Griffin31 Data Processing Addendum

OnCloud Ltd. · Version 1.0 · Last updated 25 June 2026

This Data Processing Addendum (“DPA”) forms part of the Griffin31 Terms and Conditions (the “Agreement”) between OnCloud Ltd. (“OnCloud”) and the customer that accepted them (“Customer”). It applies when OnCloud processes Customer Personal Data while providing the Griffin31 service. Customer accepts this DPA by accepting the Agreement; no separate signature is required. If this DPA and the Agreement conflict on the processing of personal data, this DPA prevails.

1. Definitions

Terms not defined here have the meaning given in the Agreement.

- **Data Protection Laws** means all laws on the processing of personal data that apply to that processing. These include the EU General Data Protection Regulation 2016/679 (“GDPR”), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, and the Israeli Protection of Privacy Law 5741-1981 and its regulations.
- **Customer Personal Data** means personal data that OnCloud processes on behalf of Customer under the Agreement, as described in Annex I.
- **Sub-processor** means a third party engaged by OnCloud that processes Customer Personal Data.
- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
- **Standard Contractual Clauses** or **SCCs** means the clauses adopted by European Commission Implementing Decision (EU) 2021/914.
- **Controller**, **processor**, **data subject**, **personal data** and **processing** have the meanings given in the GDPR.

2. Scope, roles and instructions

1. **Roles.** Customer is the controller of Customer Personal Data, and OnCloud is its processor. If Customer is itself a processor for a third party, OnCloud is a sub-processor, and Customer is responsible for passing on the relevant obligations.
2. **Instructions.** OnCloud processes Customer Personal Data only on Customer’s documented instructions. Those instructions are the Agreement, this DPA, and Customer’s use and configuration of the service. OnCloud will tell Customer if, in its opinion, an instruction breaches Data Protection Laws. OnCloud may also process the data where Union, Member State or other applicable law requires it, and will inform Customer before doing so unless that law forbids it.
3. **Read-only access.** Griffin31 reads Customer’s Microsoft 365 configuration through read-only permissions and the Global Reader role. It makes no changes to Customer’s tenant. It does not read or store email, file, chat or document content. OnCloud collects only the data needed to produce recommendations, and avoids collecting personal data that isn’t required. Personal data from Customer’s tenant is limited to user principal names and the Microsoft security signals linked to them. It is held only in the data lake and is never copied into the application database.
4. **No AI training.** Customer Personal Data is not used to train, fine-tune or evaluate any artificial intelligence model, and is not sent to any third-party AI service.
5. **Customer responsibilities.** Customer is responsible for the lawfulness of the data it makes available to OnCloud. This includes granting administrative consent only through an authorised administrator, and revoking consent when it stops using the service.

3. Confidentiality of personnel

OnCloud ensures that everyone authorised to process Customer Personal Data has committed to confidentiality or is under an appropriate statutory duty of confidentiality. Access is limited to personnel who need it to provide, support or secure the service. Personnel are background-checked, sign a non-disclosure agreement and the Code of Conduct, and complete security and privacy training when they join and every year after.

4. Security measures

OnCloud implements and maintains the technical and organisational measures in Annex II, as Article 32 GDPR requires. These measures are independently audited under a SOC 2 Type II examination.

OnCloud may update these measures as technology and risks change, as long as an update does not materially reduce the overall level of protection.

5. Sub-processors

1. **General authorisation.** Customer gives OnCloud general written authorisation to engage Sub-processors. The current Sub-processors are listed in Annex III and on the Griffin31 website at https://kb.griffin31.com/trust-center/sub-processors/.
2. **Sub-processor terms.** OnCloud engages each Sub-processor under a written contract with data protection obligations that are no less protective than this DPA. OnCloud assesses each Sub-processor's security before engagement and at least once a year. OnCloud remains liable to Customer for each Sub-processor's performance.
3. **Notice of changes.** OnCloud will email the account owner at least 30 days before a new Sub-processor begins processing Customer Personal Data.
4. **Right to object.** Customer may object in writing on reasonable data protection grounds within that 30-day period. The parties will discuss the objection in good faith. If they can't resolve it, Customer may terminate the affected part of the service by written notice.

