Serverpod Data Processing Agreement

Serverpod AB · Version 1.0 · 15 September 2026

Part A: Cover terms

A1. Parties and scope. This Data Processing Agreement ("DPA") is entered into between Serverpod AB, a Swedish company (org. nr 559337-1213) ("Serverpod"), and the customer that uses Serverpod Cloud (the "Customer"). It applies whenever Serverpod processes personal data on the Customer's behalf while providing Serverpod Cloud under the Serverpod Cloud Terms of Service (the "Terms"). That covers personal data in the content the Customer deploys, stores or sends through Serverpod Cloud, such as application code, databases, files, logs, environment variables, passwords and secrets, and emails sent to the Customer's end users ("Customer Personal Data").

A2. What this DPA does not cover. Serverpod processes data about the Customer's own account (names and email addresses of users of the console at console.serverpod.dev and the CLI, billing details and usage data) as a controller. That processing is described in Serverpod's privacy policy, not in this DPA.

A3. Acceptance. This DPA forms part of the Terms. By accepting the Terms, the Customer enters into this DPA and is listed as a Party in Annex I. A Customer that needs a signed copy can request one at privacy@serverpod.dev.

A4. Roles. The Customer is the controller and Serverpod is the processor. Where the Customer itself acts as a processor for a third party, Serverpod is a sub-processor. The Customer is then responsible for passing on instructions and information between Serverpod and that third party.

A5. Instructions and use of data. The Terms, this DPA and the Customer's use and configuration of Serverpod Cloud through the console, the CLI and the API are the Customer's documented instructions under Clause 7.1. Additional instructions must be given in writing. If the Customer gives an additional instruction about the processing of Customer Personal Data that Serverpod cannot carry out through Serverpod Cloud as offered, Serverpod tells the Customer without undue delay and is not required to carry it out. The parties may agree on a way to meet it, including any cost. If they do not, the Customer may terminate the affected services. Serverpod does not use Customer Personal Data for its own purposes, and does not use it to train machine-learning models.

A6. Structure and precedence. This DPA consists of Part A, the standard contractual clauses in Part B (the "Clauses") and Annexes I to IV. In a conflict, the Clauses prevail over Part A, and this DPA prevails over the Terms. Nothing in Part A is meant to contradict the Clauses or reduce the rights of data subjects.

A7. Sub-processors. The Customer gives Serverpod general written authorisation under Clause 7.7(a), Option 2, to engage the sub-processors listed in Annex IV. Serverpod keeps the current list at https://serverpod.dev/legal/subprocessors. Serverpod notifies the Customer of any intended addition or replacement at least 30 days in advance, by email to the account owner and on that page. The Customer may object in writing within that period on

reasonable data protection grounds. If the parties cannot resolve the objection, the Customer may terminate the affected services before the change takes effect and receives a refund of any prepaid fees for them.

A8. International transfers. Serverpod hosts each Customer project in the region the Customer selects, and does not change the region or location of an existing project unless the Customer instructs it to. Where a sub-processor in Annex IV transfers Customer Personal Data outside the EEA, the transfer is based on an adequacy decision of the European Commission where one covers the recipient, including the EU–US Data Privacy Framework for certified recipients, and otherwise on the standard contractual clauses under Decision (EU) 2021/914 (Module 3), as permitted by Clause 7.8(b). If an adequacy decision is annulled or a recipient's certification lapses, the standard contractual clauses apply to that transfer instead.

A9. Personal data breaches. Serverpod notifies the Customer of a personal data breach affecting Customer Personal Data without undue delay, and in any case within 48 hours after becoming aware of it. Notices go to the account owner's email address. They contain the information in Clause 9.2, and Serverpod adds further information as it becomes available. A notice is not an admission of fault or liability by Serverpod.

