Terms and Conditions

Green Mini host BV

These terms and conditions of delivery apply to any offer or quotation of Service Provider concerning Services, and are an integral part of any Agreement between Service Provider and Client. Client regulations or conditions that contradict or do not appear in these Terms and Conditions bind Service Provider only to the extent that Service Provider has accepted them explicitly In Writing.

Definitions

Service Provider: Green Mini host BV (GMH), a Dutch entity registered with the Chamber of Commerce under number 61482005.

Website: the website of Service Provider, available via the domain names greenmini.nl, greenminihost.com, greenmini.host and others.

Portal: the online customer environment(s) through which Client orders, configures, manages and pays for the Services, including API

API: the programmatic interface(s) made available by Service Provider through which Client can order, configure and manage Services.

Order: a request for Services placed through the Portal or accepted by quotation.

Subscription: an Agreement under which Services are delivered continuously for an agreed period (e.g. a 12-month hosting contract).

Account: the right of access to a user interface with which Client can manage and monitor (certain aspects of) the Services, as well as the configurations and the files stored for Client itself.

Terms and Conditions: the regulations of this document

AUP: the Acceptable Use Policy set out in these Terms and Conditions.

Client: the natural or legal person with whom Service Provider achieved an Agreement, including whoever negotiates with Service Provider on that, as well as their representatives, delegates, legal recipients and heirs.

Consumer: a Client who is a natural person not acting in the course of a trade, business, craft or profession.

Services: the products and/or services provided by Service Provider to Client on the basis of an Agreement.

Materials: all works, like websites and (web) applications, software, house styles, logos, folders, brochures, leaflets, lettering, advertisements, marketing and/or communication plans, concepts, images, texts, drafts, documentation, advice, reports and other products of the mind, as well as any preparatory material involved and data (coded or not),

Content: the data, software and material Client or its end users store, transmit, host or process on or through the Services

Agreement: any agreement between Service Provider and Client on the basis of which Service Provider delivers Services to Client.

In Writing: on paper, by email, or by message through the Portal or the support ticket system. Communication sent from or to the email addresses registered in Client's Account, or sent through Client's Portal account, is deemed to come from and to have reached the party concerned.

Applications with Increased Risk: applications in which an error in Services can lead to death or severe injury, severe environmental damage, or loss of (personal) details resulting in extensive

damage or harm. Examples include transportation systems in which an error may lead to derailed trains or plane crashes; medical systems in which an error may lead to patients not receiving treatment or receiving the wrong treatment; systems on which a substantial part of society depends for governmental services; core financial systems; systems which store medical data or other special categories of personal data, or other highly sensitive data.

Sanctions Lists: restrictive-measures and sanctions lists maintained by the European Union, the Netherlands, the United Nations and other applicable authorities.

Data Processing Agreement (DPA): the agreement between Service Provider (as Processor) and Client (as Controller), based on the GDPR. The standard DPA is attached to these Terms, but can also be a separate or customised agreement.

Technical and Organisational Measures (TOMs): the document, referenced in the DPA, that describes the security measures Service Provider applies to protect the Services and the personal data processed through them, and the split of shared responsibility between Service Provider and Client.

Article 1. Signing the contract

1.1 Client orders Services through the Portal, API or by accepting a quotation In Writing. By placing an Order, Client accepts these Terms and Conditions. Service Provider may require a verified Portal account before accepting an Order.

1.2 The Agreement comes into existence when Service Provider confirms the Order through the Portal or by email, or when payment for the first period is received and the Service is activated, whichever occurs first.

1.3 New Services are activated after payment of the first period has been received and any verification is complete. Service Provider may provision Services automatically once these conditions are met.

1.4 Accepted Orders are final, subject to Article 19 (Provisions for Consumers) where a statutory right of withdrawal applies.

1.5 The standard DPA is an integral part of these Terms and Conditions and comes into force at the same time. Client is obliged to inform Service Provider immediately in case any sensitive personal data will be processed and/or when the standard DPA does not cover the intended purpose of the data processing for which Client is responsible.

Article 2. Execution of the Agreement

2.1 After creation of the Agreement, Service Provider shall perform the activities mentioned as well as it is able, applying sufficient care and expertise.

2.2 Service Provider shall make efforts to realise high-quality and uninterrupted availability of Services and the systems and networks required, and to realise Client access to the data stored. However, Service Provider does not offer any guarantees concerning quality or availability, unless stated otherwise in the Agreement through an explicitly agreed Service Level Agreement (SLA).

2.3 Terms of delivery provided by Service Provider are exclusively indicative, except when the applicable SLA mentions terms that cannot be interpreted in any other way than as binding.

2.4 If and in so far as a good execution of the Agreement demands so, Service Provider has the right to have certain activities performed by third parties. These Terms and Conditions also apply to activities that third parties perform in the light of the Agreement.

2.5 Every action performed through Client's Account, sub-accounts or API credentials counts as an action of Client. Client keeps its credentials confidential and secure. If Client knows or should reasonably suspect that its Account or credentials are being misused, Client informs Service Provider as soon as possible so that Service Provider can take measures.

2.6 Service Provider provides best-effort technical support through the Portal ticket system and by email during regular Dutch business hours. Support above this best-effort level, including guaranteed response times, availability targets or extended cover, is provided only under a separate Service Level Agreement that is explicitly agreed.

