Service Description for the Product “cyan Guard 360” and Data Processing Agreement (“DPA”)

Version: 2.0
Status: April 1, 2026

Thank you for using the product!

Preamble

cyan Security Group GmbH is an internationally active technology company based in Vienna, Austria, specializing in cloud-based cybersecurity solutions. cyan develops and operates innovative security products designed to protect networks, end devices, and digital identities, with a particular focus on business customers in B2B and B2B2C environments.

The product “cyan Guard 360” is a cloud-based DNS security solution designed to effectively protect companies against cyber threats such as phishing, malware, fraudulent domains, and malicious content. The solution combines preventive security mechanisms with centralized administration via a web-based dashboard, thereby enabling effective, scalable, and location-independent protection of networks and end devices.

This Service Description is intended to transparently describe the functional scope, technical framework conditions, and legal classification of the use of “cyan Guard 360.” It supplements the respective contractual arrangements and, where applicable, forms the basis for the technical provision of services by cyan.

Gender Note

For reasons of readability, this Service Description predominantly uses the masculine or a gender-neutral form. All personal designations apply equally to all genders.

1. Definitions

For the purposes of this Service Description, the following definitions shall apply:

“cyan” means cyan Security Group GmbH, company registration number FN 416622 f, with its registered office at Wiedner Gürtel 13, 1100 Vienna, Austria, as well as all affiliated companies (“Affiliates”) that directly or indirectly control cyan, are controlled by cyan, or are under common control with cyan.

“Contract” means the contract for the purchase and use of the Product, which, where applicable and depending on the relevant sales and contract model that is concluded
(i) between the End Customer and cyan, or
(ii) between the End Customer and an authorized Sales Partner or Reseller.

“Dashboard” means the web-based management interface for loggin, configuring, administering, and evaluating the Product.

“**Direct Customer Model**” means a contractual model under which a direct usage or contractual relationship regarding the Product is established between the End Customer and cyan. This includes both the model based on electronic acceptance in the Dashboard pursuant to Section 2.3(a) and the model involving a direct contractual and payment relationship pursuant to Section 2.3(b).

“End Customer” means a business customer (in particular a small or medium-sized business, “SMB”) within the meaning of Section 2.2 that purchases and uses the Product for purposes related to its professional or business activity.

“Product” means the cloud-based DNS security solution “cyan Guard 360,” including all associated applications, features, updates, further developments, and documentation.

“Reseller” means a Sales Partner that distributes the Product to End Customers in its own name and for its own account.

“Sales Partner” means a company authorized by cyan to market the Product to End Customers under a sales model and to handle billing and payment processing vis-à-vis the End Customer.

“Step-in Case” means a case in which cyan, at its own discretion, offers the End Customer continuation of the use of the Product under a new usage or contractual relationship (see Section 9.2).

“User” means a natural person authorized by the End Customer to use the Product in the course of activities for the End Customer, in particular employees, administrators, or other agents of the End Customer.

“White-Label Model” means a distribution model in which the Product is offered under the brand of an authorized Sales Partner.

2. Scope of Application and Contract Models

2.1 Scope This Service Description governs the functional scope and use of the Product. It applies exclusively to the contract models described in Section 2.3 lit. a) to c), in which a contractual usage relationship for the Product is established between the End Customer and cyan. In White-Label and Reseller models pursuant to Section 2.3 lit. d) and e), this Service Description serves solely as the service basis between cyan and the respective Reseller or White-Label provider and does not form part of the End Customer contract.

2.2 End Customer Group (B2B) For the purposes of this Service Description, an End Customer is exclusively a business customer within the meaning of the Austrian Commercial Code (Unternehmensgesetzbuch). Purchase of the Product by consumers is excluded. No contract for the Product shall be concluded with consumers.

2.3 Contract Models Depending on the relevant sales and contract model, the Product is offered in the following variants:

a) Direct customer model with use based on the Service Description (consent via opt-in) The Product is offered under the “cyan” brand. The End Customer’s use of the Product is based on this Service Description and the Data Processing Agreement integrated therein, which is accepted by the End Customer by electronic acceptance (checkbox confirmation) in the Dashboard. The Service Description establishes an independent, legally binding usage relationship between the End Customer and cyan, governing the technical terms of use, rights and obligations, and the data protection-related processing. Billing and payment processing for the Product are carried out exclusively through an authorized Sales Partner and are not part of the legal relationship between the End Customer and cyan.

b) Direct customer model with direct contractual and payment relationship The Product is offered under the “cyan” brand. The contract for the use of the Product is concluded between the End Customer and cyan. The contractual relationship relating to billing and payment processing is established directly between the End Customer and cyan. This Service Description forms the binding basis for the use of the Product and the product-related service provision by cyan.

c) Contract takeover by cyan (Step-in Case) If, in the event of insolvency, termination of contract, or loss of distribution authorization of a Sales Partner, cyan is entitled to assume over the existing contractual relationship with the End Customer (“Step-in Case”), further service provision shall from the time of such contract takeover be based on this Service Description.

d) White-Label Model The Product is offered under the brand of an authorized Sales Partner. The visual design (e.g. logo, colors, product name) may differ from the appearance of the “cyan” brand. The End Customer concludes the contract for the Product exclusively with the respective Sales Partner; in this case, cyan is not a contractual partner of the End Customer.

e) Reseller Model The Product is distributed under the “cyan” brand and displayed accordingly in the Dashboard. The Reseller distributes the Product to the End Customer in its own name and for its own account. The contract for the Product is concluded exclusively between the End Customer and the Reseller. In this case, cyan is not a contractual partner of the End Customer.