6. International transfers

1. **Hosting location.** Customer Personal Data is hosted in the Microsoft Azure North Europe region (Ireland).
2. **Access from Israel.** OnCloud is established in Israel, and its personnel may access Customer Personal Data from Israel. The European Commission has recognised Israel as providing an adequate level of protection (Decision 2011/61/EU), and the UK and Switzerland also recognise Israel as adequate.
3. **Onward transfers.** Where a Sub-processor processes Customer Personal Data in a country without an adequacy decision, OnCloud ensures an appropriate safeguard under Chapter V GDPR. This means the Sub-processor's certification under the EU–US Data Privacy Framework (with the UK Extension and Swiss–US framework where relevant), or the Standard Contractual Clauses (Module 3, processor to processor), with the UK Addendum and Swiss amendments where relevant. The safeguard for each Sub-processor is shown in Annex III.
4. **Supplementary measures.** Data is encrypted in transit and at rest. OnCloud will challenge any government request for Customer Personal Data that it considers unlawful, and will inform Customer of such a request unless the law forbids it.

7. Data subject requests and assistance

1. **Data subject requests.** If OnCloud receives a request from a data subject about Customer Personal Data, it will forward the request to Customer without undue delay and won't respond itself unless Customer authorises it. Taking into account the nature of the processing, OnCloud will provide reasonable assistance for Customer to respond.

2. **Other assistance.** OnCloud will provide reasonable assistance with Customer's data protection impact assessments and prior consultations with supervisory authorities, to the extent they relate to OnCloud's processing and the information is available to OnCloud.

8. Personal data breach notification

1. OnCloud will notify Customer without undue delay after becoming aware of a Personal Data Breach, and in any case within 24 hours of confirming it. OnCloud will not delay confirmation unreasonably. Notice goes to the account owner's email address.
2. The notice will include, as far as known at the time: the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, the measures taken or proposed, and a contact point. OnCloud will provide more information as it becomes available.
3. OnCloud will take reasonable steps to contain and investigate the breach and to reduce its effects.
4. Notifying Customer of a breach is not an admission of fault or liability.

9. Return and deletion

1. **Export.** During the subscription, or within 30 days after the Agreement ends, Customer may ask in writing for an export of its assessment results, recommendation states and history in JSON or CSV format.
2. **Deletion.** After that 30-day period, OnCloud will delete Customer Personal Data from its production systems in line with the Agreement and Data Protection Laws, following its documented Data Erasure Procedure. Copies in backups and soft-deleted storage expire automatically within 14 days after that.
3. **Exceptions.** OnCloud may keep Customer Personal Data only where the law requires it. Any data kept stays protected under this DPA and is used for no other purpose.
4. **Confirmation.** On request, OnCloud will confirm in writing that deletion is complete.

10. Audits and information

1. **Reports.** On request, OnCloud will provide its most recent SOC 2 Type II report and penetration test summary under a confidentiality agreement, along with the information reasonably needed to show compliance with this DPA.
2. **Audits.** If those materials aren't enough to meet an obligation under Data Protection Laws, or a supervisory authority requires it, Customer may audit OnCloud's compliance. Customer must give at least 14 days' written notice, and audits are limited to once in any 12 months unless a Personal Data Breach has occurred. Audits take place during business hours, through an independent auditor bound by confidentiality, and at Customer's cost. They must not compromise the security of other customers' data.

11. General

1. **Liability.** Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement, except where Data Protection Laws do not allow them.
2. **Term.** This DPA applies for as long as OnCloud processes Customer Personal Data, including after the Agreement ends until deletion under section 9 is complete.
3. **Changes.** OnCloud may update this DPA to reflect changes in Data Protection Laws or in the service. Material changes will be notified to the account owner at least 30 days in advance and will not reduce the protection of Customer Personal Data.
4. **Order of precedence.** If there is a conflict, the following documents apply in this order: (a) the Standard Contractual Clauses, where they apply; (b) this DPA; (c) the Agreement.
5. **Governing law.** This DPA is governed by the law that governs the Agreement, except where the Standard Contractual Clauses or Data Protection Laws require otherwise. The Agreement and this DPA are governed by the laws of the State of Israel, and the competent courts of Tel Aviv-Jaffa have exclusive jurisdiction. Where the Standard Contractual Clauses apply, they are governed by the laws of Ireland.

6. **Contact.** Privacy questions: privacy@griffin31.ai. Security incidents: support@griffin31.ai. A countersigned copy of this DPA is available on request at privacy@griffin31.ai.