2.7 All changes to the Agreement, either at the request of Client or because a different execution is required regardless of the cause, are regarded as extra work when they include extra costs and as less work when they include fewer costs. These shall be invoiced to Client accordingly.

2.8 Service description. Service Provider mainly provides dedicated physical servers and colocation of Client-owned equipment, together with related infrastructure, connectivity and data traffic. The specifications, included data traffic and any agreed service levels are set out in the Order or in a separately agreed document In Writing. Hardware that Service Provider owns is a finite resource: it is allocated to Client for the paid term and reclaimed and reissued after the Service ends (see Article 18). For colocation, the equipment is owned by Client, remains at Client's risk at all times.

2.9 Where a hardware component of a Service Provider-owned server, or any supporting infrastructure fails, Service Provider repairs or replaces it within a reasonable time. Repair or replacement may require downtime.

2.10 Physical transfers and shipments. Where hardware or storage media are shipped, delivered, collected, handed over or otherwise physically moved at Client's request or for Client's benefit, for example colocation delivery or collection, hardware returns, RMA, or migration of drives, this takes place at Client's risk. Service Provider is not liable for loss of, damage to, or unauthorised access to data or equipment during such a transfer. Client takes appropriate measures to protect its data before any transfer, including encryption of storage media. Service Provider may set security conditions for a transfer or refuse it.

2.11 Third-party software and services. Where Service Provider resells, sublicenses or makes available third-party software or services as part of or alongside the Services, for example control panels, operating-system licences or other vendor tools, the terms of the relevant third party apply to Client's use of them and Client accepts those terms. Service Provider passes through such third-party software and services as is, gives no warranty for them beyond what the third party provides, and limits its support to passing through the third party's support. Service Provider is not liable for any act, omission, change or discontinuation by such third parties.

2.12 Maintenance. Service Provider may perform maintenance, repairs, modifications or upgrades on the Services, the network and the infrastructure. Where Service Provider expects maintenance to materially affect the Services, it announces this in advance through the Portal, a status page or by email, and schedules the work where reasonably possible at times of low usage. Emergency maintenance needed to resolve or prevent a security incident or imminent failure may be performed at any time without prior notice; Service Provider informs Client without undue delay. Time during announced or emergency maintenance does not count as unavailability. Service Provider is not liable for failing to identify or apply a patch or update for software under Client's control.

Article 3. Obligations of Client

3.1 Client shall do and refrain from doing everything that is reasonably necessary and desirable to achieve a timely execution of the Agreement. In particular, Client shall provide Service Provider with all data that Service Provider indicates it requires, or that Client should reasonably know to be required, to perform the Services. The term within which Service Provider should execute the Agreement shall not start before all required data has been received by Service Provider.

3.2 If Client knows or can expect that Service Provider shall have to take certain (additional) measures to meet its requirements, for example an abnormal peak in system load, Client shall inform Service Provider immediately. Upon receiving the warning, Service Provider shall do

everything in its power to prevent inaccessibility of Services. All reasonable extra costs may be charged to Client.

3.3 If Client requires any permit or other legal or governmental consent for the intended use of the Services, Client shall arrange for those itself. Client guarantees Service Provider that all permits and/or consents required for the use of the Services are in the possession of Client.

3.4 Client is obliged to inform Service Provider of any changes in categories of data processing, especially when it comes to sensitive personal data.

3.5 Client warrants that all information it provides when ordering and during the Agreement is true, accurate, complete and current, and concerns Client's own identity or an entity Client is authorised to represent. Client keeps this information up to date in the Portal and shall not impersonate any person or misrepresent any affiliation.

3.6 Service Provider may, before activation or at any time during the Agreement, verify Client's identity and the legitimacy of an Order. This may include requesting a government-issued identity document, a Chamber of Commerce extract, proof of address, proof of ownership of the payment method, or confirmation of a business email address or VAT number. Service Provider does this to prevent fraud and abuse, to meet legal obligations including sanctions screening, and to protect the security of the Services and other clients. Service Provider may suspend or refuse activation while verification is pending or where Client does not cooperate within a reasonable period. Personal data processed for verification is handled in line with Service Provider's Privacy Statement.

3.7 Authorised representative. The holder of Client's Portal (sub)account is Client's authorised representative for placing Orders, making changes, and giving and receiving notices under the Agreement, unless Client designates another representative In Writing. Service Provider may rely on instructions given through the Portal account as validly given by Client.

Article 4. Acceptable Use Policy

4.1 This AUP governs all use of the Services by Client and by every end user, sub-user, reseller customer or other person who uses the Services through Client's account or access. Client is responsible for all such use as if it were its own.

4.2 Compliance with law. Client shall not use the Services in breach of any applicable Dutch, EU or other law, or in breach of the rights of others.

4.3 Sanctions and export control. Client warrants that it, its owners and its end users are not subject to any Sanctions List, and shall not make the Services available to, or use them for the benefit of, any sanctioned person, entity or territory, nor in breach of export-control law. Service Provider may refuse, suspend or terminate the Services to comply with sanctions, without liability.

