General Terms and Conditions / Allgemeine Geschäftsbedingungen

As of March 2025

MindBytes GmbH | Probststraße 15 | 70567 Stuttgart
hallo@mind-bytes.de | +49 711 20709567

Geschäftsführung: Christian Stehle, Nina Wagner, Simon Holl
Amtsgericht Stuttgart | HRB 790784 | USt-IdNr. DE363069855
Volksbank Alb eG, IBAN DE04 6309 1300 0513 9800 16

1 CONTENTS

The English version of this document is provided for ease of understanding. The legally binding version is the German version.

Die englische Version dieses Dokumentes wird der einfacheren Verständlichkeit halber zur Verfügung gestellt. Die rechtlich bindende Version ist die deutsche.

2 General Terms and Conditions

These General Terms and Conditions (“GTC”) shall apply to all services provided by MindBytes GmbH ("Contractor") to the customer ("Customer"). Together with an offer of Contractor signed by Customer for services to be provided for Customer, the GTC form the basis of the contract between the parties (“Parties”).

2.1 Terms Used

- „Office hours" are Monday to Friday (with the exception of public holidays at Contractor's registered office) between 8 AM and 6 PM.
- In the business relationship, "Infrastructure" refers to everything affected by Contractor's services for Customer, e.g. IT systems (and parts thereof) and services ("IT Infrastructure"), web applications, but also non-technical infrastructure such as office buildings or rooms, data centers and the server space contained therein.
- A "Penetration Test" is a controlled attempt to penetrate a computer or network system from the outside in order to detect and localize vulnerabilities in the affected systems. This attempt involves techniques that would also be used in a real attack on the system. Identifying the vulnerabilities enables them to be corrected before they are exploited by a real attack and third parties can gain unauthorized access to the system.
- "Red Team" is a group of Contractor’s employees whose task is to improve the effectiveness of Customer’s safety management by acting as an opponent and trying to identify security gaps.
- „Zero-Day Vulnerabilities" are vulnerabilities for which no generally available patches or countermeasures exist at the time of their discovery, and which are therefore or for other reasons classified as particularly dangerous. In this contractual relationship, a "Critical Zero-Day Vulnerability" is a Zero-Day Vulnerability that can only be remedied by the manufacturer of the affected software (e.g. by a so-called "patch"), and the discovery of which would enable any attacker to compromise the security of third parties, e.g. if the vulnerability is discovered in a cloud service (also called software/platform/other "as a service").

2.2 Subject of Contract

2.2.1 Offers

- Contractor shall be bound by its offers for 30 days from the date of issue, unless otherwise stated in the respective offer.

2.2.2 Subject of Performance

- Contractor's services for Customer are based on the information provided by Customer regarding the infrastructure. It is therefore critical for the effectiveness of the services that Customer informs Contractor of the infrastructure to be tested (cp. section 2.4.1).
- In order to fulfill its services in accordance with the contract, Contractor shall owe serious efforts and at least market-standard quality in the fulfillment, but not the production of a work or the achievement of an objective intended by Customer with Contractor's services.
- Depending on the specifications in the offer, Contractor shall carry out Penetration Tests in Customer's Infrastructure and/or provide Red Team services. In both cases, the discovery of vulnerabilities is the objective of Contractor's services. Neither is the elimination of vulnerabilities subject of Contractor's services as is any kind of hosting, incident response or ongoing monitoring of Customer's Infrastructure.
- Customer gives Contractor its express consent to the measures necessary for the provision of Contractor's services, in particular to any associated access to and procurement of data, possibly by overcoming any access security of the systems specified by Customer and/or from a non-public data transmission and/or from the electromagnetic radiation of a data processing system (§ 202 ff. StGB, German Criminal Code). Customer also expressly agrees that data may be altered or deleted during the provision of the services (§ 303a StGB).Changes to Scope of Services (Change Requests)
- If Customer requests changes to agreed services ("Change Request"), Contractor shall examine the costs and feasibility arising from the Change Request in return for payment at the agreed rates and inform Customer as soon as possible of the financial and time frame for the change. Unless otherwise agreed, Contractor shall invoice the expenses for said checks at the agreed rates.
- In order to clarify the consequences of a change request, Customer may request the interruption of the provision of services if it assures Contractor, at the latest at the time of the respective request for interruption, that it will remunerate the downtimes and the possibly more costly resumption of project implementation due to the interruption. Agreed performance deadlines and schedules shall be extended by the time of the downtime and the possibly more costly resumption.
- Change requests must be made in text form to be effective and must be accepted by both parties. If the parties are unable to agree on a change request, the originally agreed

services shall continue to be the subject matter of the contract, taking into account the delays caused by the change request.

2.2.3 Notification Channel When Vulnerabilities Are Discovered

- Contractor shall provide Customer with information on findings made during the provision of its services electronically in encrypted form. The access data required for opening (e.g. password) shall be transmitted via a second channel (e.g. Signal Messenger or SMS).

2.3 Obligations of Contractor

- Contractor must inform Customer immediately in the following cases:
    - Upon gaining knowledge of damage to its infrastructure or if the occurrence of such damage is foreseeable;
    - If vulnerabilities are identified that Contractor classifies as critical at its own discretion (based on the current version of the Common Vulnerability Scoring System).
- When providing its services, Contractor shall only deploy appropriately qualified personnel who are subject to at least the same confidentiality obligations as Contractor has towards Customer.
- Contractor shall retain all information obtained in the course of providing its services to Customer (e.g. on the identification of vulnerabilities and infrastructure development) for 3 (three) years after the end of the contractual services.

