GENERAL TERMS AND CONDITIONS OF INFINITAS SECURITY GMBH

ENGLISH CONVENIENCE TRANSLATION

Note: This is a non-binding English translation of the German version of this document, including its annexes. Only the German version is legally binding and authoritative. This translation is provided for information purposes only and does not form part of the agreement.

The German version is available here.

Valid from: 23.03.2026

GENERAL TERMS AND CONDITIONS OF INFINITAS SECURITY GMBH

ENGLISH CONVENIENCE TRANSLATION

1. Scope of Application, Contracting Party, Consumer Notice

1.1 These General Terms and Conditions (hereinafter the "GTC") apply to all contracts between Infinitas Security GmbH, with registered seat in Munich, Germany (hereinafter "Infinitas Security"), and its customer (hereinafter the "Customer") regarding the use of the software-as-a-service platform "Infinitas CyberPilot", as well as any other services provided by Infinitas Security in connection therewith and any contracts concluded with Infinitas Security.

1.2 For the purposes of these GTC, a Customer shall exclusively be an entrepreneur within the meaning of Section 14 of the German Civil Code (BGB), a legal entity under public law, or a special fund under public law. Consumers within the meaning of Section 13 BGB are excluded as contractual counterparties.

1.3 Any deviating, conflicting or supplementary general terms and conditions of the Customer shall not become part of the contract unless Infinitas Security has expressly agreed to their applicability in writing. This requirement for consent shall apply in all cases, including, for example, where Infinitas Security provides services without reservation while being aware of the Customer's general terms and conditions.

2. Subject Matter of the Contract, Contract Documents and Order of Precedence

2.1 The subject matter of the contract is the use of the Infinitas CyberPilot platform via the internet (SaaS), including any related modules and functions, as well as the provision of ancillary services (e.g. support, training, implementation assistance), in each case in accordance with the agreement concluded between the parties, the terms of use, service descriptions and price lists, each in the version valid at the time of conclusion of the contract.

2.2 The exact scope of services owed shall be determined primarily by the respective individual contract or order confirmation and the service description referenced therein. The following order of precedence shall apply:

- the individual contract concluded between the parties
- these GTC in the version valid on the date of conclusion of the contract

3. Conclusion of Contract, Offers, Performance Dates

3.1 The contract shall be concluded upon completion of the ordering process via the Infinitas Security website by the Customer or upon commencement of the chargeable provision of services by Infinitas Security, whichever occurs first.

3.2 Performance dates, deadlines and provisioning dates shall only be binding if they are expressly designated as such.

4. Services of Infinitas Security (Scope of Services of CyberPilot)

4.1 Infinitas Security shall provide the Customer with access to Infinitas CyberPilot as a SaaS platform for the planning, management and tracking of improvements to information security.

4.2 Infinitas Security shall provide the services in accordance with the state of the art. Unless expressly agreed otherwise, the services constitute support services for the Customer, who remains solely responsible. Infinitas Security does not owe any specific economic success, the attainment of any particular maturity level, or results of any particular scope. In particular, Infinitas Security does not owe any specific level of security or freedom from security vulnerabilities. Advisory content and recommendations, including those generated by the AI assistance, are regularly based on assumptions, estimates and information provided by the Customer and must be reviewed by the Customer at its own responsibility. They do not constitute a guarantee, an assurance of specific characteristics, or a legally binding agreement on quality or characteristics.

4.3 Infinitas Security shall be entitled to modify services, functions or technical interfaces where there are objective reasons for doing so that lie outside the control of Infinitas Security (e.g. requirements imposed by third parties, security requirements, legal provisions or statutory changes), provided that the agreed fees do not change by more than 10% as a result. The Customer shall be informed of any material changes at least two weeks before such material change takes effect. The Customer shall have the right to object to any change in fees. If the Customer objects to the change in fees, the parties shall enter into negotiations regarding an adjustment of the fees within 10 (ten) business days (business day: Monday to Friday). If the parties fail to reach agreement on a fee adjustment within twenty (20) business days after entering into such negotiations, Infinitas Security may terminate the contract for good cause by giving ten (10) business days' notice after the day on which one of the parties has declared that the negotiations have failed. Such termination must be declared within five (5) business days after the failure of the negotiations. To comply with this declaration period, it shall be sufficient if a copy of the notice of termination is received in advance in electronic form. Infinitas Security may modify user interfaces or make purely technical changes to the system environments at any time.