A10. Audits. Serverpod first meets requests under Clause 7.6 with written information: its security documentation, answers to reasonable questionnaires and its sub-processors' current certifications and audit reports, where Serverpod is allowed to share them. If that is not enough, or there are indications of non-compliance, the Customer or an independent auditor bound by confidentiality may carry out an audit or inspection. Unless a supervisory authority requires otherwise or there are indications of non-compliance, inspections take place at most once every 12 months, during business hours and with at least 30 days' notice. The parties agree the scope and timing of an inspection in advance. An auditor may not be a competitor of Serverpod. An inspection covers Serverpod's own premises, systems and records. It does not give access to other customers' data, and for the data centres and systems of sub-processors Serverpod relies on their audit reports and certifications. The Customer treats audit results as confidential, but may share them with a supervisory authority under Clause 7.6(e). Each party bears its own costs of an audit.

A11. Special categories of data. The Customer decides what data it processes with Serverpod Cloud, and is responsible for assessing whether the safeguards in Annex II and Annex III are appropriate for that data. Where the Customer processes special categories of personal data under Article 9 GDPR, or personal data relating to criminal convictions and offences, these restrictions apply under Clause 7.5: the Customer does not place that data in environment variables, build configuration, logs or file names, and does not include it in app builds (see Annex IV, Codemagic). Serverpod Cloud is not offered for protected health information under the US Health Insurance Portability and Accountability Act (HIPAA) or for payment card data under PCI DSS, unless Serverpod has agreed to this in writing.

A12. Assistance. Serverpod assists the Customer under Clause 8 mainly through self-service tools: the Customer can access, export, correct and delete Customer Personal Data in its own databases and storage, and can view its logs. Log entries cannot be corrected or deleted individually; they are deleted automatically after the retention period in Annex II. Serverpod forwards data subject requests it receives to the Customer without undue delay

and does not answer them itself. Assistance that goes beyond reasonable effort may be charged at Serverpod's standard rates, agreed with the Customer in advance.

A13. Deletion and return. While its account is active, the Customer can export its data with standard tools, for example a database dump or a download of its storage buckets. Exports count as usage, so normal usage charges and limits apply. For 30 days after termination (the retrieval period), and whenever the Customer cannot export the data itself, for example because its account is suspended or a usage limit has been reached, Serverpod makes the data available on written request. The retrieval period ends early if the Customer deletes its projects or asks for earlier deletion. This is how data is returned under Clause 10(d); for all other data, the Customer chooses deletion. After the retrieval period, Serverpod deletes Customer Personal Data under Clause 10(d). Live data is deleted within 30 days after the retrieval period ends. Backups and logs expire on their normal schedule: database snapshots within 35 days and logs within 30 days. Sub-processors remove deleted data from their own systems and backups within the periods in their own terms, which can be longer (for Google Cloud, up to 180 days). Serverpod confirms the deletion in writing on request.

A14. Customer responsibilities. The Customer is responsible for the lawfulness of the processing it instructs. It has a legal basis for the Customer Personal Data it processes with Serverpod Cloud, gives data subjects the information the law requires, and gives Serverpod only instructions that comply with the law. Where the Customer acts as a processor, it confirms that its controller has authorised its instructions and the use of Serverpod and the sub-processors in Annex IV. The Customer is also responsible for what it controls: the security of its own application code and dependencies, its credentials and access tokens, who it invites to its projects, how it configures Serverpod Cloud, the region it selects, and any copies of its data it needs beyond the backups described in Annex II. The Customer keeps the account owner's email address up to date, because notices under this DPA are sent there.

A15. Customers outside the EEA. Where the Customer is established in a country outside the European Economic Area that is not covered by an adequacy decision of the European Commission, and Serverpod making Customer Personal Data available to the Customer is a transfer under Chapter V GDPR, Module Four (processor to controller) of the standard contractual clauses in the Annex to Implementing Decision (EU) 2021/914 applies to that transfer and forms part of this DPA. Serverpod is the data exporter and the Customer is the data importer. The docking clause (Clause 7 of those clauses) and the optional wording in their Clause 11(a) do not apply. Those clauses are governed by the law of Sweden, and disputes under them are resolved by the courts of Sweden. Annex I and Annex II of this DPA give the information for their Annex I.