2.4 Obligations of Customer

2.4.1 Affected Infrastructure

- Customer guarantees that it is authorized to commission Contractor to perform the contractual services.
- Customer shall define for Contractor the Infrastructure affected by its services as early as possible, but no later than 3 working days before the start of its services and, if applicable, also name parts of the Infrastructure that Contractor may not actively test for vulnerabilities (e.g. due to secrecy protection or inviolability of system parts operated by third parties that do not permit Contractor's services). By naming the Infrastructure affected by Penetration Tests, Customer grants Contractor permission to take the agreed measures (permission to attack).
- Prior to the provision of services by Contractor, Customer must take all security measures that may be necessary in order to be able to restore systems and data affected by Contractor's services to their original state (e.g. via backups) in the event of damage (e.g. data loss) following a service provided by Contractor.

- Customer is aware that, despite comprehensive precautionary measures taken by Contractor in the course of the provision of its services, damage to existing systems and data may occur, particularly as a result of Penetration Tests. Such damage may be so irreversible that it can only be remedied by restoring the systems from backups and, in the worst case, by extensive reworking on Customer's end.
- Customer must inform Contractor immediately if it becomes aware that an action by Contractor has led to damage to the Infrastructure.

2.4.2 Participation

- Customer must support Contractor in the provision of its services for Customer to the extent necessary. Depending on the agreement, this may include
    - Coordination/agreement of deployment and/or service dates;
    - Provision of information, material, out-of-jail cards, etc.;
    - Providing an appropriate working environment for on-site appointments with Customer;
    - Granting of access and/or access to infrastructure and Internet access;
- Customer shall inform internal entities (e.g. employees, superiors, employee representatives) and third parties affected by Contractor's services in due time before the services are provided.
- If, to the extent and as long as Customer's failure to fulfill one or more obligations to cooperate leads to a delay in the agreed course of Contractor's performance, the provisions on remuneration (section 2.5.1) and on the selection of test objects (section 2.5.2, 1st indent) shall apply.

2.4.3 Use of Contractor's Work Results

- Customer may not use any material or work results of Contractor (e.g. software to reproduce vulnerabilities) against third parties or in infrastructure not controlled by Customer. At Contractor's first request, Customer shall indemnify Contractor comprehensively against all third-party claims and reasonable legal defense costs incurred by third parties due to claims against Contractor arising from the use of work results of Contractor that Customer has obtained within the scope of the contractual services. The aforementioned indemnification costs include in particular costs for the defense against claims of third parties, including any correspondence with competent supervisory authorities and courts.
- Customer must obtain Contractor's permission for any publication of material/information from Contractor's reports or about services provided for Customer.

2.5 REMUNERATION

2.5.1 General Rules on Remuneration

- Contractor shall invoice its services in accordance with the underlying offer. If or insofar as not specified in the offer, services from an offer with a service contingent shall be invoiced at a fixed price after the final report has been made available to Customer, other services (in particular those with remuneration according to time and material) at the end of a calendar month for the services rendered up to that point and not yet invoiced.
- Unless otherwise agreed with Customer, Contractor's invoices shall be due immediately and payable without deduction by bank transfer within 14 (fourteen) days of receipt.
- The parties agree that Contractor's implementation phases require considerable preparation and that it cannot provide its services elsewhere if an implementation phase is postponed at short notice. Customer therefore assures that it will pay the full price of the services in the affected implementation phase in the event of postponements of implementation phases requested by it that were not communicated at least 14 days prior to the start of the implementation phase.
- Contractor may claim damages for default from Customer in the amount of 9 percentage points above the applicable base interest rate pursuant to § 247 BGB (German Civil Code). Customer shall pay a lump sum of €20 for the first reminder and €30 for the second reminder.
- Customer shall only be entitled to offset its own claims against Contractor if Customer's claims are undisputed or have been legally established.

2.5.2 Service Packages

- If or to the extent that Customer's delay in cooperating with the agreed services of Contractor is detrimental to Customer (cp. section 2.4.2) results in Contractor being unable to perform its services for Customer (e.g. due to missing access data), Contractor shall be entitled to refrain from testing the infrastructure affected by the failure to cooperate without Customer being released from the obligation to pay the corresponding remuneration.
- If Customer has not called up any service from Contractor within 6 (six) months of the conclusion of the contract, Contractor shall be invoiced for the full agreed service package irrespective of the provision of the service, and Customer shall be obliged to pay.
- If Customer wishes the work to be carried out outside office hours, unless otherwise defined in the offer, the following surcharges will be charged per hour or part thereof:
    - €100 for working hours from Monday to Friday;
    - €175 for working hours on weekends or public holidays at Contractor's place of business.

2.6 Vicarious Agents of Contractor

- Contractor may, at its own discretion, engage vicarious agents to provide all or part of its services, provided that these vicarious agents have at least the same qualifications, skills and expertise as Contractor and are subject to the same confidentiality and other requirements of the contract between the parties.
- Contractor shall be liable to Customer for any misconduct or failure of its vicarious agents as for its own.
- Customer shall always address instructions for the provision of Contractor's services to Contractor, even when using vicarious agents.

2.7 Granted Rights of Use

- In principle, Customer shall not be granted any rights of use to the tools or the hardware/software used in the context of the provision of services. Exceptions to this is software that Contractor makes available to Customer for the traceability of vulnerabilities, to which it grants Customer a simple, non-transferable right of use to trace the respective vulnerabilities in its own infrastructure.
- Customer warrants that it will not use Contractor's contractual services – whether report content, software or in any other form – to discover vulnerabilities in the infrastructure of third parties or to harm third parties in any way whatsoever.
- If/insofar as Contractor provides Customer with software or other copyrighted works as part of its contractual services, Customer may not remove or have removed copyright and other proprietary notices.