4.4 Infinitas Security shall be entitled to engage suitable third parties (subcontractors) for the provision of the services. Infinitas Security shall remain responsible to the Customer for the performance of the contract.

4.5 Infinitas Security offers certain services free of charge. There shall be no entitlement to free services. Infinitas Security shall be entitled at any time to modify, restrict or discontinue the scope, functionality or availability of free services.

5. Availability, Maintenance, Support

5.1 Infinitas Security shall make CyberPilot available with availability appropriate to the purpose of the contract. Planned maintenance work shall, where possible, be carried out outside normal business hours and shall be announced to the Customer within a reasonable notice period.

5.2 In the event of disruptions, Infinitas Security shall provide reasonable standard support on business days during normal business hours.

6. Duties and Obligations of the Customer

6.1 The Customer shall provide all required provisioning and cooperation services in a timely manner, to the extent required and free of charge. This includes, in particular, the provision of all necessary information, data and systems.

6.2 The Customer shall ensure that the data and files provided by it are technically and substantively correct and free from malware. If the Customer breaches this obligation, it shall compensate Infinitas Security for any resulting damage and expenses.

6.3 The Customer guarantees, by way of an independent guarantee undertaking, that it may freely dispose of all rights, data and information required for the performance of the contract without infringing any third-party rights. The Customer further guarantees that it will not transmit, or cause to be processed, any unlawful content or any content that violates official or statutory prohibitions.

6.4 The Customer shall keep access credentials and authentication methods confidential and protect them against access by unauthorized third parties. Access accounts may only be used by the respective authorized users. The Customer shall inform Infinitas Security without undue delay of any suspected misuse or security incidents.

6.5 The Customer shall be solely responsible for reviewing, validating and implementing all notices, assessments, recommended measures and plans made available in CyberPilot. Decisions regarding security measures, budgets, priorities and roadmaps shall rest solely with the Customer. The Customer acknowledges that, notwithstanding analysis and advisory services, an unavoidable residual risk remains, as threat scenarios, attack methods and technical conditions are subject to continuous change.

7. Rights of Use

7.1 For the term of the contract, the Customer shall receive the simple, non-exclusive, non-transferable and non-sublicensable right to use Infinitas CyberPilot via the internet within the contractually agreed scope. The right of use shall be limited to the number of users and purposes defined in the contract. Reverse engineering, decompilation and any other interference are prohibited unless mandatorily permitted by law. The Customer may not circumvent any technical protection measures.

7.2 To the extent that, in the course of providing the services, Infinitas Security creates independent work results, analyses or documents outside the platform, and such items are not already licensed as part of the SaaS service, the Customer shall receive, subject to the condition precedent of full payment of the agreed remuneration, a simple, transferable right of use thereto, unlimited in time, territory and subject matter, for all known types of use, unless otherwise agreed.

7.3 Open-source components within the platform shall be subject to the applicable open-source licences, which shall be identified in the documentation. Their provisions shall prevail with respect to the relevant components.

7.4 If the Customer voluntarily provides Infinitas Security with feedback, ideas or suggestions for improvement, the Customer grants Infinitas Security a royalty-free, non-exclusive right, unlimited in time and territory, to use, modify and exploit the same.

8. Retention of Title and Reservation of Rights

Infinitas Security retains title to physical items (e.g. documents) and reserves any rights to be granted until full payment of the remuneration owed has been made. Subject to mandatory statutory provisions, resale or pledging prior to full payment shall not be permitted.

9. Remuneration, Prices, Due Dates, Payments

9.1 All prices are net prices plus the applicable statutory value added tax and any incidental costs in accordance with the prices specified in the individual contract.

9.2 If the parties have agreed on monthly payment, payments shall be due monthly in advance. If the parties have agreed on annual payment, the annual fee shall be due in full and in advance at the beginning of the respective annual period. Remuneration based on time spent (e.g. consulting services) shall be determined upon conclusion of the contract and invoiced at the agreed rates.

9.3 Invoices shall be paid to the account specified in the invoice and must be credited no later than on the tenth day after receipt of the invoice. In the case of SEPA direct debit, the debit shall not be made before the seventh day after receipt of the invoice. The Customer shall bear the costs of returned direct debits for which the Customer is responsible.

9.4 The Customer shall only have a right of set-off to the extent that its counterclaim has been finally adjudicated or is undisputed. The Customer may only exercise rights of retention in respect of counterclaims arising from the same contractual relationship.

