

VNC-SAAS-LEG-06 · Version 1.2 · Effective 15 October 2026

Data Processing Agreement

Agreement on the processing of personal data on behalf of the Customer, with Annexes

This Data Processing Agreement ("DPA") is concluded between the Customer as controller and VNC – Virtual Network Consult AG, Poststrasse 24, 6302 Zug, Switzerland ("VNC") as processor. It implements Article 28 of the EU General Data Protection Regulation (GDPR) and Article 9 of the Swiss Federal Act on Data Protection (FADP) for the processing of personal data within **VNC**lagoon SaaS. It is accepted during signup and forms part of the Agreement.

1. Subject matter and duration

- 1.1 VNC processes personal data contained in Customer Data on behalf of the Customer for the purpose of providing **VNC**lagoon SaaS as described in the Service Description. Details of the processing are set out in Annex 1.
- 1.2 This DPA applies to **VNC**lagoon SaaS only. Deployments under a Master Services Agreement are governed by the Data Processing Agreement at vncagoon.com/data-processing.
- 1.3 The DPA applies for the duration of the Agreement and until all Customer Data has been deleted or returned under the Cancellation and Data Export Policy.

2. Instructions

- 2.1 VNC processes personal data only on documented instructions from the Customer. The Agreement, the configuration of the tenant by the Customer and the use of the service functions constitute the documented instructions. Additional instructions are given in writing to info@vnc.biz.
- 2.2 VNC informs the Customer without delay if it considers an instruction to infringe applicable data protection law.

- 2.3 Where VNC is required by Union, Member State or Swiss law to process personal data beyond the instructions, it informs the Customer of that requirement before processing, unless the law prohibits such information.

3. Confidentiality and personnel

- 3.1 VNC ensures that persons authorised to process personal data are bound by confidentiality and have received appropriate training. Access is granted on a need-to-know basis and logged.

4. Security

- 4.1 VNC implements the technical and organisational measures described in Annex 3 and reviews them regularly. VNC may update the measures provided the level of protection is not reduced.
- 4.2 The data centres used are certified to ISO 27001 and BSI C5 Type 2. VNC provides summaries of certificates and attestation reports on request under confidentiality.

5. Sub-processors

- 5.1 The Customer gives general authorisation to the engagement of the sub-processors listed in Annex 2. VNC imposes data protection obligations on sub-processors equivalent to those in this DPA and remains liable for their performance.
- 5.2 VNC informs the Customer of intended additions or replacements at least 30 days in advance by e-mail to the administrator and in the admin console. The Customer may object on reasonable data protection grounds within that period. If no solution is found, the Customer may terminate the Agreement with effect from the date of the change and receives a pro-rata refund of prepaid fees.

6. Location of processing and transfers

- 6.1 Personal data is stored and processed in data centres located in the European Union or in Switzerland. VNC does not transfer Customer Data to countries outside the EU, the EEA or Switzerland for the operation of the service.

- 6.2 Where a sub-processor listed in Annex 2 is established outside these territories or is subject to the laws of a third country, the transfer safeguard named in Annex 2 applies, in particular the EU Standard Contractual Clauses with the Swiss addendum, together with the supplementary measures described there.

7. Assistance to the Customer

- 7.1 VNC assists the Customer, taking into account the nature of the processing, in responding to requests from data subjects through the functions of the service and, where these are insufficient, through reasonable additional support.
- 7.2 VNC assists the Customer with data protection impact assessments and prior consultations, security of processing and breach notification, to the extent the information is not available to the Customer itself. Assistance beyond reasonable effort may be charged at VNC's standard rates.

8. Personal data breach

- 8.1 VNC notifies the Customer without undue delay and in any case within 36 hours after becoming aware of a personal data breach affecting Customer Data. The notification contains the information required by Article 33(3) GDPR to the extent available and is supplemented as information becomes available.
- 8.2 Notification is made to the administrator and the data protection contact recorded in the admin console.

