

PATCHSTACK DATA PROCESSING ADDENDUM

Version 1.0 (October 2026)

This Data Processing Addendum ("**DPA**") is an agreement between Patchstack OÜ ("**Patchstack**") and the customer named in the signature block below ("**Customer**"). This DPA supplements the Patchstack Terms of Service, the Patchstack Master Solution Agreement, or any other agreement between the parties under which Patchstack provides the Patchstack Solution to Customer (the "**Agreement**"). Capitalised terms not otherwise defined herein will have the meanings given to them in the Agreement.

Customer acknowledges that the Patchstack Solution processes HTTP traffic, vulnerability data, and related technical information associated with Customer Operations, some of which may contain Personal Data as defined below. Such Personal Data is processed as a necessary incident of the Patchstack Solution's security monitoring, vulnerability detection, and virtual patching functions. Patchstack does not determine the purposes for which Customer Operations generate or collect such data, nor does Patchstack inspect, select, or make decisions based on the substance of such data except as required to provide the Patchstack Solution.

Customer may be the controller of Personal Data, or the processor of Personal Data. When Customer is the controller and Personal Data is processed by Patchstack in providing the Patchstack Solution, Patchstack will be the processor of that Personal Data. When Customer is the processor and Personal Data is processed by Patchstack in providing the Patchstack Solution, Patchstack will be the sub-processor of that Personal Data.

This DPA applies only to the extent that Patchstack processes Personal Data for Customer as Customer's processor or sub-processor.

DEFINITIONS

"**Customer Operations**" means websites, platforms, operations, offerings, or services owned or operated by Customer.

"**Data Protection Law**" means all applicable data protection and privacy legislation, including: (a) the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"); (b) the EU GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**UK GDPR**"); (c) the UK Data Protection Act 2018; (d) the Swiss Federal Act on Data Protection of 25 September 2020 ("**Swiss FADP**"); (e) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020; and (f) any other applicable data protection legislation, in each case as amended, superseded, or replaced from time to time.

"**EU Standard Contractual Clauses**" means the standard contractual clauses annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, specifically Module 2 (controller to processor) and Module 3 (processor to processor) as applicable, and any modifications and replacements to them, or other standard contractual clauses adopted by the European Commission and entered into by the parties, from time to time.

"**GDPR**" means the EU GDPR and/or the UK GDPR, as applicable.

"**Instructions**" means (a) the Agreement (including this DPA), (b) Customer's use of the Patchstack Solution including Customer's preferences, settings, and controls within the Patchstack Solution, and (c) any other written instructions provided by Customer and acknowledged by Patchstack as valid instructions with which Patchstack agrees to comply.

"**Patchstack Solution**" means the Patchstack services, deliverables, and ancillary services that Patchstack provides to Customer under the Agreement.

"**Personal Data**" means any information relating to an identified or identifiable natural person that is processed by Patchstack in connection with the provision of the Patchstack Solution, and which is subject to Data Protection Law.

"**Standard Contractual Clauses**" or "**SCCs**" means the EU Standard Contractual Clauses and/or the UK Addendum, as applicable.

"**Sub-processor**" means any processor that is engaged by Patchstack to assist in its processing of Personal Data for Customer.

"**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018, as amended from time to time, and available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>.

The terms "controller", "data subject", "processor", "processing", and "supervisory authority" have the meanings given to them in the EU GDPR or the UK GDPR, as applicable. Where this DPA refers to the Swiss FADP, such terms will be interpreted in accordance with the Swiss FADP.

DATA PROTECTION

1. **General Compliance.** Both parties will comply with their respective obligations under Data Protection Law. This DPA is in addition to, and does not relieve, remove, or replace, a party's obligations under Data Protection Law.
2. **Scope and Roles.** This DPA applies to Personal Data processed by Patchstack for Customer, if any. In this context, Patchstack may act as processor to Customer, who may act either as controller or processor with respect to Personal Data. If Customer acts as a processor, Customer represents and warrants on an ongoing basis that the relevant controller has authorised: (a) the Instructions; and (b) Customer's engagement of Patchstack and its Sub-processors. Customer will forward to the relevant controller promptly and without undue delay any notice provided by Patchstack under this DPA.
3. **Processing Details.** Details of Personal Data processing (constituting Annex I and Annex II to the EU Standard Contractual Clauses and/or Appendix Information for the UK Addendum, as applicable):

Data Exporter: Customer, at the address and with the contact details given in the signature block below.