2.8 Confidentiality

- Contractor undertakes to treat all information and data that it receives or obtains within the scope of this contract or in connection with the services provided as strictly confidential, and not to pass it on to third parties or use it for its own purposes either during the term of the contract or thereafter, unless expressly permitted by Customer in text form, or the third parties are vicarious agents for the provision of the services for Customer.
- Contractor is aware of its statutory duties of confidentiality and secrecy and warrants that it will act in accordance with these duties. In particular, it shall not disclose any secret information in accordance with § 203 StGB (disclosure of secrets according to the German Criminal Code), § 35 SGB I (social secrecy according to the German Social Code), or data protected by the secrecy of correspondence or telecommunications which it obtains as a result of its activities under this contract.
- Contractor shall only disclose confidential information within its company to those employees who need this information for the proper execution of this contract, and, as the

case may be, vicarious agents, and only on condition that these employees are also subject to the confidentiality obligations of the contract between the parties.

2.9 Data Protection

- Contractor is aware of the importance of its services with regard to data protection and ensures compliance with applicable data protection law and information security measures in accordance with the current state of the art.
- The processing of personal data on behalf of Customer is not subject of Contractor's services; therefore, the parties agree no commissioned data processing pertaining to Art. 28 GDPR takes place.

2.10 Reference of Customer

- Contractor shall be entitled to name Customer as a reference on its website and in marketing materials, including, but not limited to, case studies, reference lists, brochures and presentations, and to use logos (trademarks). Said reference may include, in addition to the company name, a rough description of the services or projects provided, but without giving details of any weaknesses discovered.

2.11 Liability

- The parties shall be liable to each other in accordance with the statutory provisions, i.e. for intent and gross negligence without limitation in terms of amount. They shall only be liable for slight negligence if an obligation is breached without the fulfillment of which the purpose of the contract cannot be achieved (cardinal obligation), and only up to the amount specified in the 4th indent of this section.
- Customer is aware that careful testing for vulnerabilities in the relevant IT and other infrastructure is a core obligation (cardinal obligation) of Contractor, and that data and/or systems may be damaged in the process through no fault of Contractor. Customer therefore releases Contractor from liability for damage that it does not cause intentionally or through gross negligence, even in the context of the performance of its cardinal obligations.
- Liability for consequential damages, loss of profit, loss of savings and/or damages from third-party claims is excluded.
- Contractor shall only be liable for damages arising directly from its activities to an amount that is foreseeable and typical for the contract. In the event of data loss, its liability shall be limited to the value typically incurred for the restoration if Customer fails to fulfill its obligation to protect its infrastructure (cp. section 2.4.1) and, in particular, has made restorable backups of data and systems. To the extent permitted by law, the total amount of Contractor's liability shall be limited to the total fee for the contractual relationship.

- For a separate fee to be agreed between the parties, Contractor may increase its limitation of liability for slight negligence above the maximum limit specified in the fourth indent of this clause. The amount of the increased limitation of liability shall be set out in a separate written agreement between the parties.
- To the extent permissible, claims of Customer against Contractor shall become time-barred one year after the beginning of the statutory limitation period, taking into account the statutory suspension and renewal provisions.
- Mandatory liability regulations, e.g. § 14 ProdHG (German Product Liability Act), shall not be affected.

2.12 Handling of Zero-Day Vulnerabilities

- Contractor shall notify Customer of all vulnerabilities that it discovers in the course of providing its contractual services to Customer. However, if, to the extent and for as long as it discovers critical zero-day vulnerabilities in its IT infrastructure, it reserves the right to shorten the notification of these vulnerabilities so that the following two objectives can be achieved.
    - On the one hand, Customer should be put in a position to eliminate the affected vulnerability as quickly as possible.
    - Secondly, the vulnerability should enable the manufacturer of the affected software to provide a patch to eliminate the vulnerability within a reasonable period of time (usually within 90 days), which can protect the Customer and all other affected third parties from exploitation of the vulnerability by any attacker.
- Contractor will never offer zero-day vulnerabilities for sale to third parties, regardless of whether they are government organizations or private companies. For the avoidance of doubt, exploitation within bug bounty programs (cp. section 2.13) is excluded from the obligation in this paragraph.

2.13 Exploitation of Vulnerabilities in Bug Bounty Programs

- Customer shall permit Contractor to report and exploit vulnerabilities discovered in so-called bug bounty programs in the course of providing its contractual services. It is irrelevant whether the respective bug bounty program is operated by the manufacturer of the software or any third party. For each report within the scope of a bug bounty program, Contractor shall comply with the requirements set out in section 2.8 in particular to eliminate any reference to Customer by name and content, so that recipients of the bug bounty report cannot draw any conclusions about Customer.
- "Utilize" within the meaning of this para. 1 means that Contractor may receive rewards and/or bonuses for reporting the respective vulnerability and use them for its own purposes without this leading to a reduction in the remuneration agreed with Customer.

2.14 Publication of Vulnerabilities in Third-Party Software

- If vulnerabilities are identified in third-party components (e.g. software or hardware) during the provision of services for Customer, Contractor is entitled to inform the manufacturer, apply for CVE (Common Vulnerabilities and Exposures) numbers and publish them as part of a responsible disclosure process.

2.15 Term And Termination

- If and to the extent that the contract between the parties includes a continuing obligation, an initial minimum term of 12 months shall apply, which shall run from the date of commencement of the contract. The contract shall be automatically extended by 3 months in each case after expiry of the initial minimum term if it is not terminated by one of the parties at least 3 (three) months before expiry of the respective extension period.
- Contracts without a continuing obligation (e.g. for a one-off contingent of services to be provided within a certain period of time) cannot be terminated with notice.
- The right of either party to terminate the contractual relationship for good cause remains unaffected.
- Any termination must be declared in text form.