9.5 In the event of default in payment, Infinitas Security shall be entitled to demand default interest at a rate of nine percentage points above the base interest rate, as well as a flat-rate default charge of EUR 40. The Customer may prove that the damage was lower. The assertion of further default damages and other rights shall remain unaffected.

9.6 Payment processing may also be carried out via external payment service providers. Depending on the selected payment method, additional contractual relationships may arise between the Customer and the payment service provider. In such case, the terms and conditions of the external payment service provider shall apply in addition. If certain payment methods are selected, the payment service providers may carry out a credit assessment. Further information on this, as well as the applicable terms, can be viewed during the ordering process.

10. Objections to Invoices

Any objections to the amount or content of invoices must be raised without undue delay after receipt of the invoice and must be received by Infinitas Security within eight weeks of receipt of the invoice. If no timely objection is made, the invoice shall be deemed approved. Any statutory claims of the Customer shall remain unaffected.

11. Amendments to the GTC and Service Descriptions

Infinitas Security shall be entitled to amend these GTC and the service descriptions with effect for the future, provided there is an objective reason for doing so, for example adjustment to changes in legislation, case law, security requirements or market conditions, and provided that such amendments are communicated to the Customer in text form with reasonable notice. Amendments to the detriment of the Customer shall take effect no earlier than two months after notification. The Customer shall have the right to object to such amendments. If the Customer objects in due time, either party may terminate the contract for good cause with effect as of the date on which the amendment is to take effect. If the Customer does not object, the amendments shall be deemed approved.

12. Default, Suspension, Termination Rights

12.1 If the Customer is in default with two consecutive monthly payments or a substantial part thereof, or if, over a period extending across more than two payment dates, the Customer is in default with an amount equal to two months' fees, Infinitas Security shall be entitled to terminate the contractual relationship without notice for good cause. Any further rights arising from default in payment shall remain unaffected.

12.2 In the event of default in payment or material breaches of duty by the Customer, Infinitas Security may, after prior warning, suspend the services in whole or in part until the contractual status has been restored. The Customer's obligation to pay shall remain in force during any justified suspension.

13. Warranty

13.1 Infinitas Security warrants that the contractually agreed quality characteristics will be complied with in all material respects. The Customer shall notify Infinitas Security of any identifiable defects without undue delay after becoming aware of them. Section 377 of the German Commercial Code (HGB) shall apply accordingly.

13.2 Infinitas Security does not assume any guarantees, in particular not with regard to specific qualities or characteristics, unless such guarantee has been expressly designated as a guarantee in writing. No guarantee is given for the representativeness, completeness, accuracy or timeliness of results, analyses or recommendations. Infinitas Security does not warrant or guarantee that the Customer's IT systems, networks or organizational structures are or will remain free from vulnerabilities, or that cyberattacks, data loss or other IT security incidents can be prevented.

13.3 In the event of proven defects, Infinitas Security shall, at its own discretion, be entitled to cure by re-performing the service free of defects or by remedying the defect. Infinitas Security shall have at least two attempts to do so. If cure fails definitively, the Customer may reduce the remuneration or, in the case of a defect that is not merely insignificant, withdraw from the contract. The right to claim damages shall remain unaffected in accordance with these GTC. Infinitas Security shall bear the expenses necessary for cure only if it subsequently turns out that a defect actually existed.

14. Liability

14.1 Infinitas Security shall be liable without limitation in cases of intent and gross negligence, in the event of culpable injury to life, body or health, upon the assumption of a guarantee, and pursuant to the provisions of the German Product Liability Act.

14.2 In cases of slight negligence, Infinitas Security shall, except in the event of injury to life, body or health, be liable only if essential contractual obligations have been breached. Essential contractual obligations are obligations whose fulfilment is a prerequisite for the proper performance of the contract and on the observance of which the Customer may regularly rely. In such case, liability shall be limited to damage typical for the contract and foreseeable at the time of conclusion of the contract.

14.3 Any further liability is excluded unless otherwise agreed in writing.

14.4 Except in the cases set out in Section 14.1, the liability of Infinitas Security shall be limited in amount to twice the remuneration agreed for the respective project or contract year.

14.5 The above limitation of liability shall also apply to the personal liability of the employees, representatives and corporate bodies of Infinitas Security.

14.6 Contractual and non-contractual claims against Infinitas Security that are based on a defect must be asserted within one year from the date on which they arise.

