more security. usd

General Terms and Conditions for usd AG Security Platforms

Status: 13 December 2023

more security.

General Terms of Use for the Security Platforms of usd AG (Status: 13/12/2023)

Part A: General Part

Contracts with usd AG (hereinafter referred to as "usd" or "Supplier") in the context of services via the usd Security Platforms shall be concluded and performed exclusively in accordance with these General Terms of Use. Any conflicting conditions of the Client shall not be valid if and as long as they have not been accepted in writing by the Supplier.

§ 1 Subject matter of the contract; scope of application

(1) usd (for provider data see: https://www.usd.de/en/legal-notice/) is the Supplier of the following online portals (hereinafter referred to as usd Platforms):

1. usd PCI Scanning Platform, https://my-pci.usd.de
   (hereinafter referred to as Scanning Platform)
2. usd Security Awareness Platform, https://my-awareness.usd.de
   (hereinafter referred to as Awareness Platform)

(2) Within usd's Platforms, usd provides on-demand, digital services.

(3) usd offers access to and use of the Platforms to companies (hereinafter referred to as Clients) and their responsibly acting internal and external employees as well as, if applicable, third-party partners (hereinafter referred to as Users).

(4) These General Terms of Use (hereinafter referred to as GTU) shall apply to all Clients and Users of the usd Platforms with the first access to the public and non-public contents and Internet services provided on the usd Platforms.

(5) Counter-confirmations of the Clients and Users with reference to their own terms and conditions of business and/or purchase are hereby rejected. Individual agreements remain unaffected by this.

(6) The Clients and Users are entitled to use the services and information provided on the usd Platforms in accordance with the following provisions.

(7) This general Part A of the GTU is supplemented by the Data Processing Agreement (Part B) and the Technical and Organizational Measures pursuant to the GDPR (Part C) in their respective current version.

§ 2 Services; fees; prices

(1) The usd Platforms enable Clients and Users to retrieve information from the restricted areas of the usd Platforms, to exchange information, messages, comments and documents and to order services after registration and after approval by the Supplier pursuant to §3.

(2) The services offered on the Platforms consist of, but are not limited to:

(2.1) Provision of a scanning Platform for security audits and supplementary services in accordance with PCI DSS:

- The Supplier shall provide its services irrespective of whether Clients are obliged to achieve PCI DSS certification in accordance with PCI DSS.

- Upon admission according to §3, the Client can order individual services on the Platform according to the product description and schedule their execution depending on the available capacities and time restrictions of the Supplier.

- If the Client is seeking certification in accordance with PCI DSS, the type, scope and frequency of the certification measures to be carried out will depend on the Client's classification and rating.

- With or after its registration, the Client shall define all data required for classification and categorization according to PCI DSS on the Platform or shall transmit such data to the Supplier for processing and use for a specific purpose.

- The applications and services provided through access to the Platform consist of, but are not limited to:

  - PCI DSS compliant IT security scans (hereinafter referred to as ASV scans) of the customer's infrastructure accessible via the Internet, including reporting
  - Online Self-Assessment Questionnaires
  - Provision of reports, certificates and seals
  - Support services rendered by the PCI Competence Center of usd
  - Consultancy, service and support services for customers in accordance with a separate agreement with the Supplier

- Within the scope of the ASV scans offered, Clients check their IT infrastructure accessible via the Internet for the requirements specified by the PCI DSS. For this purpose, Clients use the applications provided on the Platform and the supplementary services offered by the Supplier.

- Results and conclusions of the ASV scans and the complementary services are made available to the Client by means of a report that can be downloaded from the Platform.

- Provided that the Client demonstrably complies with the PCI DSS requirements as specified by the Client on the platform, the Supplier shall provide a PCI DSS certificate as well as a seal. The PCI DSS certificate and the seal may only be used by the Client for the duration of the validation period indicated in each case.

(2.2) Provision of an Awareness Platform for training and sensitization of employees:

- With its admission according to §3, the Client can order individual services on the Platform according to the product description and schedule their execution depending on the available capacities and time restrictions of the Supplier.

- The usd Awareness Platform offers Clients and Users access to web applications, services and content through which Users can train and test their knowledge, risk awareness and application strategies in the area of technical and non-technical protection of trade and business secrets.