4.4 Prohibited content. Client shall not use the Services to host, distribute or link to: (a) child sexual abuse material or content that sexualises minors; (b) content that incites or supports terrorism or violence, or that is unlawfully discriminatory, hateful or defamatory; (c) material that infringes intellectual-property or related rights; (d) malware, ransomware, exploit kits, command-and-control infrastructure or hacking tools intended to harm third parties; (e) content that unlawfully breaches the privacy of others; (f) content otherwise unlawful under applicable law.

4.5 Network and platform abuse. Client shall not send spam or unsolicited bulk communications; engage in phishing, fraud, identity theft or payment fraud; run port scans of third-party networks, denial-of-service attacks or intrusion attempts; operate open mail relays or open DNS resolvers; spoof source IP or hardware addresses; consume shared resources beyond the limits of the Service; or otherwise hinder, overload or damage the Services, Service Provider's network, or other clients or internet users.

4.6 Client shall not use the Services for Applications with Increased Risk unless these have been made available explicitly for that purpose. If none of the Services are available for those applications, Client can request a custom agreement with Service Provider.

4.7 Mining, farming or plotting of cryptocurrencies is not permitted unless explicitly agreed in the Order. Where agreed, Service Provider may immediately suspend or limit the Service where such use causes or threatens material degradation of the Services, excessive power or thermal load, damage to hardware, or a breach of applicable law.

4.8 Lawful adult content is permitted only where it complies with all applicable law, including age-verification requirements, and does not otherwise breach this AUP.

4.9 Client is responsible for the conduct of all its end users and sub-users and ensures they comply with this AUP. Where Client resells the Services, it does so in its own name without presenting Service Provider as supplier or subcontractor, binds its customers to terms at least as protective as this AUP, and indemnifies Service Provider against claims arising from their use.

4.10 Service Provider does not actively monitor content stored or transmitted by Client and has no general obligation to do so. Service Provider may act on notices, complaints or detected abuse and may investigate suspected breaches. Where a breach is found or reasonably suspected, or where required by law or a competent authority, Service Provider may remove or disable access to content, suspend or limit the Services, or terminate the Agreement, following the procedure in Article 5. Service Provider is not liable for measures taken in good faith under this Article.

4.11 Client is responsible for the insurance of its equipment and Content placed with Service Provider, covering theft, damage and liability towards third parties.

4.12 Client shall be extremely careful when working in the datacentre, so as not to damage the equipment and infrastructure of third parties. Client shall always adhere to the instructions of datacentre staff and (staff of) Service Provider, as well as to the house rules.

4.13 Unless explicitly agreed otherwise, Client is responsible for making and monitoring reliable backups.

Article 5. Notice and action regarding illegal content

5.1 Any person may notify Service Provider of allegedly illegal content hosted via the Services through the contact methods listed at its Website. A notice should include: a substantiated explanation of why the content is alleged to be illegal; the exact electronic location, such as the URL or IP; and a declaration of belief that the information is accurate and complete.

5.2 Service Provider processes notices in a timely, diligent, non-arbitrary and objective manner. A sufficiently substantiated notice that lets a diligent provider identify the illegality without a detailed legal examination gives Service Provider knowledge of that content.

5.3 Where Service Provider decides to act, it may disable access to or remove the content. Where feasible it disables access rather than deleting permanently and keeps a backup, so content can be restored if a decision is reversed, and it seeks to limit any effect on unrelated content.

5.4 Where Service Provider restricts content provided by Client on the ground that it is illegal or breaches these Terms and Conditions, it informs Client and gives a statement of reasons covering the ground relied on, the relevant facts, whether automated means were used, and how Client can seek redress, unless the law prevents this.

5.5 Client may contest a decision by contacting Service Provider In Writing. Service Provider reviews such complaints in good faith.

5.6 Service Provider acts on orders from competent Dutch or EU authorities to act against illegal content or to provide information, and informs the affected party where permitted.

5.7 Where Service Provider becomes aware of information suggesting that a criminal offence involving a threat to the life or safety of a person has taken place, is taking place or is likely, it promptly informs the competent authorities.

5.8 Service Provider may provide the name, address and other identifying information of Client to a third party who has complained that Client violates their rights, but only if the accuracy of that complaint is reasonably plausible, the third party has a clear interest in the information, and there is no less intrusive way for the third party to obtain it. Service Provider assesses each such request itself, is not obliged to comply with a request from a private party, and may require a court order, except where refusal would be unlawful.

5.9 Service Provider maintains an electronic point of contact for authorities and for recipients of the Services at abuse@greenmini.nl

Article 6. Immediate threats

6.1 Where Client's use of the Services, or the equipment or software it runs, poses an imminent threat to the security, integrity or availability of the network, the Services, other clients, the datacentre, or the safety of any person, for example an ongoing or imminent denial-of-service attack, a compromised or actively abused system, or malware propagation, Service Provider may immediately suspend, isolate or limit the affected Service without prior notice and without liability. Service Provider informs Client of the measure and its grounds as soon as reasonably practicable.

Article 7. Application for domain names

7.1 Applications, assignment and any use of a domain name depend on and are subject to the rules and procedures of the registering organisations concerned, like SIDN for .nl domain names. The organisation concerned determines whether a domain name should be granted. Service Provider only fulfils a mediating role in the application and does not guarantee that an application will be successful.