Data Importer: Patchstack OÜ, Aida tn 7, 80011 Pärnu linn, Pärnu maakond, Estonia.

Subject Matter: Personal Data as described below, processed in connection with the provision of the Patchstack Solution.

Purpose: the provision of the Patchstack Solution to Customer, including vulnerability detection, virtual patching, security monitoring, and related analytics.

Nature of the Processing: collection, logging, storage, analysis, retrieval, consultation, use, disclosure by making available, alignment, combination, restriction, erasure, and destruction of Personal Data, in each case as a necessary incident of the provision of the Patchstack Solution as described in the Agreement and initiated by Customer.

Categories of Data Subjects: the data subjects may include: (a) Customer's employees and other individuals in a working relationship with Customer; (b) representatives of Customer's cooperation partners; (c) Customer's customers, users, and potential customers or users who are natural persons; (d) visitors to and users of Customer Operations (websites, platforms, and services protected by the Patchstack Solution); and (e) any other individuals whose Personal Data is transmitted to or entered into the Patchstack Solution by or on behalf of Customer.

Types of Personal Data: Patchstack processes the following categories of Personal Data as a necessary incident of providing the Patchstack Solution:

- SaaS firewall logs (collected from any CMS with the Patchstack firewall enabled): IP addresses, user agent strings, and HTTP form submission data associated with blocked threats. Form submission data may incidentally contain Personal Data such as names, email addresses, or other information submitted by website visitors, the specific contents of which vary and cannot be predetermined ("**Captured Personal Data**");
- SaaS activity logs (collected from WordPress sites with the Patchstack plugin installed): IP addresses, usernames, and email addresses, depending on the activity type logged;
- Account and contact data: names, email addresses, and other contact information of Customer's representatives provided through the Patchstack customer portal or in connection with account administration;
- Other: any other Personal Data that Customer transmits to or enters into the Patchstack Solution.

Special Categories of Data: the Patchstack Solution is not designed to process special categories of Personal Data under Article 9 GDPR, Personal Data relating to criminal convictions and offences under Article 10 GDPR, or protected health information as defined in 45 C.F.R. § 160.103 (collectively, "**Sensitive Data**"). Captured Personal Data may incidentally include Sensitive Data, subject to the safeguards in Annex 1 and section 4A.

Processing Operations: as described in this DPA, including this section [3](#).

Duration of Processing:

- Captured Personal Data and SaaS firewall logs: for the duration of Customer's subscription or until Customer's account is deleted, whichever occurs first.
- SaaS activity logs: for the duration of Customer's subscription or until Customer's account is deleted, whichever occurs first.
- Account and contact data: for the duration of the Agreement and for such further period as required to comply with applicable law.

Competent Supervisory Authority: the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) (EU); the UK Information Commissioner's Office ("**ICO**") (UK); and the Federal Data Protection and Information Commissioner (Switzerland), as applicable.

4. **Customer Warranties.** Customer will ensure and warrants on an ongoing basis that it has all necessary and appropriate consents, lawful bases, and notices in place, in any form required by Data Protection Law, to enable the lawful transfer of Personal Data to Patchstack for the duration and purposes of the Agreement. The parties agree that Personal Data processing is required as a part of Patchstack's provision of the Patchstack Solution, and that Personal Data is not exchanged for monetary or other valuable consideration.