- The applications and services provided through access to the Platform consist of, but are not limited to:

  - Access to the Awareness Platform including options to place orders
  - Continuous updating of the contents
  - Language selection German and English
  - Order of paid training and test units
  - If available, knowledge check of the Users on the learning contents imparted
  - Monitoring of the implemented trainings including reporting function
  - Automatically notify Users by email when a course needs to be renewed
  - Possibility to upload in-house security policies, including read confirmation of Users
  - Support services provided by the supplier for a fee
  - Consultancy, service and support services for Clients and Users according to a separate agreement with the Supplier

(3) Insofar as the digital offers are not provided free of charge by the Supplier, the costs and billing modalities for the individual services can be found in the current price information on the respective Platform or by contacting the sales department of usd AG. For the determination of the price of the individual service is the current price at the time of the conclusion of the contract with the (order) shall be decisive for the price determination of the individual service. In the event of a contract extension, the price information current at the time of the contract extension shall be decisive, provided that the Client was informed separately of the changed prices by the Supplier at least 14 days prior to the corresponding contract extension and the Client continues to use the services without objection. The Client shall be informed separately of the right to object and the legal consequences of silence in the event of a price change.

§ 3 Conditions of use; registration; admission

(1) The prerequisite for the use of the usd Platforms and the use of the services offered is the conclusion of a contract of use. For this purpose, the user accepts a contract offer from the Supplier through a user authorized to represent the Supplier by sending the

registration form provided by him with the minimum details online to the Supplier and acknowledging the validity of these GTU by mouse clicking. Only taxable entrepreneurs / companies, associations, societies, public corporations, institutions and foundations as well as their downstream authorities and organizational units are entitled to register as Clients, provided that they act in the exercise of their commercial or self-employed professional or service activity when using the Internet services offered on the Platforms. Internal and external employees of Clients who make use of the digital services of the Platforms in their official and employment relationship for exclusively professional or official purposes are entitled to register as Users.

In individual cases a contract can be concluded with the Supplier in writing or in text form for the use of the usd Platforms. In this case, the Client orders the use of the usd Platforms in writing or in text form and confirms the validity of these GTU with his signature.

(2) The registration enables Users acting on behalf of the Client to access exclusive services and contents in the restricted areas of the usd Platforms. Access to these contents is subject to the respective acceptance of the GTU by the Client and the User and the respective approval by the Supplier. In all cases, the right to verify the plausibility of company data provided by the Client is reserved.

(3) There shall be no entitlement to use the usd Platforms and to be granted the permission of use. The possibility of use and/or the admission to individual Platforms shall cease to exist if the prerequisites provided for this cease. Within the framework of proper considerations, the Supplier may restrict or exclude the possibility of use at any time and without stating reasons.

§ 4 Rights and obligations of Clients and Users

(1) Clients and Users are entitled to use the services of the usd Platforms within the scope of the access possibilities granted to them by the Supplier properly and on their own responsibility. They are obliged to observe all security regulations of the Supplier and to refrain from illegal actions and misuse of the access possibilities to the Internet services provided on the usd Platforms.

(2) Clients and Users are obliged to continuously check and update their company data and user master data for factual accuracy. Posted information, content, news and messages as well as files may not contain any content that [or their intended contract] violates legal or official regulations and/or the rights of third parties and/or morality.

(3) Clients and Users are entitled vis-à-vis the Supplier - and are required to do so before legal proceedings are initiated against the Supplier - to demand the blocking or removal

of posted information, content, news and messages as well as files whose factual correctness is doubtful, violates legal or official regulations or offends common decency and infringes the rights of the Client or their Users or third parties (notice-and-take-down procedure).

(4) If a claim is made against the Supplier by a third party or a Client or User on the basis of one of the violations mentioned in sections §4(1) to §4(2), the Client or User responsible for the violation undertakes to indemnify the Supplier against any claims. The obligation to indemnify refers to all expenses necessarily incurred by the Supplier as a result of a claim by a third party. The Supplier expressly reserves the right to claim further damages.