7.2 Client can only deduce that registration has been successful from the confirmation of Service Provider stating that the requested domain name has been registered. An invoice for registration costs is not a confirmation of registration.

7.3 Client protects and indemnifies Service Provider from all damage connected to (the use of) a domain name in the name of or by Client. Service Provider is not liable for Client losing its rights to a domain name or for the fact that a domain name is applied for and/or granted to a third party in the interim period, except in the case of intent or deliberate recklessness of Service Provider.

7.4 Client shall conform to the rules of registration organisations concerning the application, assignment and/or use of a domain name.

7.5 Service Provider has the right to make the domain name inaccessible or unusable, if Client demonstrably fails in the fulfilment of the Agreement, but only for as long as Client fails and only after a reasonable term for fulfilment, stated in a notice In Writing, has passed.

7.6 In case of dissolution of the Agreement due to defaults of Client, Service Provider has the right to cancel a domain name of Client after a waiting period of 30 days.

Article 8. Storage and data limits

8.1 Service Provider can set a data and/or storage limit per month that Client can actually use within the scope of the Services.

8.2 Where 'fair use' applies, no fixed data or usage limit is set. Client may use the Service without metering, provided its usage remains in reasonable proportion to the typical usage of comparable Services. Usage is in any case not fair where it structurally and materially

exceeds that typical usage, structurally saturates network or platform capacity, or is inconsistent with the nature of the Service.

8.3 If Client's usage is not fair within the meaning of 8.2, Service Provider first notifies Client and gives a reasonable period to adjust. If the usage continues, Service Provider may limit speed or capacity, set a concrete limit, or charge the excess per the rates under Article 11.2.

8.4 Should Client exceed the limits, Service Provider can charge an extra amount per data unit to the extent of the excess, according to the the rates under Article 11.2.

8.5 There is no liability for the consequences of not being able to send, receive, store or change data when an arranged storage or data limit is exceeded.

8.6 In the case of an excessive amount of data traffic caused by an external factor (e.g. a denial-of-service attack), Service Provider has the right to charge any costs involved to Client within reason.

Article 9. Rights of intellectual property

9.1 All rights of intellectual property in all Materials developed or provided by Service Provider within the scope of the Agreement lie exclusively with Service Provider and its licensors.

9.2 Client only obtains the rights of use and authorities granted in the Agreement or otherwise explicitly agreed In Writing. In all other cases, Client shall not publish or copy these Materials. Delivery of source code of Materials is obligatory only where explicitly agreed.

9.3 Client is not permitted to remove or change any indication of copyrights, brands, trade names or other rights of intellectual property, including indications concerning the confidential nature and secrecy of the Materials.

9.4 Service Provider is permitted to take technical measures to protect its Materials. Client is not permitted to remove or circumvent such protection, except in so far as mandatory law dictates otherwise.

Article 10. Prices

10.1 Unless explicitly stated otherwise with an amount, all amounts stated by Service Provider exclude VAT and other legal or governmental taxes.

10.2 If the price is based on data provided by Client and these data turn out to be incorrect, Service Provider has the right to adapt its prices accordingly, even after the Agreement has been signed.

10.3 If the Agreement concerns a Subscription, Service Provider has the right to alter the prices once per year for inflation according to the relevant price index of the CBS (Statistics Netherlands), plus 1 percentage point. Indexation under this clause is not a change within the meaning of Article 20 and gives no right to object or terminate. Any increase above indexation follows Article 20.

10.4 The same conditions and procedures apply to price changes as to changes of the Services and of these Terms and Conditions.

Article 11. Payment conditions

11.1 Service Provider invoices in advance for each Service period. Invoices may be electronic and issued through the Portal.

11.2 Some charges are invoiced after the fact, including usage above included limits, extra or one-off work, domain registrations and renewals, and other variable items. These are charged at the rates set out in the Order, the Portal, or a price list published by Service Provider, or, where no rate is set, at a reasonable rate. Extra or one-off work is quoted or agreed In Writing before it is carried out. The same payment term applies.

11.3 The payment term of every invoice is 14 days from the invoice date, regardless of the payment method used.

11.4 Client may pay using the methods offered in the Portal, which may include credit card, SEPA direct debit and bank transfer. Where Client uses an automatic method (credit card or SEPA direct debit), Client authorises Service Provider to charge the amounts due for the Services and their renewals automatically to that method on or after the invoice date. Client keeps a valid payment method on file for the duration of the Agreement and ensures sufficient funds are available. This authorisation does not change the moment payment is ultimately due.

11.5 If Client reverses, or has its bank or card issuer reverse, a payment for amounts that are due, the amounts concerned remain payable in full and the original payment term continues to apply. Where the reversal is unjustified, Service Provider may charge Client the costs imposed on it by banks, card schemes or payment providers for the reversal, plus reasonable administration costs, and may require a different payment method for future invoices. An unjustifiably reversed payment counts as non-payment for the purposes of the default and suspension provisions.

11.6 If Client does not pay an invoice in full within the payment term, it is in default automatically, without a notice of default. Statutory interest then accrues on the amount due, Client owes the extrajudicial and judicial recovery costs (including lawyers, bailiffs and recovery agencies)
If payment is not made by the date or period stated in a reminder In Writing, Service Provider may suspend access to the Services and to the Content and Materials hosted for Client until all amounts due, interest and costs are paid. Reactivation may carry a fee at the rates under Article 11.2.

