure concept, right to be forgotten, rectification, data portability and access are to be ensured directly by the Supplier in accordance with documented instructions from the Client.

5. Quality assurance and other obligations of the Supplier

(1) In addition to complying with the provisions of this Agreement, the Supplier has statutory obligations under Articles 28 to 33 GDPR; in this respect, the Supplier shall in particular ensure compliance with the following requirements:

a) Written appointment of a data protection officer who carries out his or her duties in accordance with Art. 38 and 39 GDPR:

DEUDAT GmbH
Marcel Wetzel
Zehntenhofstraße 5b
65201 Wiesbaden, Germany
Phone: +49 611 950008-40
Email: kontakt@deudat.de

b) The maintenance of confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. In performing the work, the Supplier shall only use employees who are bound to confidentiality and who have been previously familiarized with the provisions on data protection relevant to them. The Supplier and any person subordinate to the Supplier who has access to personal data may process such data exclusively in accordance with the instructions of the Client, including the powers granted in this Agreement, unless they are legally obliged to process such data. The obligation of the employees shall be proven to the Client upon request.

c) The implementation of and compliance with all technical and organizational measures required for this Agreement in accordance with Art. 28 para. 3 sentence 2 lit. c and Art. 32 GDPR [details in Section E].

d) The Client and the Supplier shall, upon request, cooperate with the Supervisory Authority in the performance of its tasks.

e) Immediate information of the Client about control actions and measures of the supervisory authority, as far as they relate to this contract. This also applies if a competent authority investigates the Supplier in the context of administrative or criminal proceedings relating to the processing of personal data in the context of commissioned processing.

f) If the Client is itself subject to a supervisory authority inspection, administrative or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the processing of the order by the Supplier, the Supplier shall assist the Client to the best of its ability.

g) The Supplier shall regularly check the internal processes and the technical and organizational measures taken to ensure that the processing within its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the rights of the data subject are protected.

h) Verifiability of the technical and organizational measures taken vis-à-vis the Client within the scope of its control powers pursuant to Section 8 of this Agreement.

(2) The Supplier shall be obliged to support the Client in its duty to process requests from data subjects pursuant to Art. 12 to 23 GDPR. In particular, the Supplier shall ensure that the information required in this respect is provided to the Client without undue delay so that the Client can in particular fulfill its obligations under Article 12 para. 3 of the GDPR.

6. "Mobile Office" regulation

(1) The Supplier may allow its employees who are entrusted with the processing of personal data for the Client to process personal data in the Mobile Office.

(2) The Supplier shall ensure that compliance with the contractually agreed technical and organizational measures is also guaranteed in the Mobile Office of the Supplier´s employees.

(3) The Supplier shall in particular ensure that if personal data is processed in the Mobile Office, the storage locations are configured in such a way that local storage of data on IT

systems used in the Mobile Office is excluded. If this is not possible, the Supplier shall ensure that any data stored locally is encrypted and that other persons in the household do not have access to this data. For reasons of security, each employee shall also work in the Mobile Office on end devices provided by usd.

(4) The Supplier shall oblige its employees within the framework of a Mobile Office guideline to process personal data in compliance with data protection requirements.

7. Sub-contractual relations

(1) For the purposes of this provision, sub-contractual relationships are understood to be those services which are directly related to the provision of the main service. This does not include ancillary services which the Supplier uses, e.g. as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers or other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

However, the Supplier shall be obligated to enter into appropriate and legally compliant contractual agreements as well as control measures in order to ensure data protection and data security of the Client's data, also in the case of outsourced ancillary services.

(2) The use of subcontractors (additional sub-processors) is not envisaged in the provision of the agreed order processing.
Outsourcing to subcontractors or a subsequent change of the existing subcontractors shall be permissible provided that:

- the Supplier notifies the Client of such outsourcing to subcontractors in writing or in text form a reasonable time in advance, and
- the Client does not object to the planned outsourcing in writing or in text form to the Supplier by the time the data is transferred, and
- a contractual agreement in accordance with Art. 28 Para. 2 to 4 GDPR is used as the basis.

(3) The transfer of the Client's personal data to the subcontractor and the subcontractor's first activity are only permitted once all the conditions for subcontracting have been met.

(4) The Supplier shall ensure that the provisions agreed in this Agreement and, if applicable, any supplementary instructions of the Client also apply to the subcontractor.

(5) If the subcontractor provides the agreed service outside the EU / EEA, the Supplier shall ensure the admissibility under data protection law by taking appropriate measures. The same applies if service providers within the meaning of Paragraph 1 Sentence 2 are to be used.

(6) Any further outsourcing by the subcontractor requires the express information and consent of the Client (at least in text form); all contractual regulations in the contractual chain must also be imposed on the further subcontractor.

(7) The Supplier shall carry out regular checks of the subcontractors. These checks shall be documented and made available to the Client upon request.