15. No Certification Effect; No Data Monitoring; No Guarantee through External Representations

15.1 Reports, presentations, statements or other work results of Infinitas Security do not constitute a certification, an audit with attest function, or a legally binding confirmation of a specific level of security, unless expressly agreed in writing as such.

15.2 Terms, summaries or assessments such as “appropriate”, “proper”, “compliant”, “secure” or similar wording merely constitute a professional assessment as of the respective time of review and do not establish any guarantee, any strict liability irrespective of fault, or any permanently owed level of security.

15.3 Information contained in offers, presentations, informational materials, on websites or in other sales materials of Infinitas Security shall not constitute an agreement on quality or characteristics and shall not constitute a guarantee unless expressly designated in writing as a binding guarantee.

15.4 The services relate exclusively to risks that are identifiable and assessable at the time the respective services are provided. Subject to Section 14, liability for future attack methods that were not identifiable at the time of performance or were novel at that time is excluded.

16. Confidentiality

16.1 The parties undertake to treat as strictly confidential all information of the other party that becomes known to them in the course of their cooperation and is either marked as confidential or is evidently confidential, including trade and business secrets within the meaning of the German Trade Secrets Act, to use such information exclusively for contractual purposes, and to disclose it to third parties only to the extent necessary for the performance of the contract or where there is a statutory obligation to do so.

16.2 Subcontractors of Infinitas Security shall not be deemed third parties, provided that they are bound by appropriate confidentiality obligations.

16.3 The confidentiality obligation shall survive termination of the contract.

17. Data Protection, Processing on Behalf, Data Security

17.1 To the extent that Infinitas Security processes personal data on behalf of the Customer in the course of providing the services, the parties hereby conclude the data processing agreement pursuant to Article 28 GDPR contained in the annex (DPA).

17.2 Infinitas Security shall implement appropriate technical and organizational measures to protect the data in accordance with the state of the art.

17.3 The Customer shall remain the controller under data protection law with respect to the personal data processed within the platform and shall ensure that an appropriate legal basis for the processing exists and that the rights of data subjects are safeguarded.

18. Export Control, Compliance

The Customer shall comply with all applicable export control, sanctions and trade law provisions in connection with the use of CyberPilot, its contents, and any data and documents

provided by Infinitas Security. The parties undertake to comply with applicable anti-corruption and anti-money laundering laws.

19. Force Majeure

19.1 Infinitas Security shall be released from its obligation to perform for the duration and to the extent of the impediment to performance, insofar as the non-performance is due to events of force majeure. Force majeure means events outside the sphere of influence of Infinitas Security that, upon reasonable consideration, could not have been avoided even with the exercise of utmost care, such as natural disasters, war, acts of terrorism, civil unrest, strikes, lawful lockouts, pandemics, epidemics, official orders, power outages, failures of telecommunications networks, or attacks on IT systems, provided that such attacks occur despite appropriate protective measures.

19.2 Infinitas Security shall inform the Customer without undue delay of the occurrence of such event and its expected duration. Payments already made for services not rendered shall be credited on a reasonable pro rata basis if the disruption continues for a prolonged period.

20. References and Contacting the Customer

20.1 If the Customer permits its use as a reference, Infinitas Security shall be entitled to name the Customer as a reference by using the company name, displaying the company logo, naming a contact person, and providing a factual description of the services rendered. This right shall also apply for five years after termination of the contract. Any statutory rights of the Customer to revoke a granted consent for good cause shall remain unaffected.

20.2 Infinitas Security shall be entitled to contact the Customer in connection with existing contractual relationships using the Customer's business contact details, in particular for contract performance, security-related information, and its own similar services. The Customer may object to marketing communications at any time.

21. Contract Term, Termination, Return of Data

21.1 Unless otherwise agreed, the contract shall commence upon provision of access to CyberPilot and shall have the term agreed between the parties in the individual contract. After expiry of the minimum term, the contract may be terminated by either party in text form with three months' notice to the end of the respective contract period.

21.2 The right to terminate for good cause without notice shall remain unaffected. Good cause for Infinitas Security shall exist in particular in the event of material or repeated breaches by the Customer of essential contractual obligations, default in payment, or unlawful use of the services.