11.7 Client is not allowed claims of postponement, set-off or deduction.

11.8 If Client fails to meet any obligation of the Agreement, Service Provider has the right to reclaim goods delivered without notice of default, in addition to suspension of the Services, without affecting Service Provider's right to reimbursement of damage, loss of profit and interest.

11.9 Amounts paid in advance for a Service period are not refunded, in whole or in part, where Client does not use the Service, ceases to use it during the paid period, or cancels per a date before the end of the paid period. This does not apply: (a) where the Agreement ends due to an attributable failure of Service Provider; (b) where Client terminates under Article 20.3 following a change of these Terms and Conditions; or (c) where Client is a Consumer and Article 19 or mandatory law provides otherwise, in which case prepaid amounts for the period after the termination date are refunded proportionally.

Article 12. Liability

12.1 Within the scope of the creation or execution of the Agreement, Service Provider is liable only as set out in this Article.

12.2 To the extent permitted by law, Service Provider's total liability under or in connection with the Agreement is limited, in aggregate, to the total fees (excluding VAT) paid by Client for the affected Service in the 90 days immediately preceding the event giving rise to the liability. A chain of connected events counts as one event.

12.3 Service Provider is not liable for indirect or consequential loss, including lost profit, lost revenue, lost savings, loss or corruption of data, or loss resulting from business interruption.

12.4 Liability of Service Provider for an attributable failure in the fulfilment of the Agreement arises only if Client gives Service Provider an immediate and sound notice of default In Writing, granting a reasonable term to remedy the failure, and Service Provider remains in failure after that term. The notice of default shall describe the failure in as much detail as possible, so that Service Provider can respond adequately.

12.5 Client reports any damage to Service Provider In Writing within 14 days after discovering it or after it should reasonably have been discovered; damage not reported in time is not eligible for compensation, unless Client demonstrates that earlier reporting was not reasonably possible. Any claim for damages lapses 12 months after the event that caused the damage, unless legal action has been commenced before then.

12.6 The exclusions and limitations in this Article do not apply if and in so far as the damage is the result of intent or deliberate recklessness of Service Provider's management, or to any liability that cannot be limited or excluded under mandatory law.

12.7 Client is liable to Service Provider for damage resulting from an attributable error or failure on Client's side. Client's indemnification obligations are set out in Article 4 and 13.

Article 13. Indemnification

13.1 Client indemnifies and holds Service Provider harmless against all third-party claims, and the resulting costs, damages and reasonable legal fees, that arise from or relate to (a) content stored, transmitted or made available through the Services by Client or its end users; (b) Client's use of the Services in breach of these Terms and Conditions, the AUP or applicable law; or (c) infringement of the rights of any third party, including intellectual-property, privacy or data-protection rights, by Client or its end users.

13.2 Service Provider notifies Client promptly of any such claim, gives Client the opportunity to assume the defence and settlement of the claim (provided no settlement imposes any obligation or admission on Service Provider without its prior written consent), and provides reasonable cooperation at Client's expense.

Article 14. Force majeure

14.1 Neither party can be held to fulfil any obligation in the case of a circumstance outside its control that could not reasonably have been foreseen upon signing the Agreement and that makes fulfilment impossible.

14.2 Force majeure includes (but is not limited to): failures of public infrastructure normally available to Service Provider on which the delivery of the Services depends but over which Service Provider has no power or contractual fulfilment claim, like the operation of the registers of IANA, RIPE or SIDN, and all internet networks with which Service Provider has no contract; failures of infrastructure and/or Services of Service Provider caused by computer crime, like (D)DoS attacks or attempts to circumvent network or system security; shortcomings of suppliers of Service Provider that Service Provider could not foresee and for which it cannot be held responsible, for example due to force majeure at that supplier; defects in items, equipment, software or other source material whose use Client has prescribed; unavailability of staff (because of illness or otherwise); governmental measures; general transportation problems; strikes; wars; terrorist attacks and civil unrest.

14.3 If a situation of force majeure lasts longer than 90 days, both parties have the right to dissolve the Agreement In Writing. Whatever has already been performed under the Agreement shall be settled proportionally, without either party owing the other anything further.

Article 15. Confidentiality

15.1 Parties shall treat information they provide to each other before, during or after the execution of the Agreement as confidential if it is marked as such or if the receiving party knows or should reasonably know that the information is intended to be confidential. Parties shall impose the same obligation on their employees and on third parties they engage.

15.2 Service Provider does not access, view, use or analyse the content Client stores or transmits via the Services, except: (a) at Client's request or with Client's implicit or explicit permission, for example to provide support; (b) where strictly necessary for the execution of the

Agreement or for the handling of abuse and notices under Articles 4 and 5; or (c) where a law, court order or order of a competent authority requires it. In those cases, access is limited to what is strictly necessary and to the persons who need it, and Client is informed where the law permits this.

15.3 Service Provider never sells Client data, never makes it available to third parties for their commercial benefit, and never uses Client content or personal data for its own purposes, including marketing, advertising, profiling or the training of AI models.