(5) The Client shall hold its Users operating on the Platforms - irrespective of whether an independent contract of use is concluded with the Users - to the corresponding compliance with its obligations from these GTU.

(6) The following special regulations apply to the use of the scanning Platform:

(6.1) Within the scope of his registration and when entering or transmitting information relevant to certification, the Client is obliged to provide truthful information and to continuously check or update this information for its factual correctness.

(6.2) The Client is only obliged to scan IT systems if he is authorized to do so. As a rule, the authorization shall exist if the Client is the owner of the scan components (IP addresses or domains) and either the owner of the IT systems associated with the scan components or has obtained written permission from the owner of the IT systems to perform the ASV scans.

(6.3) If the Client is seeking a certification according to PCI DSS, it is obligated to specify all scan components (IP addresses or domains as well as VHOSTS, if available) that must be checked with an ASV scan within the scope of PCI DSS compliance. These are, for example, web servers, application servers, routers, firewalls and load balancers.

(6.4) For the period of the ASV Scan, the Client shall be obliged to configure its intrusion detection systems or intrusion prevention systems (hereinafter referred to as IDS/IPS) in such a way that the IT systems of the Supplier executing the ASV Scan have unrestricted access to the Client‘s components that are to be scanned.

(6.5) If a claim is made against the Supplier by a third party or a customer on the basis of one of the infringements mentioned in §4 clauses (6.1), (6.2), (6.3) and (6.4), the Client responsible for the infringement undertakes to indemnify the Supplier against any claims. The obligation to indemnify refers to all expenses necessarily incurred by the Supplier as a result of the claim by a third party. The Supplier expressly reserves the right to claim further damages.

§ 5 Rights and obligations of the Supplier

(1) The Supplier undertakes to check its own editorial contributions and other services for topicality, factual correctness, completeness and security to the best of its ability.

(2) When prompted and at its discretion, the Supplier checks whether Clients and their Users observe the general laws and the contractual and regulatory framework when using the services offered on the Platforms. The Supplier follows up on plausible complaints from Clients and Users about rule violations and notifications of any illegal content on the Platforms and decides what measures are to be taken in the event of rule violations.

(3) The Supplier reserves the right to block or remove information, content, news and messages as well as files whose factual correctness is doubtful, which violate legal or official regulations, the rights of third parties, morality or which are infected by viruses, after obtaining knowledge and depending on the severity of the violation in question, even without prior consultation and announcement (notice-and-take-down procedure). Claims derived from the removal of such information or files cannot be asserted against the Supplier.

(4) If the Client or its Users violate an obligation pursuant to §4 and §5, the Supplier shall be entitled to delete the corresponding data or to withdraw access to the usd Platforms in whole or in part. The same shall apply in the event of other serious breaches of contract by the Client or its Users as well as on the basis of justified complaints by Clients and their Users in accordance with the notice-and-take-down procedure.

(5) The content and technical design, in particular the form and content of the Platforms are exclusively at the discretion of the Supplier. In this respect, the Supplier reserves the right to discontinue, restrict, expand, supplement or improve all services offered free of charge at any time.

(6) The Supplier is entitled to check all information provided by the user for its factual and actual correctness and, if necessary, to obtain separate written assurances from the Client as well as information from third parties.

In the event of serious doubts about the accuracy of the information provided by the Client, the Supplier is entitled to withdraw access to the Platform in whole or in part and to terminate the contract extraordinarily. The same applies in the event of violations by the Client of its obligations pursuant to §4 clauses (6.1), (6.2), (6.3) and (6.4) and in the event of other serious breaches of contract by the Customer. The right of the Supplier to claim damages remains unaffected.

(7) In the context of the scanning Platform, the following special rules apply:

(7.1) Within the scope of the certification procedure, the assessment of whether the actual state of the IT system to be checked corresponds to the required target state is the sole responsibility of the Supplier. In the event of a negative deviation of the actual state from the target state, the user shall have no claim to the granting of the certificate.

(7.2) The Supplier shall allocate the times at which ASV scans are performed according to the chronological order of receipt of the appointments made by the Client, taking into account the Supplier's available capacities.

The Client has no claim to the execution of certification measures at a certain point in time, unless the Supplier has free capacities available at that time.