21.3 Following termination of the contract, Infinitas Security shall, at the Customer's request, make the data stored in the Customer's system available for download within a

reasonable period in a common machine-readable format, insofar as this has been contractually agreed or is customary and reasonable in the industry. After expiry of a reasonable retention or handover period, customer data shall be deleted or anonymized in accordance with the contractual and statutory requirements.

22. Special Provisions Regarding AI Support (CyberMind)

22.1 The AI assistance functions (CyberMind) generate content automatically on the basis of the information provided by the Customer as well as additional model information. The outputs may contain factual inaccuracies, omissions, or suggestions that are unsuitable for the specific individual case. The Customer remains responsible for carefully reviewing, validating, and assessing the AI outputs from a legal and professional perspective, and shall make decisions exclusively at its own responsibility. Use of the AI outputs is at the Customer's own risk, without prejudice to mandatory liability provisions under Section 14.

22.2 To the extent that the provision of the AI functionalities requires the processing or temporary transfer of content to subcontractors or infrastructure providers, this shall take place in accordance with Section 4 and Section 16 as well as any supplementary agreements.

23. Security and Compliance Notices

23.1 Infinitas Security operates CyberPilot using appropriate organizational and technical security measures. The Customer shall be obliged to implement its own appropriate security measures, in particular to maintain regular data backups, restrict access, manage permissions carefully, and report security incidents without undue delay.

23.2 The Customer shall ensure that the use of CyberPilot within its sphere of responsibility complies with all applicable laws, official requirements and internal compliance policies, including those relating to information security, data protection and retention obligations.

24. Final Provisions Regarding Contract Performance; Severability Clause

24.1 The laws of the Federal Republic of Germany shall apply.

24.2 The exclusive place of jurisdiction for all disputes arising out of or in connection with this contract shall be Munich.

24.3 Any side agreements, amendments and supplements to this contract must be made in writing. This shall also apply to any waiver of this written form requirement.

24.4 Should any provision of this contract be or become invalid or unenforceable, the validity of the remaining provisions shall remain unaffected. In place of the invalid or unenforceable provision, such valid provision shall be deemed agreed as comes closest to the economic purpose of the invalid provision. The same shall apply to any gaps in the contract.

Annex 1

DATA PROCESSING AGREEMENT PURSUANT TO ARTICLE 28 GDPR

ENGLISH CONVENIENCE TRANSLATION

1. Scope of Application

This Data Processing Agreement ("DPA") forms part of the GTC governing the use of the software-as-a-service platform "Infinitas CyberPilot", as well as any other services provided by Infinitas Security in connection therewith and any contracts concluded between Infinitas Security and the Customer, and specifies the parties' rights and obligations under data protection law pursuant to Article 28 GDPR.

2. Subject Matter, Nature, Scope and Purpose of the Processing

2.1 The description of the processing on behalf of the Customer (the "Engagement"), including the subject matter of the engagement, the scope, nature and purpose of the data processing, the categories of personal data and the categories of data subjects, is set out in the GTC in conjunction with Annex 1.

2.2 The term of this Agreement shall correspond to the term of the main agreement concluded together with the GTC.

3. Customer's Right to Issue Instructions

3.1 Infinitas Security shall process personal data within the scope of the Engagement exclusively in accordance with the provisions of this Agreement and the Customer's instructions, unless it is required to process such data otherwise under EU law or the law of an EU Member State to which the Customer is subject. In such case, the Customer shall inform Infinitas Security of those legal requirements, unless the relevant law prohibits such information on important grounds of public interest.

3.2 The Customer's right to issue instructions shall relate to the scope, nature and method of the data processing. If instructions amend, revoke or supplement the contractual arrangements, in particular those set out in the GTC and/or in Annex 1, such instructions shall be coordinated and documented jointly by the parties.

3.3 If necessary, the Customer may also issue instructions orally or by telephone. However, instructions issued orally or by telephone must be confirmed by the Customer without undue delay in written form, with email being sufficient. Irrespective of this, the Customer shall document all instructions issued by it.

3.4 Infinitas Security shall inform the Customer without undue delay if, in its opinion, an instruction issued by the Customer violates statutory provisions. Infinitas Security shall provide reasons for its view to an extent that enables the Customer to review the matter. In such case, Infinitas Security shall, after timely prior notice to the

Customer, be entitled to suspend execution of the instruction until the Customer has amended the instruction or the parties have concluded, within the framework of the applicable escalation procedure, that no breach of data protection law exists.