15.4 To keep the Services available, secure and within the limits of the Order, Service Provider may monitor technical and operational metrics of the Services and the network, such as reachability, latency, traffic volumes, port and service status, resource use and indicators of compromise, abuse or attack. This monitoring is limited to technical metadata and network metrics. Service Provider does not inspect, read or analyse the content of Client data through this monitoring. Any processing of personal data in this context is governed by the Data Processing Agreement.

15.5 The duty of confidentiality remains in effect after termination of the Agreement, for as long as the providing party can reasonably claim the confidential nature of the information.

Article 16. Security and incidents

16.1 Service Provider takes appropriate technical and organisational measures to protect the Services, in line with its information-security management system. Further detail is in the security appendix to the Data Processing Agreement and the Privacy Statement.

16.2 Service Provider informs Client without undue delay of security incidents that materially affect the Services provided to Client, together with the measures taken.

16.3 Client applies appropriate security to its own systems, applications, credentials and content, keeps software under its control up to date, and cooperates with reasonable security measures and requests from Service Provider.

Article 17. Duration and termination

17.1 The duration of the Agreement is the time period required to deliver the Services. If the Agreement is a Subscription, the duration is one year, unless agreed or indicated otherwise.

17.2 If a fixed duration of the Subscription has been agreed, neither party can terminate the Agreement unilaterally before that duration has expired, unless special grounds for termination apply as described below. For Consumers, Article 19 prevails after the first term.

17.3 Unless terminated In Writing at least 30 days before the end of the current term, a Subscription renews automatically for successive periods equal to the initial term.

17.4 Cancellation of a Subscription takes effect at the end of the current paid term, unless Client selects an earlier effective date (including immediate effect) when cancelling through the Portal, or the parties agree a different date In Writing. The Agreement ends on the effective date; from that date Service Provider may cease the Service and reclaim hardware.

17.5 Service Provider may suspend or terminate the Agreement In Writing with immediate effect if Client is declared bankrupt or files for bankruptcy, applies for suspension of payments, ceases or liquidates its business, breaches the Acceptable Use Policy, or if Client, its owners or its use of the Services become subject to a Sanctions List. For any other material default, Service Provider may suspend or terminate only after giving Client notice In Writing and a reasonable period to put the matter right, unless the default by its nature cannot be put right.

17.6 If Service Provider suspends the fulfilment of obligations, it retains its rights under the law and the Agreement, including the right to payment for the suspended Services.

17.7 If the Agreement is terminated or dissolved, Service Provider's claims on Client are immediately due and payable. In the case of dissolution, amounts already invoiced for performances already delivered remain due, without any obligation to undo. Client can only dissolve the part of the Agreement that has not yet been performed by Service Provider. If the dissolution is attributable to Client, Service Provider has the right to compensation of the direct and indirect damage resulting from it.

17.8 The right of suspension applies to all Agreements with Client simultaneously, even if Client is in default with regard to only one Agreement, and without affecting Service Provider's right to compensation of damage, loss of profit and interest.

Article 18. Procedure upon termination

18.1 Service Provider does not retain Content stored by Client on the Services after termination. Client exports and backs up its data before the Service ends.

18.2 Upon termination of a Service, Service Provider may reclaim the hardware on which the Service ran and permanently erase all Client data on it.

18.3 Erasure takes place as part of standard re-provisioning. Certified or verifiable data destruction is available on request, in advance, for an additional fee.

18.4 Service Provider retains Client's account and administrative data, such as contact details and invoices, only as long as needed and as required by law. This does not cover content stored by Client on the Services.

18.5 Upon termination of a colocation Service, Client provides In Writing a delivery address for its equipment. Service Provider de-installs the equipment and ships it to that address at Client's expense and risk. Alternatively, Client may collect the equipment itself, or have it collected, within 14 days after termination, coordinated with Service Provider and subject to the datacentre house rules. Service Provider does not access or erase data on Client-owned equipment; that data remains Client's responsibility.

18.6 If Client neither provides a delivery address nor collects the equipment within 14 days after termination, Service Provider may, after written notice, ship the equipment to Client's last known address, or store it at Client's cost, or, after a further 30 days without response, treat it as abandoned and dispose of it.

Article 19. Provisions for Consumers

19.1 The Services are offered only to Clients acting in the course of a trade, business, craft or profession. By placing an Order, Client warrants it does not act as a Consumer. Where mandatory law nonetheless treats Client as a Consumer, this article applies and prevails over conflicting provisions to the extent mandatory consumer law requires.

19.2 A Consumer may withdraw from the Agreement within 14 days of its conclusion without giving a reason. Where the Consumer expressly requests that performance begin during this period and confirms losing the right of withdrawal once the Service is fully performed, the right lapses accordingly; for a Service partly performed at withdrawal, the Consumer owes a proportionate amount.

19.3 After the first term, a Consumer subscription that has renewed or continued for an indefinite period may be cancelled at any time with a notice period of 30 days.

19.4 A Consumer is in default only after a reminder and a 14-day period to pay.

19.5 The exclusion of set-off and the limits on suspension do not apply to Consumers to the extent the law so requires.

Article 20. Changes to Services and these Terms and Conditions

20.1 Service Provider has the right to change and add Services and these Terms and Conditions. Changes also apply to Agreements already concluded, but only with a notice period of 30 days after announcement of the change.