§ 6 System failure: availability of services and refund of counter performance

(1) The Platforms and the services offered via these Platforms are provided without any guarantee of availability.

(2) In the case of service offers subject to a charge, in the event of non-availability of the service to a considerable extent (> 2 % non-availability), the pro rata consideration shall be made, insofar as the service cannot be made up for in a manner that is reasonable for the Client.

(3) Availability is calculated on the basis of the time allotted to the respective calendar month during the term of the contract, minus scheduled maintenance and downtimes that are beyond the control of the Supplier (force majeure, fault of third parties, etc.).

(4) Scheduled maintenance work will preferably take place outside core working hours (Monday to Friday 08:00 to 18:00 CET).

(5) During maintenance work, the aforementioned services may not be available at short notice. Corresponding services will be provided by the Supplier in consultation with the Client and the Users at the next possible time, provided this is reasonable for the Client.

(6) The Supplier operates the Platforms via an internet connection with at least 2 MBit/s data rate. The response time for calling up a single web page is below 2 seconds on average. The Supplier logs the utilization of the connection and the response times.

(7) Access to the Platforms is exclusively authenticated, i.e. after entering a user ID and password. The use of the offered functionality requires workstation computers on the

part of the Users that always meet the current requirements for Internet browsers and additional add-ons.

§ 7 Term of contract; termination

(1) The user contract underlying these GTU is concluded for a period of one year. Both the Client and the Supplier may terminate this contract at any time with one month's notice to the end of the year.

(2) Unterminated user contracts are automatically extended by a further 12 months after the expiry of one year.

(3) The right of the Supplier to withdraw the Client's access to the Platforms in whole or in part pursuant to Section 5.4 shall remain unaffected.

(4) The contractual term of any chargeable services and, if applicable, the right to ordinary termination of chargeable services are regulated below for the Platforms.

- Awareness Platform: (Paid) contingents for online training have a limited contract term of 12 months from the date of provision. After expiry of the contract period, unused training quotas expire.
- Scanning Platform: (paid) contingents for ASV scans have a limited contract term: one-time scans are available for 60 days from the date of provision and annual packages are available for 15 months from the date of provision. After expiry of the contract period, unused, provided contingents expire.
- Other deviating regulations can be concluded in separate individual agreements.

(5) Each party has the right to terminate this contract for good cause without notice. An important reason for the Supplier is in particular:

- the serious breach by the Client or its Users of the provisions of these GTU;
- the tortious act of the Client or its Users or the attempt to commit such an act;
- the opening of insolvency proceedings against the assets of an Client or the rejection of the corresponding application for the opening of such proceedings for lack of assets.

(6) Any termination must be made either in writing (letter, fax) or in text form (email) to the Supplier:

- Awareness Platform Competence Center: awareness@usd.de
- Scanning Platform Competence Center: pci@usd.de
- Alternatively to usd: contact@usd.de

§ 8 Liability; exclusions of liability; limitation of liability

(1) The Supplier is liable for damages suffered by the Client only insofar as these are caused by intentional or grossly negligent acts or by the violation of essential contractual obligations. In the event of a simple negligent breach of essential contractual obligations, the Supplier shall only be liable to the extent of the foreseeable, contract-typical, direct average damage. In total, liability is limited to a maximum of 25,000.00 Euros (in words: twenty-five thousand Euros) per liability case. In all other respects liability is excluded. Essential contractual obligations are those whose fulfilment is necessary to achieve the objective of the contract.

(2) Insofar as the Platforms with links provide access to other websites, the Supplier is not responsible for the third-party content contained therein. The Supplier does not adopt the third-party content as its own. Liability for third-party content is excluded. If the Supplier becomes aware of illegal content on external websites, the Supplier will immediately remove the link to these.

(3) The Supplier is not liable for the factual correctness of data as well as for the virus-free nature of files that are posted on the Platforms by Clients and their Users. Reference is made to the possibility of initiating a notice-and-take-down procedure (Sections 4.3, 5.4).

(4) The Supplier shall not be liable for any damages to the Clients and their Users resulting from following or not following recommendations, tips, best practices or the use of templates.