3. Subject Matter of the Contract and Scope of Services

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

3.1. cyan shall technically provide the Product to the End Customer on the basis of this Service Description. cyan is responsible for the operation, security, technical provision, and further development of the Product.

3.2. The Product is offered exclusively to customers based in Germany, Austria, and Switzerland (DACH region). If the Product is used outside these countries, cyan cannot guarantee the functionality, availability, or legal compliance of the Product. The End Customer is obliged to independently inform itself in advance about the legal framework, technical feasibility, and any regulatory requirements of the relevant country of use and to review these accordingly.

3.3. If the End Customer uses the Product in sectors qualifying as critical infrastructure within the meaning of the applicable national or Union law provisions (in particular the NIS 2 Directive and its national implementing acts), such use shall take place solely at the End Customer's own responsibility. In such cases, cyan gives neither warranty nor guarantee that the Product fulfills all sector-specific, regulatory, or supervisory requirements, nor any warranty or guarantee regarding the suitability, stability, or legal compliance of the Product for use in critical infrastructure sectors. The End Customer is obliged to conduct its own risk assessment before using the Product in such sectors.

3.4. Any deviating, conflicting, or supplementary general terms and conditions of the End Customer shall not become part of the contract.

3.5. cyan undertakes not to make any materially adverse changes to the functions or scope of services of the Product during the contract term. Changes are considered material if they permanently restrict the core purpose of the DNS Security Service. Non-material changes remain unaffected. These include, in particular, security-related updates, bug fixes, technical optimizations, and adjustments required to maintain the security, stability, performance, or compatibility of the Product. Amendments to the Service Description shall be made in accordance with Section 4.

4. Acceptance of the Service Description and Amendments

4.1. This Service Description applies exclusively to contractual relationships pursuant to Section 2.3 lit. a), b), and c).

4.2. This Service Description shall be deemed agreed once the End Customer accepts it in the Dashboard
(i) prior to first use, or
(ii) again in the event of a materially adverse change.

4.3. The current version of this Service Description and of the Data Processing Agreement is available in the Dashboard.

4.4. In White-Label/Reseller models (Section 2.3 lit. d) and e)), this Service Description does not form part of the End Customer contract. In White-Label/Reseller models, technical confirmation may be given in the Dashboard without this Service Description becoming part of the End Customer contract.

4.5. cyan is entitled to amend this Service Description without further consent of the End Customer to the extent necessary to maintain security, stability, performance, or compatibility (e.g. security updates, bug fixes, technical optimizations).

4.6. If the End Customer rejects a materially adverse change, it shall be entitled to terminate the usage relationship or, where applicable, the contract for the use of the Product with effect as of the date on which the change is intended to take effect. In the contract model pursuant to Section 2.3 lit. a), such termination affects only the usage relationship between the End Customer and cyan. Payment and billing matters shall be resolved exclusively with the respective authorized Sales Partner. In this case, cyan shall not be responsible for billing or repayment processing. Termination must be declared no later than by that date. Any notice periods and settlement modalities shall be governed by the relevant contractual or usage model pursuant to Section 2.3 and, where existing, by the underlying contract.

5. Technical Product Description

5.1. The Product is offered exclusively as a cloud-based DNS security solution that filters the DNS traffic of the End Customer's corporate network in order to block security risks and inappropriate content. No

installation of software or hardware in the customer's network is required for this protection. A configuration on the customer's router/gateway is required to redirect DNS traffic to cyan. The End Customer must be able to carry out this configuration.

5.2. In addition, protection may be extended through applications that can also be used outside the corporate network on mobile devices (e.g. smartphones using iOS or Android) as well as on Windows and macOS devices. The applications support common operating systems in their respective current versions. Certain functions may be restricted depending on device configuration, system environment, or the parallel use of other security, network, or VPN services. Compatibility with such third-party applications is not warranted.

5.3. The End Customer is granted a non-exclusive right to use the Product limited to the term of the contract. All intellectual property rights in the Product, including software, trademarks, content, designs, and documentation, shall remain exclusively with cyan. The End Customer is granted only a limited, non-transferable right of use. The End Customer is not entitled to copy, modify, translate, decompile, disassemble, reverse engineer, further develop, or integrate the Product, in whole or in part, into other products or services. No part of the Product becomes the property of the End Customer by virtue of its use, branding, or the sales model. Use of cyan's brand, logo, or other distinguishing marks by the End Customer for advertising, reference, or presentation purposes is permitted only with cyan's prior express written consent.