- 4A. **Sensitive Data.** Customer shall not configure, direct, or intentionally cause the Patchstack Solution to collect Sensitive Data, and shall not otherwise submit Sensitive Data to Patchstack, including through the Patchstack customer portal or support channels, except as agreed in a document signed by both parties. As between the parties, Customer is responsible for establishing a lawful basis, and any additional condition required by Data Protection Law, for processing Sensitive Data, including Sensitive Data incidentally included in Captured Personal Data. Patchstack's obligations under section 10 apply to Sensitive Data as to other Personal Data. Patchstack will not be liable for failure to meet any requirement of Data Protection Law specific to Sensitive Data that exceeds Patchstack's obligations under this DPA, to the extent the failure arises from Customer's breach of this section 4A.
5. **Transfer Responsibility.** Customer will ensure and warrants that where Personal Data is transferred outside the European Economic Area ("EEA"), Switzerland, or outside the UK, as part of Customer's use or deployment of the Patchstack Solution, adequate measures will be taken to ensure the Personal Data will be protected to an adequate level and the data subjects' rights under Data Protection Law will not be prejudiced by such a transfer. Subject to Patchstack's obligations in section [10.5](#) below with respect to Sub-processors, and section [13](#) below with respect to the Standard Contractual Clauses if applicable, Customer acknowledges that Customer is solely responsible for ensuring that Personal Data is transferred out of the EEA, Switzerland, or the UK in full compliance with Data Protection Law.
6. **Customer Security Measures.** Customer will ensure and warrants that Customer utilises appropriate technical and organisational measures to ensure a level of security appropriate to such risks, including, as appropriate, the measures referred to in Data Protection Law.
7. **Ongoing Security Assessment.** Customer confirms that it has assessed any security measures in place at the time of entering into the Agreement, and that it will continue to do so on an ongoing basis to ensure its obligations under this DPA. Customer is solely responsible (as between the parties) if such measures fail to meet the standards required by Data Protection Law.
8. **Data Subject Information.** Customer undertakes and confirms that any information required to be provided to a data subject has been so provided, or an applicable exemption is available and is being relied upon by Customer.
9. **Independent Controllers.** Customer and Patchstack agree that to the extent each party processes any Personal Data of the other party's personnel in connection with entry into the Agreement or the management of their business relationship, such party processes such data as an independent controller.
10. **Patchstack's Obligations.** Patchstack shall, in relation to any Personal Data processed in connection with the provision of the Patchstack Solution:
- 10.1. process that Personal Data only on the Instructions, except to the extent Patchstack is required to process data by applicable law or if in Patchstack's reasonable opinion such Instructions infringe Data Protection Law. In either case, Patchstack will without undue delay notify Customer unless applicable law prohibits Patchstack from so notifying Customer;
 - 10.2. not access or use, or disclose to any third party, any Personal Data, except, in each case, as necessary to maintain or provide the Patchstack Solution, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order);
 - 10.3. ensure that it has in place appropriate technical and organisational measures set forth in Annex 1 to this DPA designed to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction, or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;
 - 10.4. ensure that all Patchstack personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;
 - 10.5. ensure that where Sub-processors are used outside the EEA, Switzerland, or the UK, such that Personal Data is transferred outside the EEA, Switzerland, or the UK, and such transfer is not to a third country recognised as providing an adequate level of protection under applicable Data Protection Law, Patchstack will use commercially reasonable efforts to ensure that appropriate transfer mechanisms are in place, which may include without limitation use of the SCCs;
 - 10.6. maintain general records of processing activities carried out on behalf of Customer as required by Data Protection Law;
 - 10.7. taking into account the nature of the processing, insofar as reasonable and practicable, assist Customer in responding to any request from a data subject and in ensuring compliance with its obligations under Data Protection Law with respect to security, breach notifications, impact assessments, and consultations with supervisory authorities or regulators. Patchstack agrees to provide, upon reasonable request and at Customer's expense, information reasonably necessary for Customer to conduct transfer impact assessments. Patchstack's obligation to provide assistance under this section [10.7](#) is limited to the Personal Data processed by Patchstack and the processing Patchstack performs. Patchstack is not obligated to provide legal advice or to assess the compliance of Customer's broader processing activities;