A16. Other data protection laws. Where the UK GDPR or the Swiss Federal Act on Data Protection applies to the Customer's processing of Customer Personal Data, this DPA applies in the same way. References to the GDPR, to Union or Member State law and to supervisory authorities are then read as references to the corresponding UK or Swiss law and authorities. Where the California Consumer Privacy Act (CCPA) applies, Serverpod is the Customer's service provider. Serverpod processes Customer Personal Data only for the business purpose of providing Serverpod Cloud under the Terms. It does not sell or share that data, does not keep, use or disclose it for any other purpose or outside its direct business relationship with the Customer, and does not combine it with personal information

from other sources unless the CCPA allows it. Serverpod gives that data the level of privacy protection the CCPA requires, and tells the Customer within five business days if it can no longer meet these obligations. The Customer may then take reasonable and appropriate steps to stop and remedy any unauthorised use. The same applies under other US state privacy laws that set equivalent requirements.

A17. Requests from public authorities. If a public authority asks Serverpod to disclose Customer Personal Data, Serverpod refers the authority to the Customer where it can. Serverpod tells the Customer about the request without undue delay, unless the law prohibits this, and discloses only what the law requires. Serverpod does not disclose Customer Personal Data to public authorities voluntarily.

A18. Liability. Each party's liability under this DPA is subject to the limitations in the Terms, to the extent the law allows. This does not limit the rights of data subjects under Article 82 GDPR.

A19. Governing law. This DPA is governed by the law of Sweden. Disputes are resolved as set out in the Terms.

A20. Changes. Serverpod may update Part A and Annexes II to IV, for example to change sub-processors under A7 or improve security measures. Serverpod notifies the Customer of material changes at least 30 days in advance. A change may not reduce the overall level of protection, and the text of the Clauses never changes.

A21. Contact. Data protection questions: privacy@serverpod.dev. Security incidents: security@serverpod.dev.

Part B: Standard Contractual Clauses

The following text is Commission Implementing Decision (EU) 2021/915, Annex, word for word. The options chosen are Article 28 GDPR in Clause 1(a), Option 2 (general written authorisation, 30 days) in Clause 7.7(a), and the GDPR references in Clauses 8 and 9. The docking clause in Clause 5 is included. Source: Official Journal L 199, 7.6.2021, p. 18.

SECTION I

Clause 1: Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2: Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3: Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4: Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5: Docking clause (optional)

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II: Obligations of the Parties

Clause 6: Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7: Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

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

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss,

alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

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

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on

the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8: Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9: Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the

personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III: Final Provisions

Clause 10: Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

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

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its

instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

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

Annex I: List of parties

Controller(s):

Name	The Customer, as identified in its Serverpod Cloud account
Address	The address given in the Customer's account or billing details
Contact person's name, position and contact details	The account owner, at the email address registered for the account. The Customer's data protection officer, if it has one, as notified to Serverpod.
Signature and accession date	Signed by accepting the Terms. The accession date is the date the Customer accepted the Terms, or the date of a signed copy.

Processor(s):

Name	Serverpod AB, org. nr 559337-1213
Address	Sjöbjörnsvägen 46, 117 67 Stockholm, Sweden
Contact person's name, position and contact details	Data protection contact, privacy@serverpod.dev. Data protection officer: none appointed.
Signature and accession date	Signed by Serverpod by publishing this DPA as part of the Terms. The date the Customer accepted the Terms, or the date of a signed copy.

Annex II: Description of the processing

Categories of data subjects whose personal data is processed

The Customer decides which data subjects' data it processes. Typically:

- End users of the Customer's applications.
- The Customer's employees, contractors and other team members whose data appears in the Customer's content.
- Any other individuals whose personal data the Customer stores in, or sends through, Serverpod Cloud.

Categories of personal data processed

The Customer decides which personal data it processes. Typically:

- Identity and contact data, such as names, email addresses and user IDs.
- Authentication data, such as password hashes, sign-in codes and session tokens.
- Application content stored in the Customer's databases and files.
- Technical data, such as IP addresses, request metadata and application logs.

- Email addresses and one-time codes, where the Customer uses the Serverpod Cloud authentication email service.