5.4. During the contract term, the End Customer shall have access to the current versions of the applications. cyan shall be entitled to carry out technical security and stability updates, bug fixes, and technical adjustments and to cease support for older versions of the applications or make updates mandatory where necessary for security, stability, or compatibility reasons. Such technical measures shall not constitute a change to the main contractual obligations and shall not give rise to any extraordinary termination right.

5.5. After activation/provisioning, the customer receives access to a Dashboard for managing devices, relevant security settings and security policies, and for viewing reports.

5.6. cyan shall provide the necessary technical information, documentation, and interfaces to the relevant authorized Sales Partner to the extent required for integration, provision, and use of the Product. If cyan is the direct contractual partner of the End Customer, cyan shall provide such information and interfaces directly to the End Customer.

6. Obligations of the End Customer

6.1. The End Customer is obliged to comply with the technical requirements provided by cyan (see in particular Section 5) and to ensure correct system configuration. Further product information is available at: https://cyanguard.com/

6.2. If cyan is not the End Customer's direct contractual partner, the End Customer shall contact its Sales Partner exclusively with regard to activation-related questions.

6.3. If cyan is the End Customer's direct contractual partner, initial provisioning and support shall be provided in accordance with the contractually agreed provisions and, supplementarily, in accordance with this Service Description.

6.4. If the End Customer breaches the obligations set out in this Service Description or misuses the Product, in particular for the unlawful monitoring of employees or third parties, cyan shall be entitled to technically block the use of the Product in whole or in part or to terminate the contract for good cause with immediate effect.

7. Availability, Warranty, and Liability

7.1. cyan's Product offers protection mechanisms against phishing, malware, and identity theft. However, it is expressly noted that no security system can guarantee the complete detection or prevention of all threats. cyan therefore does not guarantee the complete detection or prevention of all cyber threats.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

7.2. cyan monitors the cloud infrastructure 24x7x365 and strives for an average Product availability of 99.5% per year. Maintenance work that may result in Product downtime shall be carried out during night hours and announced in advance by email to minimize impact as far as possible.

7.3. Maintenance windows, in particular security-related updates, may be announced in advance by email where technically and organizationally feasible. Unplanned maintenance work or outages due to force majeure or external factors shall not constitute a defect.

7.4. The Product is used at the End Customer's own risk. cyan does not warrant uninterrupted availability or error-free operation of the Product. Technical limitations, false positives, or the failure to detect certain threats shall not constitute a defect within the meaning of statutory warranty law.

7.5. cyan shall not be liable for damages caused by phishing attacks, malware infections, identity theft, or other cyberattacks that were not detected or prevented, unless such damages are demonstrably and directly attributable to gross negligence or intent on the part of cyan or its legal representatives. The burden of proof lies with the End Customer.

7.6. To the extent permitted by law, further claims, in particular claims for damages due to loss of profit, data loss, costs associated with business interruption, or other consequential damages, shall be excluded.

7.7. In particular, no liability shall be assumed for business interruption costs, restoration costs after attacks, or other indirect damages.

7.8. In any event, the maximum aggregate liability per claim and event giving rise to liability shall be limited to 100% of the End Customer's annual subscription fee. Claims for damages shall become time-barred no later than six months after knowledge of the damage and the liable party.

8. Data Protection and Confidentiality

8.1. The processing of personal data in connection with the use of the Product shall be carried out in compliance with the General Data Protection Regulation (GDPR).

8.2. To the extent cyan processes personal data on behalf of the End Customer, such processing shall be carried out exclusively on the basis of processing under Article 28 GDPR (Data Processing Agreement, hereinafter referred to as "DPA"). The DPA forms an integral part of this Service Description. It applies exclusively to contractual relationships pursuant to Section 2.3 lit. a), b), and c) and comes into effect upon acceptance of this Service Description.

8.3. In White-Label and Reseller models (Section 2.3 lit. d) and e)), cyan processes personal data exclusively as a sub-processor within the meaning of Article 28 GDPR. In these cases, the data processing agreement pursuant to Article 28 GDPR exists exclusively between the End Customer and the respective Reseller or White-Label provider. cyan shall conclude a DPA pursuant to Article 28 GDPR with the respective Reseller or White-Label provider governing the appointment of cyan as sub-processor.

8.4. The privacy notice from cyan is available at https://cyanguard.com/datenschutz/ provides information on the processing of personal data in connection with visits to the website. The processing of personal data in connection with the End Customer's use of the Product shall be governed exclusively by the relevant DPA pursuant to Article 28 GDPR.

8.5. The End Customer itself acts as controller within the meaning of the GDPR, it shall be responsible for complying with the information obligations under Articles 13 and 14 GDPR vis-à-vis data subjects.

8.6. cyan anonymizes or aggregates data and such data no longer contains any personal reference, further use of such data shall fall outside the scope of the GDPR.

8.7. To the extent personal data is still processed in the context of analysis, product improvement, or quality assurance, such processing shall not be carried out on behalf of the End Customer but under cyan's own responsibility as controller within the meaning of Article 4(7) GDPR. The specific processing activities under cyan's own responsibility are set out in Annex V of the DPA.