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

(6) The above limitations of liability and exclusions do not apply to claims of Clients and their Users based on injury to life, limb, health and claims based on the negligent breach of essential contractual obligations. Also excluded from the exclusion of liability is liability arising from product liability and for damages based on an intentional or grossly negligent breach of duty by the Supplier, its legal representatives or vicarious agents.

(7) Insofar as the Supplier provides services to Clients outside these GTU or on the basis of an individual offer, the liability of the contractual partners in this respect shall be regulated in the contract/offer concluded separately for this purpose.

(8) Furthermore, the following special regulations apply in the context of the Scanning Platform:

(8.1) The Supplier warrants and ensures that the Security Scanner provided as an application complies with the Payment Card Industry Data Security Standard specified by the credit card organizations. This is necessary in order to certify the analyzed IT system that

complies with the standard and at the same time ensures that the scanning only has a minimal impact on the analyzed IT system. There is no further obligation or liability on the part of the Supplier. The Supplier shall not be liable for damages due to impairment of the integrity and/or availability of the analyzed IT systems in the case of proper ASV scans that comply with the Payment Card Industry Data Security Standard.

(9) The above limitations of liability and exclusions do not apply to claims by Clients arising from product liability. Furthermore, the limitations of liability do not apply to bodily injury and health damage of Users attributable to the Supplier.

§ 9 Data protection

(1) The Supplier has taken comprehensive technical and organizational precautions to ensure that data is treated confidentially and exclusively for the intended purpose. However, the misuse by illegal actions of third parties cannot be completely excluded.

(2) The Supplier undertakes to use the data stored during registration and use solely for its own purposes and for the purposes of project work as well as for the purposes of initiating or processing contracts initiated or concluded via the Platforms and not to pass it on to outside third parties unless there is an obligation to do so imposed by the authorities or the user has given its express consent. This regulation on the handling of data is substantiated and supplemented by the data protection notice.

(3) The Supplier undertakes to oblige its Users who are entrusted with the administration and/or operation of the Platforms to strictly comply with data protection regulations.

(4) When registering companies as Clients, the Supplier is entitled to retrieve creditworthiness information based on mathematical-statistical procedures from so-called credit agencies and to receive updated information for the purpose of its own credit check, if necessary.

(5) The Supplier is entitled to observe, record and evaluate the usage behavior of Clients and Users in order to ensure proper and high-performance Platform operation and to improve its offers in a targeted manner (target group-specific marketing) as well as to combat misuse. Clause (2) applies accordingly to such data.

(6) Insofar as the Client places personal data of a third party on the Platforms, it assures that it is authorized to do so. The Client is obliged to inform the third party of the transfer of any personal data.

(7) Clients and Users are entitled to use the personal data provided to them by the Supplier or other Clients exclusively for the purpose of initiating and processing contracts as well

as for project work. The Client obligates its Users acting on the Platforms in accordance with his obligations under these GTU.

§ 10 Tax regulations

(1) The remuneration agreed with the Supplier shall be net prices, which are to be paid plus the applicable statutory national value added tax.

(2) The principal shall be obliged to inform usd of the invoice address and the respective place of performance when placing the order. If this place of performance is considered to be a permanent establishment of the principal, it shall be taken into account as the place of performance and the correct tax regulation for this place shall be applied when issuing the invoice. If the customer is not informed separately in this respect, usd shall assume that the address stated in the offer is to be assumed both as the invoice address and as the place of performance of the service.

(3) Irrespective of this, the customer shall be obliged, in the case of one or more places of performance outside of Germany, to provide usd with the following information when placing the order:

1. Place of performance outside Germany but within the EU:

Indication of the valid value added tax identification number (VAT number) of the places of supply communicated to usd in accordance with paragraph 2.

2. Place of performance outside Germany and outside the EU:

Presentation of a "certificate of registration as a taxable person (entrepreneur)" issued by the competent foreign tax office of the places of supply communicated to usd in accordance with paragraph 2.

(4) If the place of performance is outside of Germany, usd shall not show value added tax when issuing the invoice, provided that the principal submits to usd before the first issuing of the invoice the necessary information or documents listed under paragraph 3 a) and b) for the consideration of the value added tax in due time. If the required evidence is not provided in due time, usd shall be entitled to issue the invoice showing the statutory value added tax applicable at that time (according to the current legal situation 19 %) and to pay it to the competent German tax office.