- 10.8. notify Customer without undue delay (and within 72 hours or any notice period mandated by Data Protection Law, whichever is shorter) on becoming aware of and validating a Personal Data security incident and will provide all information required by Data Protection Law. Patchstack is not obligated to report unsuccessful incidents or incidents that result in no unlawful or accidental destruction, loss, alteration, disclosure of, or unauthorised access to Personal Data or any of Patchstack's equipment or facilities storing Personal Data. Such non-reportable incidents may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers), or similar incidents. Patchstack's obligation to report or respond to a security incident under this section is not and will not be construed as an acknowledgement by Patchstack of any fault or liability of Patchstack with respect to the incident. Patchstack has no obligation to assess or inspect data in order to identify information subject to any specific legal requirements;
 - 10.9. make available to Customer information reasonably necessary to demonstrate compliance with Patchstack's obligations under this section 10. Patchstack may satisfy this obligation by providing: (a) summaries or attestation letters derived from third-party audits or certifications conducted within the preceding twelve months; and/or (b) written responses to reasonable written questions submitted by Customer. Patchstack may answer by referring Customer to Annex 1, Patchstack's trust centre (trust.patchstack.com) or other security documentation that Patchstack makes available, and may provide information in its own format rather than completing questionnaires or forms prepared by Customer. Customer may submit questions under this section 10.9 no more than once in any twelve-month period, except following a Personal Data security incident or where a supervisory authority requires it. A question is not reasonable to the extent it seeks information about Patchstack's other customers, its source code, or security details whose disclosure would weaken the protection of Personal Data, or asks Patchstack to assess Customer's own processing or compliance. If Customer reasonably demonstrates that the foregoing measures are insufficient to verify compliance, Patchstack will permit an audit or inspection of the processing activities covered by this DPA, subject to the following conditions: (i) Customer will provide not less than sixty days' prior written notice; (ii) such audit will be conducted no more than once per calendar year; (iii) such audit will be conducted at Customer's sole expense (including any reasonable fee charged by Patchstack for staff time and resources); (iv) the auditor must be a reputable third-party audit firm mutually agreed upon by the parties (such agreement not to be unreasonably withheld), which has entered into a confidentiality agreement acceptable to Patchstack; (v) the audit will be limited in scope and duration to that which is reasonably necessary to verify compliance with this DPA and will not extend to Patchstack's other customers' data, proprietary systems, source code, or trade secrets; (vi) the auditor's findings will be shared with Patchstack and will be treated as Patchstack's confidential information; and (vii) Customer will use reasonable efforts to minimise disruption to Patchstack's operations. For the avoidance of doubt, this section [10.9](#) supersedes any conflicting audit provisions in the SCCs to the maximum extent permitted by Data Protection Law; and
 - 10.10. at the written direction of Customer, delete Personal Data on termination of the Agreement unless required by applicable law to store the Personal Data.
11. **Reciprocal Cooperation.** Customer shall provide reasonable cooperation and information to Patchstack in connection with any inquiry, investigation, or proceeding by a supervisory authority or regulator that relates to Personal Data processed under this DPA, including by confirming the lawful basis for processing, confirming or clarifying Instructions, and providing information that is not within Patchstack's possession or control. Customer shall respond to reasonable requests for cooperation under this section without undue delay.
 12. **Consent Notification.** Customer will immediately notify Patchstack if any necessary appropriate consents and notices required to enable lawful transfer of Personal Data to Patchstack for the duration and purposes of the Agreement have been breached, terminated, withdrawn, or are otherwise no longer valid.
 13. **International Transfers.** The parties agree that (a) the EU Standard Contractual Clauses apply if Personal Data from the EEA and/or Switzerland is transferred via the use of the Patchstack Solution in a country outside of the EEA or Switzerland, and such transfer is not to a third country that the applicable data protection authority considers to provide an adequate level of protection; (b) the UK Addendum applies if Personal Data from the UK is transferred via the Patchstack Solution in a country that is outside of the UK, and such transfer is not to a country that the UK Secretary of State considers to provide an adequate level of protection (such outbound transfers of Personal Data from the EU, Switzerland, or the UK, each an "**EU/UK Outbound Transfer**"). If no EU/UK Outbound Transfer occurs, the SCCs and this section [13](#) will not apply. As used in this section, the terms "Data Importer" and "Data Exporter" will have the meanings given to them in the Standard Contractual Clauses. The parties acknowledge that for the purposes of the Standard Contractual Clauses Patchstack is acting in the capacity of a Data Importer and Customer is the Data Exporter (notwithstanding that Customer may be located outside of the EEA, Switzerland, or the UK or is acting as a processor on behalf of third-party controllers). Each party will comply with the applicable obligations of the Standard Contractual Clauses in their respective roles as Data

Exporter and Data Importer. The data subjects, categories of data, and processing operations (as required to be disclosed in the Standard Contractual Clauses) are as set forth in this DPA. Annex 1 to this DPA details the technical and security measures Patchstack has implemented, as required to be disclosed in the Standard Contractual Clauses.