8. Rights of control of the Client

(1) The Customer shall have the right to carry out inspections or to have them carried out by inspectors appointed on a case-by-case basis. The inspections must generally be announced in good time, at least 14 days in advance, unless an unannounced inspection appears necessary to avoid jeopardizing the purpose of the inspection.

(2) The Supplier shall ensure that the Client is able to verify that the Supplier complies with its obligations pursuant to Art. 28 GDPR. The Supplier undertakes to provide the Client on request with the necessary information and in particular to provide evidence of the implementation of the technical and organizational measures.

(3) Proof of such measures, which do not only concern the specific contract, can be provided by compliance with approved rules of conduct in accordance with Art. 40 GDPR, certification in accordance with an approved certification procedure in accordance with Art. 42 GDPR, current attestations, reports or report extracts from independent bodies (e.g. auditors, revision, own data protection officer, IT security department, data protection auditors, quality auditors) or by suitable certification by IT security or data protection audit (e.g. in accordance with BSI-Grundschutz).

(4) The Supplier may assert a claim for remuneration for enabling the Client to carry out checks. This shall also include compensation for the working time of personnel occupied by the Client. There shall be no remuneration entitlement if the checks are carried out on the basis of justified suspicion of a breach by the Supplier of regulations under data protection law or of the contractual agreements made and/or the instructions issued by the Client.

9. Notification of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations regarding the security of personal data set out in Articles 32 to 36 GDPR, notification obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, inter alia,

a) ensuring an adequate level of protection by technical and organizational measures which take into account the circumstances and purposes of the processing operation and the projected likelihood and seriousness of a possible infringement by security vulnerabilities and allow for the prompt detection of relevant events of infringement.

b) the obligation to notify the Client without undue delay of any infringement of data protection regulations or of the contractual agreements concluded and/or the instructions issued by the Client which has occurred in the course of the processing of data by the Supplier or other persons involved in the processing. The Supplier´s notification to the Client must in particular contain the information pursuant to Article 33 para 3. lit. a to d GDPR.

c) the obligation to assist the Client in its duty to inform the data subject and, in this context, to provide them with all relevant information without delay.

d) assisting the Client in its data protection impact assessment.

e) assisting the Client in prior consultations with the supervisory authority.

(2) For support services which are not included in the performance specifications, or which are not due to misconduct on the part of the Supplier, the Supplier may claim compensation.

10. Authority of the Client

(1) The Supplier shall process personal data exclusively within the scope of the agreements made and/or in compliance with any supplementary instructions issued by the Client. Excluded from this are legal regulations which may oblige the Supplier to process the data in another way. In such a case, the Supplier shall notify the Client of these legal requirements prior to processing, unless the law in question prohibits such notification due to an important public interest. The purpose, type and scope of data processing shall otherwise be governed exclusively by this Agreement and/or the Client's instructions. The Supplier is prohibited from processing data in any other way unless the Client has given its written consent.

(2) The Client shall confirm verbal instructions without delay (at least in text form).

The Supplier must inform the Client of the person(s) who are authorized to receive instructions from the Client.

Personnel of the Supplier who are authorized to receive instructions from the Client are:

Mr. Andreas Duchmann
Member of Executive Board
Phone: +49 6102 8631-0
Email: datenschutz@usd.de

Ms. Andrea Tubach
CEO
Phone: +49 6102 8631-0
Email: datenschutz@usd.de

In the event of a change or long-term unavailability of the contact person, the contract partner must be informed immediately in writing of the successor or the representative.

(3) The Supplier shall inform the Client without delay if it believes that an instruction violates data protection regulations. The Supplier shall be entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

11. Erasure and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the Client. Excluded from this are back-up copies, insofar as they are necessary to ensure proper data processing, as well as data which is required in order to comply with statutory storage obligations.

(2) Upon completion of the contractually agreed work or earlier upon request by the Client - at the latest upon termination of the Service Agreement - the Supplier shall hand over to the Client all documents, generated results of processing and use as well as data files that have come into its possession in connection with the contractual relationship or destroy them in accordance with data protection laws upon prior consent. The same applies to test and reject material. The protocol of the erasure is to be presented on request.

(3) Documentation which serves as proof of data processing in accordance with the order and in due form shall be kept by the Supplier beyond the end of the contract in accordance with the respective retention periods. It may hand them over to the Client at the end of the contract to be relieved of its burden.

12. Right of retention

The Parties agree that the defense of a right of retention by the Supplier in the sense of § 273 BGB (German Civil Code) with regard to the processed data and the associated data carriers is excluded.

13. Liability

The liability regulations according to Art. 82 GDPR apply.

14. Miscellaneous

(1) Should property of the Client that is in the possession of the Supplier be endangered by measures of third parties, for example by seizure or confiscation or by other events, the Supplier shall notify the Client immediately. The Supplier shall point out to the third parties that the responsibility and ownership of the data lies exclusively with the Client.