Sensitive data processed (if applicable) and applied restrictions or safeguards

The Customer may process special categories of personal data at its own choice, subject to Part A, A11. Serverpod does not read or classify the content of Customer Personal Data, except where needed to give support the Customer has asked for, to investigate a security incident or suspected misuse of the service, or to comply with the law. Serverpod does collect operational metrics about each project, such as request counts, resource use and error rates, to run the service and to show them to the Customer. Serverpod applies the same safeguards to all Customer Personal Data:

- Processing only to provide the service, never for Serverpod's own purposes.
- Staff access only where needed to operate or support the service.
- Encryption in transit and at rest (Annex III).
- Each project's resources are separated from other customers' projects (Annex III).
- No onward transfers except to the sub-processors in Annex IV.

The Customer remains responsible for deciding whether these safeguards are enough for its data. For special-category data, the restrictions in Part A, A11 also apply.

Nature of the processing

Hosting and running the Customer's server applications; building container images from the Customer's source code; hosting databases, with backups and point-in-time restore; storing files; collecting and storing application and build logs; collecting operational metrics about the Customer's projects and showing them to the Customer; storing secrets and passwords; sending authentication emails to end users; caching responses at the network edge when the Customer enables it; building and publishing mobile apps when the Customer uses app builds; and deleting data.

Purpose(s) for which the personal data is processed on behalf of the controller

To provide, maintain, secure and support Serverpod Cloud for the Customer under the Terms.

Duration of the processing

For the term of the Terms, followed by deletion as set out in Part A, A13. Within that term, data is kept as follows:

Data	**Retention**
Database content	Until the Customer deletes it or the project
Database snapshots and restore history	Up to 35 days, depending on the plan
Application logs and build logs	30 days
Uploaded source code for deployments	Deleted 3 days after upload
Files in storage buckets	Until the Customer deletes them or the project
Container images	The latest image is kept until the project is deleted. Earlier images may be kept as deployment history, up to the number of versions the plan includes. Serverpod may

	delete earlier images at any time, and deletes all images when the project is deleted.
Authentication email records (recipient address, time, type)	30 days

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

See Annex IV. Sub-processors process Customer Personal Data only to provide their part of the service, for the duration set out above.

Annex III: Technical and organisational measures

Serverpod applies the measures below to all Customer Personal Data. Serverpod does not run its own data centres; infrastructure is provided by the sub-processors in Annex IV.

Measure	**What Serverpod does**
Pseudonymisation and encryption	All data is encrypted at rest by Google Cloud and by the database provider. Customer passwords and secrets are stored in Google Cloud Secret Manager. Secrets used during builds are encrypted with authenticated encryption (AES-256 or stronger), with the key wrapped by a hardware-backed (HSM) key that only the build service can use. Console user passwords and tokens are stored as hashes with a salt and secret pepper.
Protection of data during transmission	The console and API accept HTTPS only; plain HTTP is redirected. TLS certificates are managed by Google Certificate Manager, including for custom domains. Connections from the Customer's application to its database require TLS by default. The control plane reaches the hosting cluster over a private connection secured with TLS.
Protection of data during storage	Each project's secrets are synced only into that project's own namespace. Each project's storage buckets are accessed through a separate service identity for that project. Uploaded source code is deleted after the period in Annex II.
Confidentiality, integrity, availability and resilience	Each project runs in its own Kubernetes namespace, inside a sandboxed container runtime. Network policies block direct traffic from a project's containers to other projects, to the cluster's control plane and to the cloud metadata service. Application

	containers run as a non-root user, cannot escalate privileges, have all Linux capabilities removed and have no access to the Kubernetes API. CPU, memory, disk and outbound bandwidth are limited per container. Clusters run on private nodes, and base images are minimal and pinned to exact versions.
Restoring availability after an incident	Databases are replicated across availability zones within their region. Database snapshots and point-in-time restore keep the history set out in Annex II, and a project can be restored in one step. The control-plane database is protected against accidental deletion.
Regular testing and evaluation	Synthetic monitoring checks the console, the API and customer connectivity continuously, with alerts to the engineering team. Dependencies are updated automatically, and cluster nodes are patched by Google on the regular release channel.
User identification and authorisation	Customers sign in with email and password, Google or GitHub. Personal access tokens can be named, listed and revoked, and expire after 30 days without use by default. Users get access to a project only by invitation. Serverpod staff access production through role-based Google groups, not individual grants. Automated deployments use short-lived credentials limited to Serverpod's own code repositories, with no stored keys. Two-step verification is required for all staff accounts.
Physical security	Provided by Google Cloud and Amazon Web Services data centres, which hold ISO/IEC 27001 certification and SOC 2 audit reports.
Event logging	Google Cloud records every administrative change to the infrastructure (Admin Activity audit logs). Every use of the build-secrets key is logged. Application and build logs are kept for the period in Annex II.
System configuration, including default configuration	Infrastructure is defined as code and deployed through automated pipelines. Secure defaults: HTTPS redirect, database TLS required, sandboxed non-root containers. Infrastructure changes are reviewed before they are applied.
Internal IT and IT security governance	Serverpod has a named security owner and written security policies. All staff and