20.2 Changes shall be announced to Client by email, through the Portal, or via another channel of which Service Provider can reasonably guarantee that the announcement has reached Client. Non-substantive changes of minor importance can be implemented at any time and require no notice.

20.3 If Client does not wish to accept a change, Client shall notify Service Provider In Writing within 14 days after the announcement, stating reasons. Service Provider can then reconsider the change. If Service Provider does not withdraw the change, Client can terminate the Agreement per the date the change takes effect, provided the termination is announced before that date.

20.4 Regulations concerning specific Services override general regulations concerning all Services where they conflict. Further agreements between Client and Service Provider prevail over these Terms and Conditions only if made In Writing and explicitly stated, or if this was the unmistakable intention of both parties.

Article 21. Final provisions

21.1 The Agreement is governed by Dutch law.

21.2 In so far as mandatory law does not prescribe otherwise, all disputes arising from the Agreement shall be brought before the competent Dutch court of the district in which Service Provider is located.

21.3 Any clause of the Agreement that proves void does not affect the validity of the Agreement as a whole. Parties shall in that case agree replacement terms that come as close as legally possible to the intention of the original clause.

21.4 Termination does not affect any provision that by its nature is intended to survive, including those on intellectual property, liability, indemnification, confidentiality, data return and deletion, and governing law and disputes.

21.5 Information and notifications on the Website, including published prices, are subject to typographical and programming errors. In the case of inconsistency between the Website and the Agreement, the Agreement prevails.

21.6 The log files and other electronic or analogue administration of Service Provider form full evidence of assertions of Service Provider, and the version of any (electronic) communication received or stored by Service Provider counts as authentic, unless Client provides evidence to the contrary.

21.7 Parties shall always immediately notify each other In Writing of any changes of name, postal address, email address, telephone number, bank account number, etc.

21.8 Service Provider may identify Client as a customer and use Client's name and logo for that purpose in its customer references and marketing channels. Client may opt out at any time by notice to Service Provider, after which Service Provider ceases further such use within a reasonable period.

21.9 Neither party may transfer its rights and obligations under the Agreement to a third party without the prior consent In Writing of the other party, which consent shall not be unreasonably withheld. This consent is not required in the case of a transfer to an affiliate, or in the case of a company acquisition, merger, or acquisition of the majority of the shares of the party concerned. Service Provider may condition its consent to a transfer by Client on verification of the acquiring party under Article 3.

Attachment 1: Data Processing Agreement

This data processing agreement applies to all processing of personal data undertaken by Green Mini host BV, registered with the Chamber of Commerce under number 61482005 (hereinafter: Processor), for the benefit of another party to whom it provides services (hereinafter: Controller).

Article 1. Purposes of processing

1.1 Processor agrees under the terms of this DPA to process personal data on behalf of Controller. Processing shall be done solely for the purpose of storing data on datacentre infrastructure for the benefit of Controller, and associated online services, execution of the principal Agreement and Service, and all purposes compatible therewith or determined jointly.

1.2 The personal data to be processed and the categories of data subjects are set out in Appendix 1. Processor shall not process the personal data for any other purpose except with Controller's consent. Controller shall inform Processor of any processing purposes not already mentioned in this DPA.

1.3 All personal data processed on behalf of Controller remains the property of Controller and/or the data subjects in question.

Article 2. Processor obligations

2.1 Regarding the processing operations referred to above, Processor shall comply with all applicable legislation, including the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) and the Dutch GDPR Implementation Act (Uitvoeringswet AVG, UAVG).

2.2 Upon first request, Processor shall inform Controller of the measures it has taken to comply with its obligations under this DPA.

2.3 All obligations of Processor under this DPA apply equally to any persons processing personal data under Processor's supervision, including but not limited to employees in the broadest sense.

2.4 Processor shall inform Controller without delay if, in its opinion, an instruction of Controller would violate the legislation referred to in 2.1.

2.5 Processor shall provide reasonable assistance to Controller with data protection impact assessments to be carried out by Controller.

Article 3. Transfer of personal data

3.1 Processor processes personal data primarily within the EU/EEA.

3.2 Processor may transfer personal data outside the EEA only where a valid transfer mechanism under Chapter V of the GDPR applies, such as an adequacy decision of the European Commission or appropriate safeguards within the meaning of Article 46 GDPR, including the EU Standard Contractual Clauses, supplemented or substituted where necessary with additional measures.

3.3 Processor informs Controller on request of the countries involved in the processing.

Article 4. Allocation of responsibilities

4.1 Processor makes available IT facilities to be used by Controller for the purposes mentioned above. Processor shall not itself perform processing operations on the Content unless separately agreed otherwise and except for managed components specified in the Order.

4.2 Processor is responsible only for the processing of personal data under this DPA in accordance with the instructions of Controller. For any other processing of personal data, including collection of personal data by Controller, processing for purposes not reported to

Processor, and processing by third parties engaged by Controller, Processor accepts no responsibility.

4.3 Controller represents and warrants that the content, usage and instructions to process personal data under this DPA are lawful and do not violate any right of any third party.

Article 5. Sub-processors

5.1 Controller grants Processor general authorisation to engage sub-processors for the processing under this DPA. Processor provides the current list of sub-processors on request.