9. Contract Term, Termination, and Contract Takeover (Step-in Case)

9.1. Contract term, notice periods, and other termination provisions shall be governed exclusively by the contract concluded between the End Customer and the authorized Sales Partner or—where applicable—directly with cyan. This Service Description does not govern commercial terms or provisions relating to contract duration.

9.2. Direct customer model / Step-in Case: In a Step-in Case, cyan shall be entitled, but not obliged, to offer the End Customer a new usage or contractual relationship for the Product. There shall be no automatic transfer of the existing contractual relationship. In particular, cyan shall not assume any obligations, payment arrears, liabilities, or other obligations of the Sales Partner arising prior to the Step-in date. Continuation of the service provision shall take place exclusively on the basis of the terms defined by cyan.

9.3. White-Label and Reseller models: Contract term, contract termination, and billing modalities are governed by the contract between the End Customer and the Sales Partner. In such cases, the Sales Partner's general terms and conditions shall apply.

10. Support and Incident Handling

10.1. Support for the Product is generally provided across several support levels (first-level, second-level, and third-level support).

10.2. First- and second-level support (in particular inquiries relating to order, activation, setup, access credentials, user administration, billing, and general application questions) shall be provided, depending on the respective sales and contract model, either
(i) by the authorized Sales Partner, or
(ii) by cyan itself, if and to the extent expressly agreed in the relevant contractual relationship.

10.3. Third-level support (in particular analysis and remediation of complex technical incidents, fault analysis at system or infrastructure level, and security-related incidents) shall be provided, depending on the respective sales and contract model, either
(i) by the authorized Sales Partner, or
(ii) by cyan itself, if and to the extent expressly agreed in the relevant contractual relationship.

10.4. This Service Description does not establish any specific service levels, response times, restoration times, or availability commitments. Such obligations shall apply only if expressly agreed in a separate service level agreement ("SLA").

10.5. The End Customer shall report malfunctions, security-related incidents, or functional impairments of the Product without undue delay via the designated support channels. The specific reporting channels and response times shall be governed by the relevant contractual relationship or a separate SLA.

11. Final Provisions

11.1. The laws of the Republic of Austria shall apply, excluding the UN Convention on Contracts for the International Sale of Goods.

11.2. In the event of discrepancies, inconsistencies or questions of interpretation between the German and English language versions, the German version shall prevail.

11.3. For all disputes arising out of or in connection with the usage relationship or, where applicable, the contract for the use of the Product pursuant to Section 2.3 lit. a) to c), the court with subject-matter jurisdiction in Vienna shall have exclusive jurisdiction.

11.4. Should any provision of this Service Description be or become invalid, the validity of the remaining provisions shall remain unaffected.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

DATA PROCESSING AGREEMENT ("DPA")

between

the **Controller**, being the End Customer using the product "cyan Guard 360" within the framework of a contractual relationship pursuant to the Service Description. The Controller's details shall result from the respective ordering process or the underlying contractual relationship.

(hereinafter the **"Controller"**)

and

cyan Security Group GmbH
(FN 416622f)
ICON Tower 24
Wiedner Gürtel 13
A-1100 Vienna

(hereinafter the **"Processor"** or **"cyan"**)

together also referred to as the **"Parties."**

PREAMBLE

This DPA forms part of the use of the product "cyan Guard 360" and is concluded directly between the Controller and the Processor.

This DPA is an integral part of the Service Description.

This DPA applies to the following contractual relationships:

(i) The Controller uses the product "cyan Guard 360" within the framework of a contractual relationship pursuant to Section 2.3 lit. a) on the basis of a usage relationship between the Controller and cyan established by electronic acceptance; any billing/payment processing via authorized Sales Partners is not part of this legal relationship.

(ii) The Controller uses the product "cyan Guard 360" within the framework of a contractual relationship pursuant to Section 2.3 lit. b) of the Service Description, under which a contract is concluded directly between the Controller and cyan.

(iii) In a Step-in Case pursuant to Section 2.3 lit. c) of the Service Description, cyan enters into a contractual relationship for the use of the Product; from the time of such Step-in, this DPA shall apply to the processing of personal data by cyan in connection with the continued provision of the Product.

(iv) White-Label and Reseller models pursuant to Section 2.3 lit. d) and e) of the Service Description are expressly excluded from the scope of this DPA.

This DPA applies exclusively to entrepreneurs within the meaning of the Austrian Commercial Code (B2B). Use by consumers within the meaning of EU consumer law is excluded.

The Controller is responsible for fulfilling all data protection obligations incumbent upon it as controller, in particular the information obligations pursuant to Articles 13 and 14 GDPR and—where applicable—for obtaining and documenting the necessary legal bases and consents.

The European Commission has adopted standard contractual clauses for compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the "GDPR").

The Parties agree that these standard contractual clauses shall apply (embedded here for clarification) as specified in Annexes I to VI.