9. Deletion and return

- 9.1 At the end of the Agreement, VNC deletes or returns personal data as described in the Cancellation and Data Export Policy, unless Union, Member State or Swiss law requires storage. Export functions allow the Customer to retrieve all Customer Data in commonly used formats at any time.

10. Audit

- 10.1 VNC makes available the information necessary to demonstrate compliance with this DPA, including certificates, attestation reports and summaries of audits of the data centres.

- 10.2 The Customer may conduct an audit, itself or through an independent auditor bound by confidentiality, once per year or after a personal data breach, with at least 30 days' notice, during business hours and without disrupting operations. Audits of shared infrastructure are satisfied by the third-party reports available. Costs of audits beyond the review of documents are borne by the Customer.

11. Liability and precedence

- 11.1 Liability under this DPA is subject to the liability provisions of the Subscription Terms, to the extent permitted by Article 82 GDPR and mandatory law.
- 11.2 In case of conflict between this DPA and other parts of the Agreement, this DPA prevails for the processing of personal data.

12. Annex 1 · Details of the processing

Item	Description
Subject matter	Provision of VNC lagoon SaaS: mail, calendar, contacts, chat, video, tasks, files, portal, personal hub, directory, channels, workflow and CRM in an isolated tenant.
Nature and purpose	Hosting, storage, transmission, display, backup, indexing for search, and deletion of Customer Data as directed by the Customer through the service.
Categories of data subjects	Users of the Customer (employees, contractors), the Customer's communication partners (customers, suppliers, applicants, other third parties), persons recorded in CRM and contacts.
Categories of personal data	Identification and contact data, account and authentication data, content of communications and files, calendar and task data, CRM and business relationship data, usage and log data. Special categories only where the Customer chooses to process them.
Duration	Duration of the Agreement plus the export and deletion periods of the Cancellation and Data Export Policy.
Location	Data centres in the European Union or in Switzerland.

13. Annex 2 · Sub-processors

Sub-processor	Service	Location	Safeguard
Hosting provider, EU location · legal name and address to be added before 15 October 2026	Data centre and infrastructure for the EU location	EU	Within the EU; ISO 27001, BSI C5 Type 2
Hosting provider, Swiss location · legal name and address to be added before 15 October 2026	Data centre and infrastructure for the Swiss location	Switzerland	Within Switzerland; ISO 27001
Stripe Payments Europe, Ltd., Dublin, Ireland	Payment processing and subscription billing (billing contact, payment and invoice data only; no Customer Data from the tenant)	Ireland; parent company in the USA	EU Standard Contractual Clauses and Swiss addendum within the Stripe group; EU-U.S. Data Privacy Framework certification

13.1 Changes are notified as set out in clause 5.

14. Annex 3 · Technical and organisational measures

- 14.1 Confidentiality: physical access control at certified data centres; logical access with role-based rights, single sign-on and enforced two-factor authentication for administrators; tenant isolation at application and data level; encryption of data in transit (TLS 1.2 or higher) and at rest.
- 14.2 Integrity: change management with review and staged deployment; logging of administrative actions; integrity checks on backups.
- 14.3 Availability: redundant infrastructure within the location; daily backups with retention of 30 days; tested restore procedures; monitoring and on-call operations; capacity management.
- 14.4 Resilience and recovery: documented incident response and business continuity plans; recovery objectives as stated in the Service Level Agreement.
- 14.5 Procedures for regular testing: vulnerability management, periodic penetration tests, review of measures at least annually.

- 14.6 Data minimisation and deletion: deletion routines per the Cancellation and Data Export Policy; pseudonymised log data; no use of Customer Data for product analytics beyond aggregated operational metrics.
- 14.7 Organisation: information security policy, confidentiality obligations and training for staff, sub-processor management.

PART OF THE VNCLAGOON SAAS AGREEMENT

[Service Description](#) [Subscription Terms](#) [Launch Offer Terms](#) [Cancellation and Data Export Policy](#)
[Acceptable Use Policy](#) [Service Level Agreement](#) [Sub-processors](#)