2.16 Final Provisions

- All prices quoted are net prices plus applicable VAT.
- There are no ancillary agreements to the contract or these GTC, and the waiver thereof and the termination of this contract require the text form.
- Customer shall be notified of amendments to these GTC by e-mail or post at least 6 (six) weeks before they come into force. If Customer does not object to the amendments by the time the announced amended GTC enter into force, they shall be deemed accepted by Customer.
- If Customer is a merchant and the disputed business relationship arising from these GTC is attributable to the operation of its commercial business, Stuttgart shall be the exclusive place of jurisdiction for disputes arising from or in connection with the contractual relationship between the parties. Contractor may also sue Customer at another competent court.
- German law applies.
- If individual provisions of these GTC or the main contract are or become invalid, the validity of the remaining provisions shall remain unaffected. The parties shall replace an invalid provision with a valid provision that comes as close as possible to the economic purpose of the invalid provision.

3 Allgemeine Geschäftsbedingungen

Diese Allgemeinen Geschäftsbedingungen („AGB“) gelten für alle Leistungen der MindBytes GmbH (“Auftragnehmerin“, „AN“) für den Kunden (Auftraggeber, „AG“). Die AGB bilden mit einem vom AG unterzeichneten Angebot der AN über für ihn zu erbringende Leistungen die Grundlage des Vertrages der Parteien miteinander.

3.1 Verwendete Begriffe

- Als „Bürozeiten“ gelten Montag bis Freitag (mit Ausnahme von Feiertagen am Sitz der AN) zwischen 8 und 18 Uhr.
- Mit „Infrastruktur“ wird in der Geschäftsbeziehung alles bezeichnet, das von Leistungen der AN für den AG betroffen ist, z. B. IT-Systeme (und Teile davon) und -Dienste („IT-Infrastruktur“), Webanwendungen, aber auch nicht-technische Infrastruktur wie Bürogebäude oder -räume, Rechenzentren und darin enthaltene Server-Flächen.
- Ein „Penetrationstest“ ist ein kontrollierter Versuch, von außen in ein Computer- oder Netzwerksystem einzudringen, um Schwachstellen der jeweils betroffenen Systeme aufzuspüren und zu lokalisieren. Bei diesem Versuch werden u. a. Techniken angewendet, die auch bei einem realen Angriff auf das System Verwendung finden würden. Die Identifikation der Schwachstellen ermöglicht eine Korrektur der Schwachstellen, bevor sie durch einen realen Angriff ausgenutzt werden und sich Dritte unerlaubt Zugang zum System verschaffen können.
- Als „Red Team“ gilt eine Gruppe der AN, die beim AG die Effektivität des Sicherheitsmanagements bewirken soll, indem sie – als Gegner auftretend – Sicherheitslücken aufzuspüren versucht.
- Unter "Zero-Day-Schwachstellen" sind Schwachstellen zu verstehen, für die zum Zeitpunkt ihrer Entdeckung keine allgemein verfügbaren Patches bzw. Gegenmaßnahmen existieren und die daher oder aus anderen Gründen als besonders gefährlich eingestuft werden. Als „kritische Zero-Day-Schwachstelle“ wird in diesem Vertragsverhältnis eine Zero-Day-Schwachstelle bezeichnet, die nur vom Hersteller der betroffenen Software behoben werden kann (z. B. durch einen so genannten „Patch“) und deren Bekanntwerden beliebige Angreifer in die Lage versetzen würde, die Sicherheit Dritter zu kompromittieren, z. B. wenn die Schwachstelle in einem Cloud-Dienst (auch Software/Platform/Sonstiges „as a Service“ genannt) entdeckt wird.

3.2 VERTRAGSGEGENSTAND

3.2.1 Angebote

- Die AN hält sich an ihre Angebote ab Ausstellungsdatum 30 Tage lang gebunden, sofern im jeweiligen Angebot nichts anderes angegeben ist.

3.2.2 Leistungsgegenstand

- Basis der Leistungen der AN für den AG bilden jeweils die von ihm zur Verfügung gestellten Informationen zur Infrastruktur. Für die Effektivität der Leistungen ist es deshalb kritisch, dass der AG der AN die zu prüfende Infrastruktur mitteilt (vgl. Ziff. 3.4.1).
- Die AN schuldet zur vertragsgemäßen Erfüllung ihrer Leistungen ernsthaftes Bemühen und mindestens marktübliche Qualität bei der Erfüllung, aber nicht die Herstellung eines Werkes oder Erreichung eines vom AG mit ihren Leistungen beabsichtigten Ziels.
- Die AN führt je nach Angabe im Angebot in der Infrastruktur des AG Penetrationstests durch und/oder erbringt Leistungen eines Red Teams. In beiden Fällen ist die Entdeckung von Schwachstellen der Gegenstand und das Ziel der Leistungen der AN. Die Beseitigung von Schwachstellen ist ebenso wenig Gegenstand der Leistungen der AN wie jegliche Art von Hosting, Incident Response oder laufende Überwachung der Infrastruktur des AG.
- Der AG erteilt der AN seine ausdrückliche Einwilligung in die zur Erbringung ihrer Leistungen erforderlichen Maßnahmen, insbesondere zu einem etwa damit einhergehenden Zugriff auf und das Verschaffen von Daten, ggf. unter Überwindung einer etwaigen Zugangssicherung der vom Kunden spezifizierten Systeme und/oder aus einer nichtöffentlichen Datenübermittlung und/oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage (§§ 202 ff. StGB). Er erklärt sich außerdem ausdrücklich damit einverstanden, dass bei der Erbringung der Leistungen Daten verändert oder gelöscht werden können (§ 303a StGB).