This DPA is structured as follows:

1. Standard Contractual Clauses of the European Commission
2. Annex I: List of Parties
3. Annex II: Description of Processing
4. Annex III: Technical and Organisational Measures, including measures to ensure data security
5. Annex IV: List of Sub-processors
6. Annex V: Processing under Own Responsibility
7. Annex VI: Additional Provisions

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope
a) These standard contractual clauses (the "Clauses") are intended to ensure compliance with Article 28(3) and (4) GDPR.
b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) GDPR.
c) These Clauses apply to the processing of personal data as specified in Annex II.
d) Annexes I to VI form an integral part of these Clauses.
e) These Clauses are without prejudice to the obligations to which the Controller is subject under the GDPR.
f) These Clauses do not by themselves ensure compliance with obligations relating to international data transfers under Chapter V GDPR.

Clause 2

Immutability of the Clauses
a) The Parties undertake not to modify the Clauses, except to supplement or update the information set out in the Annexes.
b) This does not prevent the Parties from incorporating these Clauses into a broader contract or adding further clauses or additional safeguards, provided that these do not directly or indirectly contradict the Clauses or prejudice the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation
a) Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in these Clauses, those terms shall have the same meaning as in the relevant Regulation.
b) These Clauses shall be interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
c) These Clauses shall not be interpreted in a manner that conflicts with the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or that prejudices the fundamental rights or freedoms of data subjects.

Clause 4

Hierarchy
In the event of a conflict between these Clauses and the provisions of related agreements existing between the Parties or entered into subsequently, these Clauses shall prevail.

In the event of a conflict between the Service Description and this DPA, the provisions of this DPA shall prevail insofar as they relate to the processing of personal data.

Clause 5 – Optional

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

Docking clause
a) An entity that is not a Party to these Clauses may, with the agreement of all Parties, accede to these Clauses at any time as a controller or processor by completing the Annexes and signing Annex I.
b) Once it has completed and signed the Annexes referred to in point (a), the acceding entity shall be treated as a Party to these Clauses and shall have the rights and obligations of a controller or processor, in accordance with its designation in Annex I.
c) The acceding entity shall have no rights or obligations arising from these Clauses for the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing
The details of the processing operations, in particular the categories of personal data and the purposes for which personal data are processed on behalf of the Controller, are set out in Annex II.

Clause 7

Obligations of the Parties

7.1 Instructions

a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In such case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest. The Controller may issue further instructions throughout the duration of the processing. Such instructions shall always be documented.

b) The Processor shall immediately inform the Controller if, in its opinion, instructions given by the Controller infringe Regulation (EU) 2016/679, Regulation (EU) 2018/1725, or applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The Processor shall process the personal data only for the specific purpose or purposes set out in Annex II, unless it receives further instructions from the Controller.

7.3 Duration of processing of personal data

The data shall be processed by the Processor only for the duration specified in Annex II.

7.4 Security of processing

a) The Processor shall implement at least the technical and organisational measures set out in Annex III in order to ensure the security of the personal data. This includes protecting the data against a personal data breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, and the risks for data subjects.

b) The Processor shall grant its personnel access to the personal data undergoing processing only to the extent strictly necessary for implementing, managing, and monitoring the contract. The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

Where processing involves special categories of data or personal data relating to criminal convictions and offences, the Processor shall apply specific restrictions and/or additional safeguards appropriate to the nature of the data and the associated risks.

7.6 Documentation and compliance

a) The Parties must be able to demonstrate compliance with these Clauses.
b) The Processor shall deal promptly and adequately with inquiries from the Controller regarding the processing of data in accordance with these Clauses.
c) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and arising directly from the GDPR and/or Regulation (EU) 2018/1725. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these Clauses at reasonable intervals or where there are indications of non-compliance. In deciding on a review or audit, the Controller may take into account relevant certifications of the Processor.
d) The Controller may conduct the audit itself or mandate an independent auditor. Audits may also include inspections at the Processor's premises or physical facilities and shall, where appropriate, be carried out with reasonable notice.
e) The Parties shall make the information referred to in this clause, including audit results, available to the competent supervisory authority or authorities upon request.

7.7 Use of sub-processors

a) The Processor has the general authorization of the Controller to engage sub-processors listed in an agreed list. The Processor shall inform the Controller at least 14 days in advance of any intended changes to that list through the addition or replacement of sub-processors. Such notification shall be made in an appropriate electronic form, in particular by updating the list of sub-processors made available in the Dashboard or on a dedicated information page. The Processor shall provide the Controller with the information necessary to enable the Controller to exercise its right to object.

b) Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, such engagement shall be governed by a contract imposing on the sub-processor, in substance, the same data protection obligations as those imposed on the Processor under these Clauses. The Processor shall ensure that the sub-processor complies with the obligations to which the Processor is subject under these Clauses and the GDPR.

c) The Processor shall provide the Controller, upon request, with a copy of such sub-processing agreement and any subsequent amendments thereto. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may redact the text of the agreement prior to sharing it.

d) The Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations under its contract with the Processor. The Processor shall notify the Controller where the sub-processor fails to fulfil its contractual obligations.

e) The Processor shall agree a third-party beneficiary clause with the sub-processor whereby—in the event that the Processor has factually or legally ceased to exist or has become insolvent—the Controller shall have the right to terminate the sub-processing contract and to instruct the sub-processor to delete or return the personal data.