(5) Invoices shall be issued in accordance with the German Value Added Tax Act (UStG) and, where applicable, the European VAT Directive. Accordingly, the provision of another service to an entrepreneur resident in a third country is not taxable in Germany. This has the consequence that the invoice is issued without showing VAT (net).

It is agreed that any taxes and duties that may be due under laws other than German laws are owed by the recipient of the service (economically) and that the recipient is responsible for a proper declaration to the local tax authorities. This Agreement includes all types of taxes, in particular sales tax and all withholding taxes. Alternatively, the price for the services rendered shall be increased by these taxes and duties. The service Supplier shall be entitled to claim these taxes and duties from the service recipient even after the conclusion of the exchange of services.

§ 11 Copyrights and property rights

(1) The Supplier is the owner of all property rights, protection rights and copyrights with regard to its own contributions and other own content, unless otherwise indicated.

(2) The uploading Client retains ownership, property rights and copyrights to contributions and content uploaded by the Client on the Platforms for the purpose of retrieval by the Supplier or other Clients. Insofar as necessary, the uploading Client grants the Supplier a simple right of use for the respective intended purpose, without the Supplier thereby making the third-party content its own.

(3) The Client undertakes neither to remove nor to make unrecognizable the copyright notices or other references of the Supplier or other Clients to such rights contained on the Platforms.

§ 12 Supplementary information in electronic business transactions according to § 312 i BGB in conjunction with Article 246 c EGBGB

(1) In essence, the rules of these GTU inform the user about all mandatory information in electronic business transactions in accordance with § 312 i BGB in conjunction with Article 246 c EGBGB, so that only the following additions are required:

(2) Supplier identity:

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

Power of representation:
Executive Board: Andreas Duchmann, Matthias Göhring, Christopher Kristes, Andrea Tubach, Manfred Tubach (CEO)

Chairman Supervisory Board:
Dr. Dietmar Kirchner

Commercial Register:
County Court Offenbach am Main
HRB 34667

VAT ID:
DE163774242

Contact:
Phone: +49 6102 8631-0
Fax: +49 6102 8631-88
Email: contact@usd.de

(3) The essential features of the services offered as well as the period of validity of time-limited offers can be found in the individual product and/or service descriptions on the Supplier's Platforms.

(4) The language available for the conclusion of the contract is exclusively German and English.

(5) The various ways of concluding the contract are described in § 3 of these GTU.

(6) The User can identify any input errors when submitting his order during the final order submission and correct them at any time using the delete and change function before sending the order.

(7) The prices stated by the Supplier are net final prices plus legally valid taxes within the Federal Republic of Germany.

(8) The Client/User may submit any complaints to the Supplier at any time by letter, fax or e-mail or by telephone during business hours. The Supplier shall contact the User within a reasonable period of time.

(9) Liability and warranty shall be governed by the relevant provisions of these GTU; otherwise by the statutory provisions.

(10) The data required for the processing of the contract between the Client and the Supplier are stored by the Supplier. After leaving the order level, the order remains accessible to the Client /User on the Internet. Section A9 of these General Terms of Use and the provisions of our data protection notice (https://www.usd.de/en/privacy-protection/) apply.

(11) The Client/User can print out this information, the General Terms of Use, the data protection notice and all other information on this website or save it in reproducible form as follows: The respective page can be printed with the browser by selecting the "Print" function in the main menu of the browser. The respective page can be saved by the user selecting the function "Save as" in the main menu of his browser. In addition, all

contractual provisions are saved by us. We will also be happy to send you the contractual provisions by email on request.

(12) We are not subject to any special codes of conduct not mentioned above.

§ 13 General

(1) The law of the Federal Republic of Germany shall apply exclusively to the exclusion of the reference standards of private international law (IPR) and the United Nations Convention on Contracts for the International Sale of Goods (CISG). The usd Platforms take into account the legal requirements of the Federal Republic of Germany. The Supplier assumes no responsibility that the usd Platforms, their services, information and/or documentation may also be accessed or downloaded at locations outside the Federal Republic of Germany. If Clients/Users access the usd Platforms from locations outside the Federal Republic of Germany, the Client/User shall be solely responsible for compliance with the relevant provisions of the law of the respective country. Access to the usd Platforms, their services, information and/or documentation from countries in which such access may be illegal is not permitted.