	contractors are bound by confidentiality undertakings and receive security training.
Certification and assurance	Serverpod holds no certifications of its own. Its infrastructure sub-processors are audited: Google Cloud (ISO/IEC 27001, 27017, 27018, SOC 2) and Databricks/ Neon (SOC 2 Type 2, ISO/IEC 27001). Serverpod provides their reports on request under Part A, A10 where it is allowed to share them, and otherwise points the Customer to the sub-processor's published compliance documentation.
Data minimisation	Serverpod processes only the data the Customer deploys or sends, and does not read its content except as set out in Annex II. Build credentials sent to the app-build service are removed after each build.
Data quality	The Customer controls its own data and can correct it at any time through its application, the console, the CLI or a direct database connection.
Limited data retention	Retention periods are set out in Annex II. When a project is deleted, Serverpod deletes its database, secrets, storage buckets, container images and running workloads. Remaining logs expire on the schedule in Annex II. Deletion after termination follows Part A, A13.
Accountability	Serverpod keeps this DPA, the sub-processor list and a record of processing activities (Article 30(2) GDPR).
Data portability and erasure	While its account is active, the Customer can export its database with standard PostgreSQL tools and download its storage buckets. Otherwise Serverpod makes the data available on request (Part A, A13). Erasure follows the project deletion described above.

Measures to assist the controller (Clauses 8 and 9)

- Data subject requests: Serverpod forwards any request it receives to the Customer without undue delay. The Customer can act on most requests itself through its own databases and storage. Log entries cannot be corrected or deleted individually; they are deleted automatically after the retention period in Annex II.
- Data protection impact assessments: Serverpod provides this DPA, the sub-processor list and the information in this Annex, and answers reasonable follow-up questions.
- Personal data breaches: Serverpod notifies the Customer within 48 hours of becoming aware of a breach (Part A, A9). The notice includes the information in Clause 9.2, and

the contact point is security@serverpod.dev. Serverpod follows a written breach response procedure.

Measures of sub-processors

Each sub-processor is bound by a contract with data protection obligations in substance equal to these Clauses (Clause 7.7(b)). Serverpod reviews each sub-processor's security documentation and certifications before engaging it.

Annex IV: List of sub-processors

The agreed list of sub-processors under Clause 7.7(a), Option 2, is the list published at https://serverpod.dev/legal/subprocessors as it stood on the date the Customer accepted the Terms, with any later changes made under Part A, A7. For each sub-processor, the list gives its name and address, the processing it carries out, the location of the processing and the basis for any transfer outside the EEA. Serverpod keeps a dated record of every change to the list. References in this DPA to the sub-processors in Annex IV are to the sub-processors on that list.

Some sub-processors are used only for specific features or support channels, as the list states. If the Customer does not use those features or channels, they process no Customer Personal Data for the Customer. A support channel or the AI assistant processes Customer Personal Data only if the Customer shares it there, and the Customer should do so only where that is needed to resolve its request.

The sub-processors on the list use sub-processors of their own, such as Amazon Web Services for the managed databases. These are not on the list. Serverpod keeps links to each sub-processor's own published list at the same address, and gives the Customer the current details on request.

Recipients the Customer instructs Serverpod to send data to, such as Apple App Store Connect and Google Play when publishing an app, are not sub-processors. They receive data on the Customer's behalf and under the Customer's own agreements with them.