7.8 International transfers

a) Any transfer of data by the Processor to a third country or an international organisation shall be made only on the basis of documented instructions from the Controller or in order to comply with a specific requirement under Union or Member State law to which the Processor is subject, and shall take place in compliance with Chapter V GDPR or Regulation (EU) 2018/1725, as applicable.

b) The Controller agrees that where the Processor engages a sub-processor in accordance with Clause 7.7 and the processing activities involve a transfer of personal data within the meaning of Chapter V GDPR, the Processor and the sub-processor may ensure compliance with Chapter V GDPR by using standard contractual clauses adopted by the European Commission pursuant to Article 46(2) GDPR, provided that the conditions for the use of such clauses are met.

Clause 8

Assistance to the Controller
a) The Processor shall promptly inform the Controller of any request it has received from the data subject. It shall not respond to such request itself unless authorized to do so by the Controller.
b) Taking into account the nature of the processing, the Processor shall assist the Controller in fulfilling its obligation to respond to requests from data subjects exercising their rights. In fulfilling its obligations under points (a) and (b), the Processor shall comply with the Controller's instructions.
c) In addition to the Processor's obligation to assist the Controller pursuant to Clause 8(b), the Processor shall further assist the Controller, taking into account the nature of processing and the information available to the Processor, in ensuring compliance with the following obligations:

1. carrying out a data protection impact assessment where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2. consulting the competent supervisory authority or authorities prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

3. ensuring that personal data is accurate and kept up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

4. compliance with Article 32 GDPR.
   d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this clause as well as the scope and extent of the assistance required.

Clause 9

Notification of personal data breaches
In the event of a personal data breach, the Processor shall cooperate with and assist the Controller in complying with its obligations under Articles 33 and 34 GDPR or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725, taking into account the nature of processing and the information available to the Processor.

9.1 Personal data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller as follows:
a) in notifying the competent supervisory authority or authorities of the personal data breach without undue delay after the Controller becomes aware of it, where relevant;
b) in obtaining the information to be included in the Controller's notification under Article 33(3) GDPR;
c) in complying with the obligation under Article 34 GDPR to communicate the personal data breach to the data subject without undue delay where such breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Personal data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after becoming aware of the breach. Such notification shall contain at least:
a) a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects concerned and data records concerned;
b) the contact details of a contact point from whom more information may be obtained;
c) the likely consequences of the breach and the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects.

If not all such information can be provided at the same time, the initial notification shall contain the information then available, and further information shall be provided without undue delay as soon as it becomes available.

The Parties shall set out in Annex III any other elements to be provided by the Processor when assisting the Controller in complying with Articles 33 and 34 GDPR.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

a) Without prejudice to the GDPR and/or Regulation (EU) 2018/1725, where the Processor is in breach of its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The Processor shall promptly inform the Controller if it is unable to comply with these Clauses for any reason.

b) The Controller shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where:

1. the Controller has suspended the processing of personal data by the Processor pursuant to point (a) and compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

2. the Processor is in substantial or persistent breach of these Clauses or its obligations under the GDPR and/or Regulation (EU) 2018/1725;

3. the Processor fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses, the GDPR and/or Regulation (EU) 2018/1725.

4. The Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where the Controller insists on compliance with instructions that, after having been informed by the Processor that such instructions infringe applicable legal requirements pursuant to Clause 7.1(b), remain unlawful.

5. Following termination of the contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or return all personal data to the Controller and delete existing copies, unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

ANNEX I

LIST OF PARTIES

The Controller:
The Controller's details (company, address, contact person) shall be automatically taken from the ordering process.

The Processor:
cyan Security Group GmbH
ICON Tower 24
Wiedner Gürtel 13
A-1100 Vienna
privacy@cyansecurity.com

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

ANNEX II

DESCRIPTION OF PROCESSING

a)	Categories of data subjects whose personal data is processed:	Employees and Users of End-Customer
b)	Categries of personal data processed:	IP addresses, Network data (DNS traffic), domains Log files (date and time of access, referrer URL, target URL, type and version of end device, browser information) In the event of additional use of email monitoring: Email addresses Data processed in the context of support (e.g. telephone number, email address, technical error descriptions, reports, evaluations, other text and image files, and ticket content including processing; 'support data') Customer ID, line ID and configuration settings Amount of data transferred Location of the radio cell
c)	Sensitive data (if applicable) processed and applied restrictions or safeguards that fully take into consideration the nature oft he data and the risks involved:	n/a
d)	Nature of the processing:	DNS traffic is redirected to the processor by changing the configuration on the controller's router/gateway. Optional mobile apps on employees' devices redirect DNS traffic in non-company networks to the processor. DNS traffic is checked for vulnerabilities and blocked/filtered if necessary. Optional mobile apps implement an anti-virus module that checks files on the end device for malicious code. The signatures for this anti-virus module are downloaded via the systems of a sub-processor.
e)	Purpose(s) for which the personal data is processed on behalf of the Processor:	Filtering of DNS traffic on the controller's company network in order to block security risks and inappropriate content Creation of statistical evaluations for the controller Support data and log files are processed for 3rd Level support Periodic checking of data leaks
f)	Duration of the processing:	The duration of the processing or the DPA shall be determined based on the provisions of the Main Agreement.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