3.2.3 Änderungen des Leistungsumfangs (Change Requests)

- Soweit der AG Änderungen vereinbarter Leistungen wünscht („Change Request"), wird die AN gegen Vergütung nach den vereinbarten Sätzen den durch den Change Request entstehenden Aufwand und die Machbarkeit prüfen und ihn möglichst kurzfristig über den finanziellen und zeitlichen Änderungsrahmen informieren. Wenn nicht anders vereinbart, berechnet die AN die Aufwände für die besagten Prüfungen nach den vereinbarten Sätzen.
- Der AG darf zur Klärung der Konsequenzen eines Change Requests die Unterbrechung der Leistungserbringung fordern, wenn er der AN spätestens zum Zeitpunkt der

Forderung der Unterbrechung zusichert, die Ausfallzeiten und die durch die Unterbrechung eventuell aufwändigere Wiederaufnahme der Projektrealisierung zu vergüten. Vereinbarte Leistungsfristen und Zeitpläne verlängern sich um die Zeit des Ausfalls und der eventuell aufwändigeren Wiederaufnahme.

- Change Requests sind für ihre Wirksamkeit in Textform zu verfassen und von beiden Parteien zu akzeptieren. Wenn sich die Parteien nicht über ein Änderungsverlangen einigen können, sind die ursprünglich vereinbarten Leistungen unter Berücksichtigung der durch den Change Request entstandenen Verzögerungen weiterhin Vertragsgegenstand.

3.2.4 Mitteilungsweg bei Entdeckung von Schwachstellen

- Informationen über Feststellungen bei Erbringung ihrer Leistungen für den AG übermittelt die AN ihm elektronisch in verschlüsselter Form. Die zum Öffnen benötigten Zugangsdaten (z. B. Passwort) werden über einen zweiten Kanal (z. B. Signal Messenger oder SMS) übermittelt.

3.3 Pflichten der Auftragnehmerin

- Die AN hat den AG in den folgenden Fällen unverzüglich zu informieren:
  - bei Erlangung von Kenntnis eines Schadens an seiner Infrastruktur oder wenn der Eintritt eines solchen Schadens absehbar ist;
  - bei Feststellung von Schwachstellen, die die AN nach eigenem Ermessen als kritisch einstuft (wobei sie sich am Common Vulnerability Scoring System in der jeweils aktuellen Fassung orientiert).
- Die AN hat bei der Erbringung ihrer Leistungen ausschließlich angemessen qualifiziertes Personal einzusetzen, das mindestens derselben Vertraulichkeit unterworfen ist wie die AN dem AG gegenüber.
- Die AN hat sämtliche im Rahmen ihrer Leistungserbringung für den AG erlangten Informationen (z. B. zu Feststellungen von Schwachstellen und Infrastrukturaufbau) 3 (drei) Jahre nach Ende der vertraglichen Leistungen aufzubewahren.

3.4 Pflichten des Auftraggebers

3.4.1 Betroffene Infrastruktur

- Der AG garantiert, dass er befugt ist, die AN mit der Durchführung der vertraglichen Leistungen zu beauftragen.
- Der AG hat der AN möglichst frühzeitig, spätestens aber 3 Werktage vor Beginn ihrer Leistungen für ihn die von ihren Leistungen betroffene Infrastruktur zu definieren und hierbei ggf. auch Teile der Infrastruktur zu nennen, die die AN nicht aktiv auf Schwachstellen prüfen darf (z. B. wegen Geheimnisschutz oder Unantastbarkeit von

Systemteilen, die von Dritten betrieben werden, die die Leistungen der AN nicht erlauben). Durch die besagte Nennung der von Penetrationstests betroffenen Infrastruktur erteilt der AG der AN die Erlaubnis, die vereinbarten Maßnahmen zu ergreifen (permission to attack).

- Der AG ist verpflichtet, vor Erbringung der Leistungen seitens der AN alle Sicherheitsmaßnahmen zu treffen, die notwendig sein können, um von den Leistungen der AN betroffene Systeme und Daten im Falle von Schäden (z. B. Datenverlust) nach einer Leistung der AN wieder in den ursprünglichen Zustand zurück versetzen zu können (z. B. über Backups).
- Der AG ist sich bewusst, dass trotz umfassender Vorsichtsmaßnahmen der AN im Rahmen ihrer Leistungserbringung vor allem durch Penetrationstests Schäden an bestehenden Systemen und Daten auftreten können. Solche Schäden können so irreversibel sein, dass sie nur durch Wiederherstellung der Systeme aus Backups und im worst case durch umfangreiche Nachbearbeitung seitens des AG zu beseitigen sind.
- Der AG hat die AN unverzüglich zu informieren, wenn er Kenntnis davon erlangt, dass eine Handlung der AN zu einem Schaden an der Infrastruktur geführt hat.

3.4.2 Mitwirkung

- Der AG muss die AN bei der Erbringung ihrer Leistungen für ihn im erforderlichen Rahmen zu unterstützen. Hierzu kann je nach Vereinbarung gehören:
  - Abstimmung/Vereinbarung von Einsatz- und/oder Leistungsterminen;
  - Zurverfügungstellung von Informationen, Material, Out-of-Jail-Karten o. a.;
  - bei Vor-Ort-Terminen beim AG Zurverfügungstellung eine angemessenen Arbeitsumgebung;
  - Gewährung von Zutritt und/oder Zugang zu Infrastruktur und Internetzugang;
- Der AG hat interne Stellen (z. B. Mitarbeiter, Vorgesetzte, Arbeitnehmervertretung) und Dritte, die von den Leistungen der AN betroffen sind, rechtzeitig vor der Erbringung der Leistungen zu informieren.
- Wenn, soweit und solange die Nichterfüllung einer oder mehrerer Mitwirkungspflichten des AG zu einer Verzögerung des vereinbarten Ablaufes der Leistungserbringung der AN führt, gelten die Regelungen zur Vergütung (Ziff. 3.5.1) und zur Auswahl der Prüfungsgegenstände (Ziff. 3.5.2, 1. Spiegelstrich).