14. **SCC Governing Law.** The parties further agree that for all EU/UK Outbound Transfers, the governing law of the Standard Contractual Clauses entered into by Patchstack and Customer will be: (a) the laws of Estonia, unless Customer is located in the UK; or (b) the laws of the UK, if Customer is located in the UK. If any inconsistency arises between this section [14](#) and any other provision for the governing law of the Standard Contractual Clauses entered into between Customer and Patchstack, this section [14](#) will take precedence.
15. **Conflict with SCCs.** To the extent required by applicable Data Protection Law, in the event of any conflict between this DPA and the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will prevail, and in the event of any conflict between this DPA and the UK Addendum, the UK Addendum will prevail.
16. **Audit Rights.** Customer agrees that it shall exercise any audit rights under this DPA (including any audit rights granted by the Standard Contractual Clauses or Data Protection Law) in accordance with section [10.9](#) above.
17. **Government Access.** Patchstack represents and warrants that, as of the DPA Effective Date, it has not received any order, request, or other communication from a governmental body for the disclosure of Personal Data and it shall:
 - 17.1. if it receives such order, request, or other communication, attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Patchstack may provide Customer's basic contact information to the relevant body. If compelled to disclose Personal Data to a governmental body, then Patchstack will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Patchstack is legally prohibited from doing so;
 - 17.2. provide information to Customer on request regarding: (a) the number of orders, requests, or other communications from governmental bodies for the disclosure of Personal Data and/or assistance in surveillance processes and the type of information requested, (b) its responses to the foregoing, and (c) its process for challenging such orders, requests, and communications; and
 - 17.3. notify Customer if Patchstack becomes aware that its ability to maintain the confidentiality and security of Personal Data has been materially compromised for any reason.
18. **Sub-processors.** Customer agrees that Patchstack may use Sub-processors to fulfil its contractual obligations under this DPA or to provide certain services on its behalf, such as providing hosting and infrastructure services, and consents to the use of Sub-processors as described in this section. The Patchstack website (currently posted at <https://patchstack.com/subprocessors/>) lists Sub-processors that are currently engaged by Patchstack to deliver the Patchstack Solution. (Such webpage constitutes Annex III/Appendix 3 to the Standard Contractual Clauses if and as applicable.)
 - 18.1. At least ten business days before Patchstack engages any new Sub-processor to carry out processing activities on Personal Data on behalf of Customer, Patchstack will endeavour to update the applicable website and provide Customer notice of that update as per the means specified for notices in the Agreement. The notice will identify the new Sub-processor, describe in reasonable detail the processing activities to be performed, and specify the country or countries in which the processing will take place.
 - 18.2. Customer may object to a new Sub-processor by notifying Patchstack in writing within ten days of receiving Patchstack's notice under section [18.1](#). An objection must set out in reasonable detail the specific data protection or information security grounds on which it is based (a "Qualifying Objection"). An objection constitutes a Qualifying Objection only if Customer demonstrates, on reasonable grounds, that the new Sub-processor's technical and organisational measures for the protection of Personal Data are materially inferior to those maintained by the Sub-processor it is replacing, or, where the new Sub-processor is not replacing an existing Sub-processor, materially inferior to the measures described in Annex 1 to this DPA. For the avoidance of doubt, objections based on grounds unrelated to data protection or information security do not constitute Qualifying Objections.
 - 18.3. If Customer does not notify Patchstack of an objection within the period specified in section [18.2](#), Customer will be deemed to have consented to the new Sub-processor's appointment.
 - 18.4. On receipt of a Qualifying Objection, the parties will engage in good faith discussions for a period of not more than 30 days (the "Resolution Period") to resolve the objection. Patchstack will refrain from engaging the new Sub-processor for processing of Customer's Personal Data during the Resolution Period. During the Resolution Period, Patchstack may: (a) appoint on an interim basis an alternative Sub-processor whose technical and organisational measures address the grounds of the objection; or (b) continue with the current Sub-processor, if any.
 - 18.5. If the Qualifying Objection cannot be resolved through good faith discussions under section [18.4](#), and Patchstack reasonably determines that use of the new Sub-processor is reasonably necessary to provide the affected service, Patchstack may terminate the affected portion of the Patchstack Solution, or if not practicable, the relevant subscription, on 30 days' written notice without penalty as to the terminated affected service. Where Patchstack

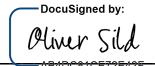
terminates the relevant subscription in its entirety under this section [18.5](#), Patchstack will refund any prepaid fees covering the remainder of the subscription term following the effective date of termination, provided all Patchstack fees accrued prior to termination have been paid.