Annex I: Details of processing

Item	Description
Controller (data exporter)	Customer, as identified in its Griffin31 account
Processor (data importer)	OnCloud Ltd., 49 Hasivim St., Petah Tikva 49170, Israel. Contact: privacy@griffin31.ai
Subject matter	Assessment of the security and compliance posture of Customer's Microsoft 365 tenant
Nature of processing	Reading tenant configuration through read-only Microsoft Graph and Exchange Online permissions; storing snapshots; evaluating them against rules; showing findings and recommendations in the web interface; sending service emails that contain a link to Griffin31 but no security findings or personal data other than the recipient's address
Purpose	Providing the Griffin31 service under the Agreement, including support and security of the service
Data subjects	Customer's Microsoft 365 users, administrators and guests whose directory records are read; Customer's users of Griffin31
Personal data	From Customer's tenant: user principal names (UPNs) and the Microsoft security signals linked to them, such as role assignments, authentication method registration, sign-in and risk signals, and device compliance. These are collected only where a recommendation needs them, and stored only in the data lake. Griffin31 user data: identifier, email address, role, activity history, stored in the application database. Operational logs that may contain identifiers
Excluded data	Email, file, chat and document content; passwords
Special categories	None intended
Frequency	Continuous for the subscription term; tenant scans run on a schedule or when a user requests them
Retention	For the subscription term, then deleted as described in section 9
Location	Microsoft Azure North Europe (Ireland). Sub-processor locations are in Annex III

Annex II: Technical and organisational measures

Area	Measures
Assurance	Annual SOC 2 Type II examination (Security, Availability, Confidentiality); annual independent penetration test; security policies reviewed and approved every year

Area	Measures
Encryption	TLS 1.2 or higher in transit; AES-256 at rest for the database, storage and container registry
Customer tenant access	Read-only permissions and the Global Reader role; access through workload identity federation with no stored secret; customer can revoke consent at any time
Application access	Sign-in through the customer's Microsoft Entra ID, so the customer's MFA and Conditional Access apply; role-based access, denied by default; each session scoped to one customer account
Personnel access	Single sign-on with MFA; least privilege and role-based access; just-in-time administrative credentials; annual access reviews; access removed when personnel leave
Network	Production isolated from development and staging; no inbound internet access except through the Cloudflare web application firewall; database without a public endpoint; administration only through zero-trust remote access from managed devices
Secure development	Peer and code-owner review before every merge; signed commits; automated code, dependency and secret scanning; separate environments; production data never used in development or testing
Vulnerability management	Continuous cloud posture monitoring; regular vulnerability scans; remediation within 2 weeks (critical), 1 month (high), 3 months (medium), 6 months (low)
Monitoring	Centralised security monitoring and SIEM; tamper-protected logs; alerts reviewed by security personnel
Availability and recovery	Zone-redundant application tier; geo-redundant database backups with 14-day point-in-time restore; recovery tested quarterly; database recovery time objective 2 hours, recovery point objective 5 minutes
Incident response	Documented incident response plan, tested every year, including breach notification
Endpoints	Company-managed devices with MDM, full-disk encryption and EDR
Personnel	Background checks; confidentiality agreements; security and privacy training at onboarding and every year
Vendors	Security assessment before engagement and every year; data processing terms with every Sub-processor

Annex III: Sub-processors

The five Sub-processors below process Customer Personal Data. They are current as of the date of this DPA. OnCloud announces changes as described in section 5.

Sub-processor	Purpose	Personal data	Location	Transfer safeguard
Microsoft Azure (Microsoft Ireland Operations Ltd.)	Hosting of compute, storage and database	All Customer Personal Data, encrypted at rest: tenant UPNs and security signals in the data lake; Griffin31 user accounts in the application database	North Europe (Ireland)	Within EEA
Microsoft Entra ID (Microsoft Ireland Operations Ltd.)	Customer sign-in and administrative consent	Identity metadata	European Union	Within EEA
Cloudflare, Inc.	DNS, TLS termination, web application firewall	Data in transit only	Global edge network	EU–US Data Privacy Framework; SCCs as fallback
Datadog	Application monitoring and logs	Telemetry that may contain identifiers	European Union	Within EEA
Postmark (ActiveCampaign, LLC)	Transactional email such as invitations and alerts	Recipient email address only. Emails contain a short notification and a link to Griffin31, with no security findings or other personal data	United States	Standard Contractual Clauses

Other services OnCloud uses to run its business, such as source control and credential management, receive no Customer Personal Data and are not Sub-processors.