3.4.3 Verwendung von Arbeitsergebnissen der AN

- Der AG darf keinerlei Material oder Arbeitsergebnisse der AN (z. B. Software zur Nachvollziehung von Schwachstellen) gegen Dritte oder in nicht von ihm kontrollierter Infrastruktur einsetzen. Der AG stellt die AN auf deren erste Aufforderung hin umfassend von allen Ansprüchen Dritter und angemessenen Rechtsverteidigungs-kosten frei, die dadurch entstehen, dass Dritte gegen die AN Ansprüche wegen des

Einsatzes von Arbeitsergebnissen der AN entstehen, die der AG im Rahmen der vertraglichen Leistungen erlangt hat. Die genannten Freistellungskosten beinhalten insbesondere Kosten für die Verteidigung gegen Ansprüche des Dritten einschließlich eventueller Korrespondenz mit zuständigen Aufsichtsbehörden und Gerichten.

- Der AG hat für jede Veröffentlichung von Material/Informationen aus Berichten der AN bzw. über Leistungen für ihn die Erlaubnis der AN einzuholen.

3.5 Vergütung

3.5.1 Allgemeines zur Vergütung

- Die AN rechnet ihre Leistungen nach Maßgabe des zu Grund liegenden Angebotes ab. Wenn bzw. soweit nicht im Angebot spezifiziert, werden Leistungen aus einem Angebot mit einem Leistungskontingent zu einem Festpreis nach Zurverfügungstellung des Abschlussberichtes an den AG abgerechnet, sonstige Leistungen (insbesondere solche mit Vergütung nach Aufwand) am Ende eines Kalendermonats für die bis dahin erbrachten und noch nicht abgerechneten Leistungen.
- Rechnungen der AN sind vorbehaltlich anderer Vereinbarung mit dem AG sofort fällig und ohne Abzug innerhalb von 14 (vierzehn) Tagen ab Erhalt durch Banküberweisung zu begleichen.
- Die Parteien sind sich darüber einig, dass Durchführungsphasen der AN erheblicher Vorbereitung bedürfen und sie ihre Leistungen bei kurzfristiger Verschiebung einer Durchführungsphase nicht anderweitig erbringen kann. Der AG sichert deshalb zu, bei von ihm gewünschten Verschiebungen von Durchführungsphasen, die nicht jeweils mindestens 14 Tage vor Start der Durchführungsphase kommuniziert wurden, den vollen Preis der Leistungen in der betroffenen Durchführungsphase zu zahlen.
- Die AN darf Verzugsschäden gegenüber dem AG in Höhe von 9 %-Punkten über dem jeweils geltenden Basiszinssatz gem. § 247 BGB geltend machen. Für die jeweils 1. Mahnung hat der AG eine Pauschale iHv. 20 €, für die 2. Mahnung iHv. 30 € zu zahlen.
- Der AG ist zur Aufrechnungen eigener Ansprüche gegen die AN nur berechtigt, wenn seine Ansprüche unbestritten oder rechtskräftig festgestellt wurden.

3.5.2 Leistungspakete

- Wenn bzw. soweit der Verzug des AG bei seiner Mitwirkung an den vereinbarten Leistungen der AN für ihn (vgl. Ziff. 3.4.2) dazu führt, dass die AN ihre Leistungen für den AG nicht erbringen kann (z. B. wegen fehlenden Zugangsdaten), ist die AN berechtigt, die Prüfung der jeweils von der unterlassenen Mitwirkung betroffenen Infrastruktur zu unterlassen, ohne dass der AG von der Pflicht zur Zahlung der entsprechenden Vergütung befreit wird.

- Wenn der AG innerhalb von 6 (sechs) Monaten ab Vertragsschluss keinerlei Leistung der AN abgerufen hat, ist sie unabhängig von der Leistungserbringung zur Abrechnung des vollen vereinbarten Leistungspaketes berechnet und der AG zur Zahlung verpflichtet.
- Sollte der AG eine Durchführung außerhalb der Bürozeiten wünschen, sofern nicht anders im Angebot definiert ist, so werden folgende Aufpreise pro angefangene Stunde berechnet:
    - 100 € für Arbeitszeiten von Montag bis Freitag;
    - 175 € für Arbeitszeiten an Wochenend- oder Feiertagen am Sitz der AN.

3.6 Erfüllungsgehilfen des AN

- Die AN darf nach eigenem Ermessen zur Erbringung ihrer gesamten Leistungen oder von Teilen davon Erfüllungsgehilfen hinzuziehen, sofern diese Erfüllungsgehilfen mindestens dieselben Qualifikationen, Fähigkeiten und Fachkenntnisse wie die AN aufweisen und denselben Vertraulichkeits- und sonstigen Anforderungen des Vertrages zwischen den Parteien unterliegen.
- Die AN haftet gegenüber dem AG für jegliches Fehlverhalten oder Versagen ihrer Erfüllungsgehilfen wie für eigenes.
- Der AG hat Weisungen zur Erbringung der Leistungen der AN auch beim Einsatz von Erfüllungsgehilfen stets an die AN zu richten.