19. **DPA Revisions.** Patchstack may propose revisions to this DPA by replacing it with any applicable controller-to-processor standard clauses or similar terms forming part of an approved code of conduct or applicable certification scheme (which will apply when replaced by attachment to the Agreement). Customer and Patchstack will negotiate such changes in good faith as soon as reasonably practicable.
20. **SCC Updates.** The parties agree that, if any new versions or revisions to the EU Standard Contractual Clauses are approved by the European Commission, or new versions or revisions of the UK Addendum are approved and published by the ICO, such that the implementation of the Standard Contractual Clauses in this DPA no longer applies or is no longer appropriate, the parties shall work together to enter into new standard contractual clauses as appropriate.
21. **EU SCC Elections.** Where the EU SCCs apply to transfers of Personal Data governed by this DPA, the following options are deemed to be selected and incorporated, each clause reference in this section being a reference to a clause in the EU SCCs: (a) Clause 7 (docking clause) will not apply; (b) at Clause 9 (use of sub-processors), Option 2 (general written authorisation) will apply for both Module 2 and Module 3; (c) at Clause 11 (redress), the optional redress mechanism will not apply; and (d) the competent supervisory authority under Clause 13 will be the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) for transfers subject to the EU GDPR.
22. **Swiss FADP.** Where the Swiss FADP applies to transfers of Personal Data governed by this DPA, the EU Standard Contractual Clauses will apply as modified by the following: (a) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP; (b) references to specific articles of Regulation (EU) 2016/679 will be interpreted as references to the equivalent provisions of the Swiss FADP; (c) references to "EU", "Union", and "Member State" will not be interpreted in a way that excludes data subjects in Switzerland from exercising their rights in their place of habitual residence; (d) references to the "competent supervisory authority" will be interpreted as references to the Federal Data Protection and Information Commissioner; (e) references to "Member State" law will be interpreted as including Swiss law; and (f) the EU Standard Contractual Clauses will be governed by Swiss law and disputes will be resolved before the competent Swiss courts.
23. **CCPA.** This section [23](#) applies to the extent that Patchstack processes Personal Data that is subject to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA") ("California Personal Data"). For the purposes of the CCPA, Patchstack is a "Service Provider" as defined in California Civil Code section 1798.140(ag). In its capacity as Service Provider, Patchstack:
 - 23.1. shall process California Personal Data solely for the specific business purpose of providing the Patchstack Solution to Customer as described in the Agreement, or as otherwise permitted by the CCPA;
 - 23.2. shall not sell or share (as those terms are defined by the CCPA) California Personal Data;
 - 23.3. shall not retain, use, or disclose California Personal Data for any purpose other than the business purpose specified in the Agreement, including any commercial purpose other than providing the Patchstack Solution, except as permitted by the CCPA;
 - 23.4. shall not combine California Personal Data received from or on behalf of Customer with personal information received from any other person or collected from Patchstack's own interaction with data subjects, except as permitted by the CCPA;
 - 23.5. shall provide reasonable assistance to Customer (at Customer's expense) in responding to verifiable consumer requests under the CCPA, to the extent that such requests relate to Personal Data processed by Patchstack;
 - 23.6. shall notify Customer if Patchstack makes a determination that it can no longer meet its obligations under the CCPA;
 - 23.7. shall permit Customer to take reasonable and appropriate steps to help ensure that Patchstack uses California Personal Data in a manner consistent with Customer's obligations under the CCPA, provided that such steps do not require Patchstack to disclose its confidential information or trade secrets; and
 - 23.8. hereby certifies that it understands and will comply with the restrictions and obligations set out in this section 23.
24. **UK Addendum.** Where the UK Addendum applies to transfers of Personal Data governed by this DPA, the parties agree that:
 - 24.1. the UK Addendum will be populated by reference to this DPA and its Annexes and that any changes in formatting (including for the avoidance of doubt with respect to Part 1: Tables) will not adversely affect the validity of the DPA or the compliance with Data Protection Law of any international transfers of Personal Data made thereunder;
 - 24.2. any formatting changes do not reduce the standard of Appropriate Safeguards (as defined in the UK Addendum) provided; and
 - 24.3. neither party will be entitled to end the UK Addendum pursuant to Section 19 except where a revision under Section 18 materially reduces the Appropriate Safeguards.