ANNEX III

TECHNICAL AND ORGANISATIONAL MEASURES, INCLUDING MEASURES TO ENSURE DATA SECURITY

	Requirement	Measures implemented
a)	Organization	**Responsibility** • cyan provides a CISO who is responsible for the design, coordination, and monitoring of IT security guidelines. • cyan implements an ISMS (Information Security Management System) that is certified according to the ISO27001 standard. • cyan's CISO reviews the IT security guidelines and all technical and organizational measures every 12 months in order to implement improvements where necessary. **Guidelines** • cyan has implemented guidelines that define security measures and guarantee the responsibilities of employees who have access to customer data. **Risk management** • cyan conducts ongoing risk analyses as part of the ISMS. **Confidentiality** • Employees who have access to customer data are trained in confidentiality and ensure that it is maintained. **Training** • cyan provides ongoing training for employees in the following areas: ○ Basic topics related to data protection ○ Technical and organizational measures in the guidelines ○ Employee-specific tasks in connection with these guidelines ○ Personal consequences of non-compliance with the guidelines or violations of data protection
b)	Physical security	**Business premises** • cyan restricts access to business premises where customer data is processed to authorized personnel. **Fail-safe** • cyan implements state-of-the-art measures to prevent data loss or system failure. **Contingency plans** • cyan creates and continuously reviews emergency plans to ensure that services can be restored as quickly as possible in the event of a disaster. • Where technically possible, customer data is restored to the latest version or to a state corresponding to the time before the disaster occurred. **Mobile working** • Employees are prohibited from storing customer data on portable devices such as USB drives. Remote access to cyan systems, e.g., from home offices, is via secure VPN connections.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

c)	Access	**Authentication** • Wherever technically possible, cyan implements two-factor authentication (2FA) for internal and external services. • cyan implements a strict password policy designed to prevent passwords from being guessed. • cyan monitors access to systems and detects repeated login attempts and rejected passwords. • cyan automatically blocks access for employees who leave the company as part of the offboarding process. **Authorization** • cyan keeps records of all systems and employees who have access to customer data. • cyan restricts the group of employees who can grant, change, and delete access to systems. Changes to access are subject to an approval process and are logged. • cyan only allows access to systems and customer data to the extent that this is absolutely necessary for the performance of tasks. **Workplace security** • cyan implements a clear desk policy. • Employees must lock their computers when they leave their workstations.
d)	Ongoing operation	**Backup & recovery** • cyan creates backups of the systems and ensures that these backups can be restored promptly. • cyan ensures that backups cannot be accessed without authorization. **Malware** • cyan protects its company network from Internet access with a firewall system. • cyan has rolled out anti-malware software on employee devices to provide protection against malware and ransomware. • cyan prohibits employees from installing software that has not been expressly approved. **Encryption** • cyan ensures that data is encrypted during transmission. The transmission of customer data via unsecured media is prohibited. **Deletion of customer data** • cyan implements policies that specify the deletion of customer data and rules for handling media containing such data. **Data protection violations** • Internal reporting and escalation processes are in place for security-related incidents. If there is a breach of personal data protection, the responsible party will be notified immediately in accordance with clause 9.2. • cyan logs data protection breaches and details of incidents:

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

	○ Description of the incident ○ Period and duration of the incident ○ Name of the person who reported the incident ○ Name of the person who registered the incident ○ Measures taken • cyan ensures that data breaches are reported to the relevant authorities.

For clarification, it is noted that changes in line with the state of the art are permitted.

ANNEX IV

LIST OF SUB-PROCESSORS

The Processor has the general authorization of the Controller to engage sub-processors listed in an agreed list. The Processor shall expressly inform the Controller in writing at least two weeks in advance of any intended changes to this list through the addition or replacement of sub-processors and shall thereby grant the Controller sufficient time to object to such changes before the relevant sub-processor(s) are engaged. The Processor shall provide the Controller with the necessary information by publication on the website so that the Controller may exercise its right to object.

Any objection by the Controller must be reasonably substantiated; otherwise, it shall be deemed invalid.