3.7 Eingeräumte Nutzungsrechte

- Dem AG werden grundsätzliche keine Nutzungsrechte an den Werkzeugen bzw. der im Rahmen der Leistungserbringung eingesetzten Hard-/Software eingeräumt. Ausnahmen stellt Software dar, die die AN dem AG zur Nachvollziehbarkeit von Schwachstellen zur Verfügung stellt, an der sie ihm ein einfaches, nicht übertragbares Nutzungsrecht zur Nachvollziehung der jeweiligen Schwachstelle(n) in der eigenen Infrastruktur einräumt.
- Der AG sichert zu, Vertragsleistungen der AN – gleich ob Berichtsinhalte, Software oder in sonstiger Form – nicht einzusetzen, um Schwachstellen in der Infrastruktur Dritter zu entdecken oder Dritten in jedweder Form zu schaden.
- Wenn/soweit die AN dem AG im Rahmen ihrer vertraglichen Leistungen Software oder andere urheberrechtlich geschützte Werke zur Verfügung stellt, darf der AG urheber- und sonstige schutzrechtliche Vermerke nicht entfernen oder entfernen lassen.

3.8 Vertraulichkeit

- Die AN verpflichtet sich, alle Informationen und Daten, die sie im Rahmen dieses Vertrages oder in Zusammenhang mit den erbrachten Dienstleistungen erhält oder

erlangt, streng vertraulich zu behandeln und weder während der Vertragslaufzeit noch nach deren Beendung an Dritte weiterzugeben oder für eigene Zwecke zu verwenden, es sei denn, es wurde ausdrücklich in Textform vom AG erlaubt, oder die Dritten sind Erfüllungsgehilfen zur Erbringung der Leistungen für den AG.

- Die AN ist sich ihrer gesetzlichen Pflichten zur Vertraulichkeit bzw. Geheimhaltung bewusst und sichert zu, sich gemäß diesen Pflichten zu verhalten. Insbesondere wird sie keine geheimen Informationen gem. § 203 StGB (Offenbarung von Geheimnissen), § 35 SGB I (Sozialgeheimnis) oder vom Brief- oder Telekommunikationsgeheimnis geschützten Daten offenbaren, die sie aufgrund ihrer Tätigkeit im Rahmen dieses Vertrages erlangt.
- Die AN hat vertrauliche Informationen nur innerhalb ihres Unternehmens an diejenigen Mitarbeitenden oder ggf. Erfüllungsgehilfen weiterzugeben, die diese Informationen für die ordnungsgemäße Durchführung dieses Vertrages benötigen, und nur unter der Bedingung, dass diese Mitarbeiter ebenfalls den Vertraulichkeitspflichten des Vertrages zwischen den Parteien unterliegen.

3.9 Datenschutz

- Die AN ist sich der Bedeutung ihrer Leistungen in Datenschutzhinsicht bewusst und gewährleistet die Einhaltung geltenden Datenschutzrechts und Maßnahmen der Informationssicherheit nach dem jeweils aktuellen Stand der Technik.
- Die Verarbeitung personenbezogener Daten im Auftrag des AG ist nicht Gegenstand der Leistungen der AN; deshalb sind sich die Parteien einig, dass keine Auftragsverarbeitung iSv. Art. 28 DSGVO vorliegt.

3.10 Referenznennung des Auftraggebers

- Die AN ist berechtigt, den AG als Referenz auf ihrer Website und in Marketingmaterialien zu nennen, einschließlich, aber nicht beschränkt auf, Fallstudien, Referenzlisten, Broschüren und Präsentationen, und hierbei auch Logos (Marken) zu nutzen. Die besagte Referenznennung kann neben der Firmennennung eine grobe Beschreibung der erbrachten Dienstleistungen oder Projekte umfassen, jedoch ohne dass Details zu entdeckten Schwachstellen genannt werden.

3.11 Haftung

- Die Parteien haften einander wie nach den gesetzlichen Bestimmungen, also für Vorsatz und grobe Fahrlässigkeit der Höhe nach unbegrenzt. Für leichte Fahrlässigkeit haften sie nur, soweit eine Pflicht verletzt wird, ohne deren Erfüllung der Vertragszweck nicht erreicht werden kann (Kardinalpflicht), und nur bis zur in der im 4. Spiegelstrich dieser Ziffer genannten Höhe.

- Der AG ist sich bewusst, dass das sorgfältige Testen auf Schwachstellen der jeweils betroffenen IT- und sonstigen Infrastruktur Kernpflicht (Kardinalpflicht) der AN ist und dass hierbei ohne jegliches Verschulden der AN Daten und/oder Systeme beschädigt werden können. Der AG entbindet die AN deshalb von der Haftung für Schäden, die sie nicht vorsätzlich oder grob fahrlässig auch im Rahmen der Erbringung ihrer Kardinalpflichten verursacht.
- Die Haftung für Folgeschäden, entgangenen Gewinn, ausgebliebene Einsparungen und/oder Schäden aus Ansprüchen Dritter ist ausgeschlossen.
- Die AN haftet für direkt durch ihre Tätigkeit entstehende Schäden nur in vertragstypisch vorhersehbarer Höhe. Bei Datenverlust ist ihre Haftung auf den Wert beschränkt, der für die Wiederherstellung typischerweise anfällt, wenn der AG seine Pflicht zum Schutz seiner Infrastruktur (vgl. Ziff. 3.4.1) erfüllt, insbesondere wiederherstellbare Backups von Daten und Systemen hergestellt hat. Die Gesamtsumme der Haftung der AN ist, soweit gesetzlich zulässig, auf die Höhe des gesamten Honorars des Vertragsverhältnisses beschränkt.
- Gegen gesondertes Entgelt, das zwischen den Parteien zu vereinbaren ist, kann die AN ihre Haftungsbegrenzung für leichte Fahrlässigkeit über die im 4. Spiegelstrich dieser Ziffer festgelegte Höchstgrenze hinaus erhöhen. Die Höhe der erhöhten Haftungsbegrenzung wird in einer gesonderten schriftlichen Vereinbarung zwischen den Parteien festgelegt.
- Soweit zulässig, verjähren Ansprüche des AG gegen die AN unter Berücksichtigung der gesetzlichen Hemmungs- und Erneuerungstatbestände ein Jahr nach Beginn der gesetzlichen Verjährungsfrist.
- Zwingende Haftungsvorschriften, z. B. § 14 ProdHG, sollen nicht angetastet werden.