25. **Liability.** Liability arising out of or relating to this DPA (whether in contract, tort, or otherwise) is subject to the limitations and exclusions of liability set out in the Agreement.
26. **Governing Law.** This DPA is governed by and construed in accordance with the governing law and jurisdiction provisions of the Agreement, except to the extent that a different governing law is mandated by the SCCs or by applicable Data Protection Law.
27. **Conflicts.** In the event of any conflict between this DPA and the Agreement, this DPA will prevail with respect to matters of data protection. In the event of any conflict between this DPA and the SCCs, the SCCs will prevail to the extent required by Data Protection Law.
28. **Severability.** If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions will continue and remain in full force and effect.
29. **Updates.** Patchstack may update this DPA from time to time to reflect changes in law, regulatory guidance, or its practices. Notice of material changes will be provided in accordance with the Agreement, such changes to take effect upon the next renewal of Customer's subscription. Customer's renewal of its subscription indicates Customer's acceptance of and agreement to the modified DPA.
30. **Assignment.** This DPA will be binding upon and inure to the benefit of the parties and their respective successors and permitted assigns. Patchstack may assign or transfer this DPA in connection with any assignment of the Agreement permitted under the Agreement, without requiring Customer's separate consent. Customer agrees that any such assignment or transfer includes the transfer of all rights, obligations, and associated data (including Personal Data) to the extent necessary to ensure continuity of service under the Agreement. Any assignee or successor will be bound by the obligations of this DPA to the same extent as Patchstack. For the avoidance of doubt, following any such assignment, references to "Patchstack" in this DPA will be read as references to the assignee or successor entity, and the Instructions will continue in effect.
31. **Execution.** This DPA takes effect on the later of the date Customer signs it and the date the Agreement takes effect (the "**DPA Effective Date**"), and applies for as long as Patchstack processes Personal Data under the Agreement. This DPA replaces any data processing addendum previously forming part of the Agreement, except a data processing agreement that the parties have negotiated and signed separately, which will continue to prevail over this DPA. Patchstack's signature applies only to the text of this DPA as published by Patchstack, and no addition, deletion, or other change made by Customer will bind Patchstack unless an authorised representative of Patchstack signs it. This DPA may be signed electronically and in counterparts. Except for a separately negotiated data processing agreement described in this section 31, the Agreement, including this DPA, constitutes the entire agreement between the parties as to the processing of Personal Data, superseding any prior agreements, understandings, communications or proposals.

SIGNED by the authorised representatives of the parties:

PATCHSTACK OÜ

Signature:  AB4DC81CE72E42F...

Name: Oliver Sild

Title: CEO

Date: 10/26/2026

CUSTOMER

Legal name: _____

Registered address: _____

Agreement with Patchstack (tick one):

☐ Patchstack Terms of Service

☐ Patchstack Master Solution Agreement

☐ Other (name and date): _____

Data protection contact (name and email): _____

Signature: _____

Name: _____

Title: _____

Date: _____

DPA ANNEX 1: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

(Annex II to the EU Standard Contractual Clauses and/or Appendix Information for the UK Addendum, as applicable.)

In this Annex, "Processor" refers to Patchstack and "Controller" refers to Customer (or, where Customer acts as a processor, to the controller on whose behalf Customer engages Patchstack). The Processor implements and maintains the following technical and organisational measures to protect Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, or damage, in accordance with Article 32 of the GDPR.

As of the DPA Effective Date, the Processor holds SOC 2 Type II and ISO 27001 certifications, the current status of which is published at the Processor's trust centre (trust.patchstack.com). On request, the Processor will provide the Controller with summaries or attestation letters derived from those audits or certifications, subject to the Controller's obligation to keep that information confidential. Full audit reports and the Processor's internal security policies are made available under the Processor's enterprise agreements, or otherwise at the Processor's discretion.

1. Encryption

In transit. All Personal Data transmitted over public networks is encrypted using TLS 1.2 or higher. The Processor's HTTPS implementation uses industry-standard algorithms and certificates. Unencrypted connections (plain HTTP) are not accepted for any interface that processes Personal Data.