With regard to the following sub-processors, the Controller raises no objection:

Sub-processor	**Description of processing**	**Location of processing**	**Contractual relationship**
Amazon Web Services EMEA SARL	Hosting of infrastructure on the provider's cloud platform	EU / EEA, if applicable third countries	DPA
Google Ireland Limited	Provision of the app store platform for distribution of the mobile application; delivery of push notifications to users of the mobile app	EU / EEA, if applicable third countries	DPA
Apple Inc.	Provision of the App Store platform for distribution of the mobile application; delivery of push notifications to users of the mobile app	Ireland, if applicable third countries	DPA
Compax Softwaredevelopment Hungary Kft, 9400 Sopron, Agfalvi ut 2/A, Hungary	Network Operations Center and 24/7 monitoring of the cloud and software platform. [to be replaced as of 01.06.2026 by detect s.r.o.]	Vienna, Hungary	DPA

Detect s. r. o., Wolkrova 19, 851 01 Bratislava, Slovakia	Network Operations Center and 24/7 monitoring of the cloud and software platform. [effective as of 01.06.2026]	Slovakia	DPA
AVIRA GmbH & Co KG, Kaplaneiweg 1, 88069 Tettnang, Germany	Provision of anti-virus signatures through an update service	Germany	DPA
REDAMP SECURITY s.r.o., Palackého třída 879/84, 612 00 Brno, Czech Republic	The security systems collect unknown/suspicious domains appearing in customers' DNS traffic during operation and report these domains to the controller's research systems for further investigation. The exported data consists solely of the DNS domain and has no connection to any actual person.	Czech Republic	DPA
TUXGUARD GmbH, Saarbrücker Str. 9-10, 66130 Saarbrücken, Germany	Processing of personal and technical data in connection with IT security services, in particular for the detection, analysis, and mitigation of cyber threats. The processing is intended to protect sensitive data against unauthorized access, malware, or other security-related incidents.	Germany	DPA

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

ANNEX V

PROCESSING UNDER OWN RESPONSIBILITY

Independently of the processing of personal data on behalf of the Controller under this Data Processing Agreement, cyan may process personal data in certain cases in its own capacity as a controller within the meaning of Art. 4(7) GDPR.

Clear separation from processing on behalf of the Controller

Processing of personal data under cyan's own controllership is carried out strictly independently from processing activities performed on behalf of the Controller.

Personal data processed by cyan on behalf of the Controller under this DPA shall not be used by cyan for its own purposes, unless:

- such processing is required to comply with a legal obligation, or
- such use is explicitly permitted under applicable law.

cyan shall implement appropriate technical and organisational measures to ensure that personal data processed on behalf of the Controller and personal data processed under its own controllership are kept separate, both organisationally and, where feasible, technically.

Categories of processing activities under own controllership

cyan processes personal data in its own capacity as controller in particular in the following cases:

a) Business relationship management (B2B contact data): Processing of personal data of contact persons at the Controller or at distribution partners (e.g. name, email address) for the purpose of establishing, maintaining and managing business relationships.

b) Billing and accounting: Processing of personal data in the context of invoicing, payment processing, accounting, and compliance with statutory retention obligations.

c) Legal claims and compliance: Processing of personal data for the establishment, exercise or defence of legal claims, as well as for compliance with legal obligations (e.g. under applicable commercial and tax laws).

d) IT security and system operations (own purposes): Processing of log and protocol data for ensuring the security, integrity and stability of cyan's IT systems, as well as for detecting, analysing and mitigating security incidents, provided that such data is not part of the data processed on behalf of the Controller.

e) Support and quality assurance measures: Processing of personal data for internal documentation and quality assurance of support services, provided that such processing is not carried out on behalf of the Controller, but is necessary to ensure service quality and internal traceability.

f) Anonymisation and product improvement: Where data is anonymised by cyan and no longer relates to an identified or identifiable natural person, such data falls outside the scope of the GDPR.

The use of such anonymised and aggregated data for analytics, quality assurance, product improvement and further development is carried out under cyan's own controllership.

Legal bases

Processing of personal data under cyan's own controllership is based on the applicable legal provisions, in particular:

- Art. 6(1)(b) GDPR (performance of a contract),
- Art. 6(1)(c) GDPR (compliance with a legal obligation),
- Art. 6(1)(f) GDPR (legitimate interests, in particular IT security, business operations and legal defence).

ANNEX VI

ADDITIONAL PROVISIONS

a) The current version of this DPA shall be made available in the Dashboard. In the event of discrepancies, inconsistencies or questions of interpretation between the German and English language versions, the German version shall prevail.
b) In addition to Clauses 7.6(c) and (d), it is agreed that any audit by the Controller must be announced at least two weeks in advance and that all associated costs shall be borne by the Controller.
c) If the Service Description is amended, the Processor shall also be entitled to amend this DPA accordingly. The provisions of the Service Description shall apply mutatis mutandis.
d) For processing activities outside the scope of this DPA, reference is made to the privacy notice on the website.
e) The complete or partial invalidity of one or more provisions of this DPA shall not affect the validity of the remaining provisions. Invalid provisions shall be replaced by provisions coming closest to the economic intent of the invalid provision.
f) This DPA shall be governed by Austrian law, excluding the conflict of law provisions of international private law and the UN Convention on Contracts for the International Sale of Goods.
g) The Processor shall be liable for damages resulting from a culpable breach of this DPA in accordance with applicable data protection law. To the extent permitted by law, the liability limitations and exclusions set out in the Service Description shall apply accordingly to any liability arising under or in connection with this DPA. The Controller shall bear the burden of proof that the Processor culpably breached this DPA.
h) The Parties agree that all disputes arising directly or indirectly out of this DPA shall be decided by the court having subject-matter jurisdiction in Vienna.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363