3.12 Umgang mit Zero-Day-Schwachstellen

- Die AN wird den AG auf alle Schwachstellen hinweisen, die sie bei der Erbringung ihrer vertraglichen Leistungen für ihn entdeckt. Wenn, soweit und solange sie allerdings kritische Zero-Day-Schwachstellen in seiner IT-Infrastruktur entdeckt, behält sie sich das Recht vor, den Hinweis auf diese Schwachstellen zu kürzen, sodass die folgenden zwei Ziele erreicht werden können.
    - Zum einen soll der AG in die Lage versetzt werden, möglichst kurzfristig die betroffene Schwachstelle beseitigen zu können.
    - Zum anderen soll die Schwachstelle vom Hersteller der betroffenen Software in die Lage versetzt werden, innerhalb angemessener Zeit (in der Regel innerhalb von 90 Tagen) einen Patch zur Beseitigung der Schwachstelle zur Verfügung zu stellen, der den AG und alle anderen betroffenen Dritten vor der Ausnutzung der Schwachstelle durch beliebige Angreifer schützen kann.

- Die AN wird Zero-Day-Schwachstellen niemals Dritten zum Kauf anbieten, gleich ob Regierungsorganisation oder Privatunternehmen. Zur Vermeidung von Missverständnissen: Von der Pflicht in diesem Absatz ist die Verwertung innerhalb von Bug Bounty-Programmen (vgl. Ziff. 3.13) ausgenommen.

3.13 Verwertung von Schwachstellen in Bug Bounty-Programmen

- Der AG gestattet der AN, im Rahmen der Erbringung ihrer vertraglichen Leistungen für ihn entdeckte Schwachstellen in so genannten Bug Bounty-Programmen zu melden und zu verwerten. Hierbei ist irrelevant, ob das jeweilige Bug Bounty-Programm vom Hersteller der Software oder einem beliebigen Dritten betrieben wird. Die AN hat bei jeder Meldung im Rahmen eines Bug Bounty-Programms die in Ziff. 3.8 vereinbarte Vertraulichkeit zu wahren, also insbesondere jeden namentlich und inhaltlichen Bezug zum AG zu beseitigen, sodass für Empfänger der Bug Bounty-Meldung kein Rückschluss auf den AG möglich ist.
- „Verwerten" im Sinne dieses Abs. 1 bedeutet, dass die AN Belohnungen und/oder Prämien für die Meldung der jeweiligen Schwachstelle erhalten und für eigene Zwecke verwenden darf, ohne dass dies zu einer Reduktion der mit dem AG vereinbarten Vergütung führt.

3.14 Veröffentlichung von Schwachstellen in Software Dritter

- Sollten im Rahmen der Erbringung der Leistungen für den AG Schwachstellen in Komponenten (z. B. Software oder Hardware) von Drittanbietern identifiziert werden, ist die AN berechtigt, Hersteller darüber zu informieren, CVE-(Common Vulnerabilities and Exposures-)Nummern zu beantragen und im Rahmen eines Responsible Disclosure-Prozesses zu veröffentlichen.

3.15 Laufzeit und Kündigung

- Wenn und soweit der Vertrag zwischen den Parteien ein Dauerschuldverhältnis beinhaltet, gilt eine initiale Mindestlaufzeit von 12 Monaten, die ab dem Datum des Vertragsbeginns läuft. Der Vertrag verlängert sich nach Ablauf der initialen Mindestlaufzeit automatisch um jeweils 3 Monate, wenn er nicht von einer Partei spätestens 3 (drei) Monate vor Ablauf der jeweiligen Verlängerungsperiode gekündigt wird.
- Verträge ohne Dauerschuldverhältnis (z. B. über ein einmaliges Leistungskontingent, das innerhalb eines bestimmten Zeitraumes erbracht werden soll) sind nicht ordentlich kündbar.
- Das Recht jeder Partei, das Vertragsverhältnis aus wichtigem Grund zu kündigen, bleibt unberührt.

- Jede Kündigung ist in Textform zu erklären.

3.16 Schlussbestimmungen

- Alle Preisangaben verstehen sich als Nettopreise zzgl. anfallender gesetzlicher Mehrwertsteuer.
- Nebenabreden zum Vertrag oder diesen Allgemeinen Geschäftsbedingungen bestehen nicht und bedürfen, ebenso wie der Verzicht darauf und die Kündigung dieses Vertrages, der Textform.
- Änderungen dieser AGB werden dem AG mindestens 6 (sechs) Wochen vor Inkrafttreten per E-Mail oder postalisch mitgeteilt. Widerspricht der AG den Änderungen nicht bis zum Inkrafttreten der angekündigten geänderten AGB, gelten diese als von ihm akzeptiert.
- Ist der AG Kaufmann und ist die sich aus diesen Bedingungen ergebende streitige Geschäftsbeziehung dem Betrieb seines Handelsgewerbes zuzurechnen, ist Stuttgart ausschließlicher Gerichtsstand für Auseinandersetzungen aus oder in Zusammenhang mit der Vertragsbeziehung zwischen den Parteien. Die AN kann den AG auch bei einem anderen zuständigen Gericht verklagen.
- Es gilt deutsches Recht.
- Sind oder werden einzelne Bestimmungen dieser AGB oder des Hauptvertrages unwirksam, bleibt die Gültigkeit der Bestimmungen im Übrigen unberührt. Die Parteien werden eine unwirksame Bestimmung durch eine wirksame Bestimmung ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung möglichst nahe kommt.