At rest. Personal Data stored in the Processor's production environment is encrypted at rest using AES-256 or equivalent encryption. Encryption keys are managed through the cloud hosting provider's key management service or an equivalent solution that enforces key rotation and access controls.

2. Access Control

Authentication. The Processor enforces a password policy for all user-facing interfaces that requires a minimum length, complexity, and expiry cadence consistent with current industry guidance. Multi-factor authentication is required for: (a) all Processor personnel accessing production systems or infrastructure that stores Personal Data; and (b) all administrative or privileged accounts.

Authorisation and least privilege. Access to Personal Data is granted on a need-to-know basis. The Processor maintains role-based access controls that limit each user and system to the minimum privileges required to perform their function. Access rights are reviewed periodically and revoked promptly upon change of role or termination of employment.

Customer data segregation. Customer data is stored in multi-tenant systems that enforce logical separation between customers. The Processor's application layer validates each request against the authenticated customer's permissions before returning data. Customers are not permitted direct access to the underlying infrastructure.

API access. Public APIs are secured using API keys, OAuth tokens, or equivalent credential mechanisms. API credentials are unique per customer account.

3. Personnel Security

Confidentiality obligations. All Processor personnel who have access to Personal Data are bound by written confidentiality obligations, whether through employment contracts, non-disclosure agreements, or equivalent binding instruments.

Training. The Processor provides data protection and information security awareness training to personnel with access to Personal Data, at onboarding and periodically thereafter.

Background verification. The Processor conducts background verification on personnel with access to production systems to the extent permitted by applicable law.

4. **Network and Infrastructure Security**

Cloud infrastructure. The Processor hosts its production environment with a cloud infrastructure provider whose physical and environmental security controls are independently audited (e.g., SOC 2 Type II, ISO 27001, or equivalent). The Processor will identify the hosting provider and data centre region on request.

Network controls. Network access control mechanisms are designed to prevent unauthorised traffic from reaching the production environment. Technical measures include virtual private cloud segmentation, security groups, and firewall rules. Administrative access to production infrastructure is restricted to authorised personnel via secure, audited channels.

Intrusion detection. The Processor maintains monitoring capabilities designed to detect unauthorised access attempts and anomalous activity on systems that process Personal Data.

5. **Vulnerability Management**

Patching. The Processor maintains a vulnerability management programme that includes timely application of security patches to operating systems, libraries, and application dependencies. Critical and high-severity vulnerabilities are remediated within timeframes consistent with industry practice.

Code review. Security reviews of application code are performed, which may include static analysis, peer review, or automated scanning, to identify and remediate software vulnerabilities before deployment to production.

Penetration testing. The Processor conducts or commissions independent penetration testing of its production environment at least annually. Identified vulnerabilities are triaged and remediated according to severity.

6. **Logging and Monitoring**

The Processor's infrastructure logs authentication events, administrative actions, and access to systems that store Personal Data. Logs are retained for a period sufficient to support incident investigation and are protected against tampering. Automated alerting is configured to notify appropriate personnel of security-relevant events.

7. **Incident Response**

The Processor maintains a documented incident response process that includes identification, containment, eradication, recovery, and post-incident review. The process designates responsible personnel and defines escalation procedures. The notification obligations in the DPA govern the Processor's communication with the Controller in the event of a Personal Data breach.

8. **Availability and Resilience**

Redundancy. The Processor's production architecture is designed for redundancy, including deployment across multiple availability zones where supported by the hosting provider.

Backups. Production data is backed up regularly. Backups are encrypted and stored in a location that is logically or physically separate from the primary production environment. The Processor tests backup restoration periodically.

Disaster recovery. The Processor maintains a disaster recovery capability designed to restore the availability of and access to Personal Data in a timely manner following a physical or technical incident. Recovery objectives are commensurate with the nature of the service.

9. **Secure Deletion**

On termination of the Agreement or at the Controller's written request, the Processor deletes Personal Data from production systems and, within a reasonable period, from backups and replicas, unless retention is required by applicable law. Deletion is performed using methods designed to render the data unrecoverable.

10. **Audit and Compliance Verification**

The Processor makes available to the Controller, on request and subject to the Controller's obligation to keep that information confidential, information reasonably necessary to demonstrate compliance with the measures described in this Annex. The provisions of the DPA govern all audit and inspection rights.