5.2 Processor announces intended additions or replacements of sub-processors through the Portal at least 14 days before the change takes effect. Controller may object In Writing within that period on reasonable, data-protection-related grounds. If no resolution is found for a justified objection, either party may terminate the affected Service.

5.3 Processor ensures that any sub-processor is bound by data protection obligations offering a level of protection not materially less protective than this DPA, to the extent and scope relevant to the services performed by that sub-processor. Processor remains liable towards Controller for the performance of the sub-processor's obligations as for its own.

Article 6. Security

6.1 Processor implements appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk of the processing operations involved, against loss or unlawful processing. A description of the current measures, and the split of responsibility between Processor and Client, is available on request or published online. Processor may update these measures provided the level of protection is not materially reduced.

6.2 Processor does not warrant that security is effective under all circumstances. Processor shall maintain a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks for data subjects.

6.3 Controller only provides personal data to Processor for processing if it has ensured that the required security measures have been taken. Controller is responsible for compliance with measures agreed on its side.

Article 7. Notification of data breaches

7.1 Controller is at all times responsible for notifying personal data breaches to the competent supervisory authority and, where required, to data subjects. To enable Controller to comply, Processor notifies Controller of any personal data breach affecting Controller's data without undue delay after becoming aware of it, and in any event in time to allow Controller to meet its notification obligation.

7.2 The notification includes at least the nature of the breach, where possible the categories and approximate numbers of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its effects.

Article 8. Requests from data subjects

8.1 If a data subject addresses a request concerning their legal rights under data protection law to Processor, Processor passes the request on to Controller, and Controller handles it. Processor may inform the data subject of this. Processor provides reasonable assistance where Controller cannot fulfil the request without it.

Article 9. Confidentiality

9.1 All personal data Processor receives from Controller and/or collects itself is subject to strict confidentiality towards third parties. Processor shall not use this information for any purpose

other than that for which it was obtained, even if it has been converted into a form no longer related to an identified or identifiable natural person.

9.2 The confidentiality obligation does not apply where Controller has granted explicit permission to provide the information to third parties, where provision to third parties is reasonably necessary given the nature of the assignment, or where provision is legally required.

Article 10. Audit and DPIA

10.1 Controller has the right to have audits or DPIAs performed on Processor by an independent third party bound by confidentiality, to verify compliance with the security requirements, data processing regulations and this DPA.

10.2 An audit may be performed only after Processor has provided Controller, on first request, with similar recent audit reports of independent third parties, and a reasonable, substantiated suspicion of misuse or non-compliance remains, or reasonable doubt exists.

10.3 Processor gives its full cooperation to the audit and makes available employees and all reasonably relevant information, including supporting data such as system logs.

10.4 The audit findings shall be assessed by the parties in mutual consultation and implemented where reasonable.

10.5 Audits take place at most once per 12 months, on at least 30 days notice, during business hours, and without disrupting Processor's operations. The costs of an audit are borne by Controller, including the reasonable time spent by Processor's staff in preparing and supporting the audit, at Processor's standard rates. If the audit reveals a material non-compliance by Processor with this DPA, Processor bears its own costs of the audit.

Article 11. Liability

11.1 The liability of the parties under this DPA follows the limitation of liability in the Terms and Conditions: liability is limited, in aggregate, to the total fees (excluding VAT) paid by Controller for the affected Service in the 90 days preceding the event giving rise to the liability, a chain of connected events counting as one event. Liability for indirect damage is excluded. No limitation applies where damage results from intent or deliberate recklessness of the management of the party concerned, or where mandatory law (including Article 82 GDPR towards data subjects) does not permit limitation.

11.2 Any claim for damages that is not specifically notified In Writing lapses 12 months after its cause first arose.

Article 12. Term and termination

12.1 This DPA comes into force when the Agreement comes into force and lasts for the duration of the cooperation between the parties.

12.2 Upon termination of the DPA, Processor shall, at Controller's choice and within the constraints of the Terms and Conditions, return or destroy all personal data available to it, except to the extent retention is required by law. Data that Processor processes as an independent controller, such as account, billing, support and technical log data, falls outside this DPA and is retained per Processor's Privacy Statement and applicable statutory retention periods, after which it is deleted or anonymised.

12.3 Processor may amend this DPA following the same procedure as for changes to the Terms and Conditions.

Article 13. Applicable law and venue

13.1 This DPA is governed by the law and subject to the courts as stated in the Terms and Conditions.

Appendix 1: Personal data and data subjects

Processor processes non-sensitive personal data under the supervision of Controller, as specified in Article 1, such as: names and addresses, email addresses, IP addresses, phone numbers, logs, metadata and other categories of non-sensitive personal data.

Categories of data subjects: Controller's employees and affiliates; Controller's customers and users of their services; leads and potential customers; website visitors; persons who make their personal data available to Controller; other categories of data subjects whose personal data is processed using the Service.

Controller represents and warrants that this description is complete and accurate and indemnifies Processor for claims arising from a violation of this representation.

Retention and return: personal data on Service Provider-owned hardware is destroyed on reclaim of the hardware per Article 18 of the Terms and Conditions; Controller exports its data before the end of the paid term.