4. Support Obligations of Infinitas Security

4.1 Infinitas Security shall reasonably support the Customer in safeguarding the rights and satisfying the claims of data subjects, in particular with regard to the rectification, erasure and restriction of processing of personal data, as well as in providing information and data to data subjects, in particular by means of appropriate technical and organizational measures, and shall act in accordance with the Customer's instructions.

4.2 Infinitas Security shall support the Customer in carrying out a data protection impact assessment and, where required, in consulting the competent data protection supervisory authority.

4.3 If a data subject or a data protection supervisory authority contacts Infinitas Security directly in connection with the personal data processed under this Agreement, Infinitas Security shall inform the Customer thereof without undue delay and coordinate all further steps with the Customer. Infinitas Security may provide information to data subjects only upon prior instruction by the Customer.

5. Third-Country Transfers, Data Transfers

5.1 The processing of personal data shall take place exclusively within the territory of the Federal Republic of Germany, a Member State of the European Union (EU), or another contracting state to the Agreement on the European Economic Area (EEA). Any transfer to a third country, including any transfer to or access from a third country, shall only be permissible if the additional requirements under Articles 44 et seq. GDPR for transfers to third countries are satisfied.

5.2 If a subcontractor of Infinitas Security is to be engaged that is established in a third country, the specific provisions set out in Section 5 shall apply in addition to the requirements of this Section 5.

6. Confidentiality

Infinitas Security undertakes to maintain confidentiality when processing the Customer's personal data. Infinitas Security warrants that it shall make the employees engaged in the performance of the services, as well as any other persons under Infinitas Security's authority, familiar with the data protection provisions applicable to them and that such persons have committed themselves in writing to confidentiality or are subject to an appropriate statutory duty of confidentiality. Infinitas Security shall monitor compliance with data protection requirements. Infinitas Security may provide information to third parties or to the data subject only with the Customer's prior written consent.

7. Security of Processing

7.1 Infinitas Security shall ensure that appropriate technical and organizational measures are implemented so that processing is carried out in compliance with the requirements of the GDPR and the protection of the rights of the data subjects is ensured. Infinitas Security shall provide an overview of the implemented technical and organizational measures upon request.

7.2 Infinitas Security shall regularly review the technical and organizational measures in order to ensure that processing within its area of responsibility is carried out in compliance with the requirements of applicable data protection law and that the protection of the rights of the data subjects is ensured.

7.3 Infinitas Security may adapt the technical and organizational measures during the term of the engagement due to technical and organizational developments without the Customer's consent. The adapted measures must at least correspond to the previous level of security. Changes to the technical and organizational measures shall be documented by Infinitas Security in the aforementioned overview.

8. Information Obligations of Infinitas Security; Personal Data Breaches

8.1 Infinitas Security shall inform the Customer without undue delay of any processing of personal data outside the scope defined in this Agreement, as well as of any breaches of the applicable statutory data protection provisions or of the requirements set out in this Agreement. This shall apply in particular in the event of disruptions or other impairments affecting the data processing systems used by Infinitas Security.

8.2 Infinitas Security shall, without undue delay, take all reasonable measures to minimize and eliminate any risks to the confidentiality, integrity and/or availability of the personal data processed under this Agreement, to secure the data, and to prevent any possible adverse consequences for data subjects or limit such consequences as far as possible.

8.3 In the event of a personal data breach within the meaning of Article 4 no. 12 GDPR, Infinitas Security shall reasonably support the Customer in fulfilling its statutory notification and information obligations. For this purpose, Infinitas Security shall provide the Customer without undue delay with the necessary information regarding the personal data breach, insofar as such information is available to it. If and to the extent that such information cannot be provided at the same time, Infinitas Security may provide the information in stages without undue further delay.

8.4 The provisions of this Section 8 shall apply accordingly to incidents occurring in processes carried out by subcontractors of Infinitas Security.

9. Customer's Audit Rights

9.1 The Customer shall be entitled to verify, to a reasonable extent, compliance with the provisions set out in this Agreement and with the applicable data protection

requirements, insofar as they relate to the processing of the Customer's data. As evidence, Infinitas Security may provide current and meaningful attestations, reports or excerpts from reports issued by independent bodies, for example auditors, internal audit, the data protection officer, the IT security department, data protection auditors or quality auditors, proof of compliance with approved codes of conduct pursuant to Article 40 GDPR, or suitable certification pursuant to Article 42 GDPR. The Customer's own right to audit and verify shall remain unaffected.