(2) Amendments and supplements to this supplementary agreement and all its constituent parts require a written agreement.

(3) Should one or more clauses of this Agreement be invalid, this shall not affect the validity of the remainder of the Agreement.

Section E: Technical and Organizational Measures (TOMs)

The general technical and organizational measures described below comply with Art. 32 para. 1 GDPR and Art. 25 para. 1 GDPR and are valid for all consulting services of the Supplier.

§ 1 Measures to ensure confidentiality

a) Physical access controls

- Access to the premises is only possible via designated entrances.
- Customers access the premises only via a designated entrance.
- Visitors are to be met by company staff and escorted to the place where the service is to be provided or accompanied to the company contact person. If confidential or sensitive areas are entered, the visitor is to be accompanied at all times.
- Securing the business premises of the Neu-Isenburg location by means of an alarm system with an associated security service.
- Access to the server room only via a 2-factor control system with personalized access control and restrictive access concept.
- Access to the server room for external persons only in the company of an authorized company employee.
- Access to housing provider with restrictive access concept, controlled access procedures, personalized access control and prior identification.
- Operation of usd server systems at housing provider in own, exclusive and locked server cabinets.
- Documentation of the key management.
- Established check-in/check-out process for employees.

b) Equipment access control

- Complexity requirements for passwords.
- Passwords used are encrypted according to the state of the art.
- Personalized access to data processing equipment.
- Password control/protection of all PCs.
- Blocking user accounts after multiple failed login attempts.
- A restrictive role and authorization concept has been implemented.
- Implementation of a firewall concept.
- Use of up-to-date SPAM and virus filters.
- Locking of the work computer after expiry of time with password query on reactivation.

c) Data access controls

- A restrictive role and authorization concept for access to personal data has been implemented.
- Regular review of the defined authorizations or access rights of the employees.

- Locking of the work computer after expiry of time period with password query on reactivation.
- Maintenance by external service providers only in the presence of the system administrator.
- System hardening and regular system updates via software updates and patches.
- Training and awareness-raising measures for staff.
- Logging of relevant system activities.

d) Separation controls

- Client separation.
- Role and authorization concept.

e) Pseudonymization

In a risk-oriented manner and in coordination with the Client, personal data can be processed pseudonymously in technical procedures, taking into account the integrity and the task at hand.

f) Encryption

- Data is transmitted exclusively in an encrypted form in accordance with the current state of the art.
- Output of encrypted mobile data carriers (USB sticks, mobile hard disks).
- Hard drive encryption on the laptops.
- Encryption of backups.

§ 2 Measures to ensure integrity

a) Data transfer controls

- Controlled destruction of data carriers in accordance with data protection regulations.
- Data is transmitted exclusively in an encrypted form in accordance with the current state of the art.
- Controlled transmission by the respective responsible person.
- Encryption of data carriers.
- A passing on of personal data takes place exclusively in the context of the customer relationship according to contractual regulations.
- Data is transmitted exclusively via defined interfaces.

b) Input controls

- Logging of relevant system activities.
- A restrictive role and authorization concept has been implemented.
- Event-related evaluation of logs.

§ 3 Measures to ensure availability and resilience

a) Availability controls

- Existence and implementation of a concept for carrying out regular data backups (backup concept).
- Implementation of a firewall concept.
- Use of up-to-date SPAM and virus filters.
- Use of an emergency power supply (UPS).
- Monitoring of critical network and server components.
- Guarantee of availability according to contractually agreed SLA.

b) Swift recoverability

Existence and implementation of a concept for the recovery of data and IT systems based on regular data backups and monitoring and recovery tests based on this (backup concept).

§ 4 Procedures for periodic review, assessment and evaluation

a) Data protection management

- Existing data protection organization, security organization and ISMS.
- Appointed Data Protection Officer.
- In the sense of a CIP (Continuous Improvement Process), all technical and organizational measures are regularly checked for their effectiveness and adapted to the current state of the art.

b) Incident response management

Defined incident response processes for receiving, assessing, handling, and documenting privacy and security incidents.

c) Privacy-friendly default settings

- The nature of the processing and the purpose of the processing of personal data shall be carried out exclusively in accordance with the Client's instructions and/or in accordance with the contractual agreements.
- Client separation.
- Role and authorization concept.
- Deletion of personal data in accordance with the contractual agreements.
- Only those personal data are processed which are necessary to fulfil the agreed purpose of the contract.

d) Order controls

- Documentation of careful selection and control of contractors.
- Formal order placement.
- Conclusion of supplementary agreements for processing in accordance with Art. 28 GDPR.
- Obligation of employees (also of service providers with potential access to personal data) to maintain the confidentiality of personal data in accordance with GDPR and, if applicable, § 3 TDDDG.
- Processing, use and deletion of data shall only take place in accordance with the contractual provisions between the Client and the Supplier