(2) The exclusive place of jurisdiction is Frankfurt am Main in the Federal Republic of Germany, insofar as the Client is a merchant or a legally capable association, society, public corporation, institution or foundation. In addition, the Supplier is also entitled to take legal action at the general place of jurisdiction of the Client or User.

(3) In case of doubt, the German text of these GTU and its components shall take precedence over translations into other languages.

(4) The invalidity of one or more provisions of this contract shall not affect the validity of the remainder of this contract.

(5) The supplementary components of these GTU can all be accessed in the public area of the Platforms.

(6) These GTU supersede and replace all previous GTU and/or GTU. Further changes to these GTU will be communicated to the user by the Supplier electronically (e.g. email, pop-up window, interstitial, etc.) before further use of the services, pop-up window, interstitial, etc.). If the Client does not object to such changes within 14 days of receipt of the notification, the changes shall be deemed to be agreed if the Client continues to use the Supplier's services provided at www.usd.de. The right of objection and the right of the Client to withdraw from the contract shall be excluded. The Client shall be informed separately of the right to object and the legal consequences of silence in the event of an amendment to these GTU.

(7) The GTU correspond to the above-mentioned status. We will inform you about future changes and send you updated versions. For this purpose, we will contact you via the e-mail address stored in your account and use a mailing tool with whose operator we have concluded a contract for order processing with regard to data protection. Your data will be deleted from the mailing tool after notification, at the latest after four weeks.

Part B: 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, House 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 mandate 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. A 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 results from 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) Nature and purpose of the tasks of the Supplier is the potential processing of personal data in the context of the provision of a scanning Platform for security assessments and complementary services in accordance with PCI DSS or the provision of an Awareness Platform for employee training and awareness measures.

(2) The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of 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 ff GDPR are met.

(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/assessment 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 Part C].

(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: usd@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 Art. 28 para. 3 sentence 2 lit. c and Art. 32 GDPR [details in Part C].

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 shall also apply where a competent authority investigates, in the context of administrative or criminal proceedings, the processing of personal data relating to the processing of the contract at the Supplier.

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 with the Supplier, the Supplier shall assist the Client to the best of its ability.

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

h) Verifiability of the technical and organizational measures taken vis-à-vis the Client within the scope of its control powers pursuant to Clause 7 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.

7. Subcontracting relationships

(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 Supplier may only engage existing subcontractors (further processors) with the prior express consent of the Client.

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. 2-4 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) 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.

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

(6) The following special regulations apply to the use of the scanning Platform:

The Client agrees to the engagement of the following subcontractor under the condition of a contractual agreement in accordance with Article 28 (2-4) of the GDPR:

Company Subcontractor	Address/Country	Service
Qualys Inc.	919 E Hillsdale Blvd, 4th Floor Foster City, CA 94404 USA	Qualys supports the provision of ASV scans

8. Control rights of the Client

(1) The Client has the right to carry out inspections in consultation with the Supplier or to have them carried out by inspectors to be appointed in individual cases. The Client has the right to verify the Supplier's compliance with this agreement in its business operations by means of spot checks, which must be notified in good time, at least 14 days in advance.

(2) The Supplier shall ensure that the Client is able to verify that the Client complies with the obligations of the Supplier 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 the personnel employed by the Supplier. 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 breach by security breaches and allow for the prompt detection of relevant breach events.

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

In the event of a change or longer-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. Deletion 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 deletion 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.

Part C: Technical and Organizational Measures (TOMs)

The general technical and organizational measures described below comply with Art. 32 (1) GDPR and Art. 25 (1) GDPR and apply to all consulting services provided by 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.
- Non-company personnel are received by company personnel and always accompanied through the premises.
- 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 controls

- 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 commissioned data 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, § 88 TKG.
- Processing, use and deletion of data shall only take place in accordance with the contractual provisions between the Client and the Supplier.