9.2 If there is good cause, the Customer shall be entitled to enter the business premises of Infinitas Security and carry out on-site inspections there. Good cause shall exist, for example, if the evidence provided by Infinitas Security is insufficient or if, based on such evidence or for other reasons, the Customer has justified concerns that the requirements of applicable data protection law are not being complied with by Infinitas Security and/or that Infinitas Security is in breach of this Agreement. The Customer shall carry out on-site inspections during the normal business hours of Infinitas Security and shall announce such inspections in due time in advance and coordinate them with Infinitas Security. Infinitas Security shall make available to the Customer all information required by the Customer for the audit. In doing so, the Customer shall give due consideration to business operations and the legitimate confidentiality interests of Infinitas Security.

9.3 The Customer shall be entitled to carry out the audit measures under this Section 9 itself or through an authorized representative bound to confidentiality. Infinitas Security may object to the performance of audit measures by such representative if there is good cause. Good cause shall exist, for example, if Infinitas Security is in a competitive relationship with the representative.

10. Subcontractors

10.1 Infinitas Security uses subcontractors for carrying out the processing on behalf of the Customer. An overview of the subcontractors used by Infinitas Security is contained in Annex 1. The Customer hereby consents to the use of the subcontractors named therein at the time of conclusion of the contract. Infinitas Security shall also be entitled to engage additional subcontractors or replace existing subcontractors unless the Customer objects to such changes within a reasonable period of time. Infinitas Security shall inform the Customer in due time of any intended engagement or replacement of subcontractors.

10.2 Infinitas Security shall contractually ensure that the data protection obligations set out in this Agreement are imposed on the subcontractors in a corresponding manner so that the principles of Article 28(3) GDPR are preserved. This shall also include the implementation of appropriate technical and organizational measures. If a subcontractor fails to comply with its data protection obligations, Infinitas Security shall remain liable to the Customer for compliance with the obligations of that subcontractor.

10.3 For the avoidance of doubt, the parties agree that subcontracting relationships within the meaning of this Agreement are those services that directly relate to the provision of the agreed services within the framework of the cooperation under the main contract. This does not include ancillary services used by Infinitas Security, such as telecommunications services, postal or transport services, maintenance and user support, or the disposal of data carriers. Where necessary, however, Infinitas Security shall also in such cases implement appropriate and legally compliant arrangements.

10.4 Where subcontractors are engaged whose registered seat is outside the EU or the EEA, Infinitas Security shall ensure that the transfer of the Customer's personal data to such subcontractors complies with Articles 44 et seq. GDPR. Unless an adequacy decision within the meaning of Article 45 GDPR exists for the relevant third country, Infinitas Security shall ensure that a data protection agreement pursuant to Article 46(2)(c) or (d) GDPR, namely the Standard Contractual Clauses, is concluded with such subcontractors.

11. Deletion and Return of Personal Data

The deletion and return of personal data processed on behalf of the Customer shall be governed by the provisions of the main contract.

12. Term

This Agreement is concluded for the duration of the main contract. To the extent that Infinitas Security continues to process the Customer's personal data beyond the end of the engagement, the provisions of this Agreement shall continue to apply.

Annexes to the Agreement

Annex 1 – Description of the Processing and Subcontractors

Description of the subject matter, nature and purpose of the processing

Provision, hosting and operation of the SaaS platform “Infinitas CyberPilot” for the Customer, including user management, authentication, authorization management, support and, where used by the Customer, the provision of AI-supported functionalities. The processing includes, in particular, the collection, storage, organization, provision, use, transfer in the course of service delivery, and deletion of personal data. The purpose of the processing is to enable the use of the platform for the planning, management and tracking of information security measures within the Customer’s organization.

Categories of data subjects

- Employees of the Customer
- Other users of the platform created by the Customer, in particular administrators and contact persons

Categories of personal data

- Name
- Business email address
- Job title / function
- Area of responsibility
- User role / authorization role
- Authentication and access information

Special categories of personal data

- None

Subcontractors:

Name	Function
Microsoft Ireland Operations Limited	Cloud hosting, infrastructure and the provision of AI inference services via Azure, including Azure OpenAI and/or Azure Direct Models in Microsoft Foundry.
Okta Inc. (“Okta”, "Auth0")	Authentication and identity management for user access to Infinitas CyberPilot.

Stripe Payments Europe, Limited	Payment processing and provision of payment services for paid services of Infinitas CyberPilot.