Olyteck Cyber
Cybersecurity for Microsoft 365

LEGAL · CONTRACT

Data Processing Agreement

Pre-signable DPA covering Olyteck's processing of customer personal data on behalf of a controller. Includes EU Standard Contractual Clauses (Module Two) by reference.

Document	Olyteck Cyber - Data Processing Agreement
Version	1.0 - 29 May 2026
Operator	Olyteck - France
Scope	All Microsoft 365 tenant data processed by Olyteck Cyber
Classification	Public

1. Parties and definitions

This Data Processing Agreement (the "DPA") applies between the customer (the "Controller") and Olyteck (the "Processor") for the processing of personal data by Olyteck Cyber on behalf of the Controller.

Terms such as "personal data", "processing", "data subject", "controller", "processor", and "sub-processor" have the meanings given to them in the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR").

2. Scope, subject matter and duration

- Subject matter: provision of Olyteck Cyber - a security-posture scanner for Microsoft 365 - to the Controller.
- Duration: for as long as the Controller's account is active, plus the retention periods set out in section 8.
- Nature of the processing: reading configuration and permission metadata from the Controller's Microsoft 365 tenant via Microsoft Graph, evaluating it against security checks, and storing aggregate findings on Olyteck's servers.
- Categories of data subjects: end users of the Controller's Microsoft 365 tenant referenced in findings (for example, administrators without multi-factor authentication).
- Categories of personal data: administrative identifiers such as user principal names, display names, group memberships, sign-in timestamps, and access metadata. Olyteck does not process message bodies, file contents, or attachments.

3. Olyteck's obligations as processor

- Process personal data only on the Controller's documented instructions, including the act of using the product.
- Ensure that personnel with access are bound by confidentiality.
- Implement the technical and organisational security measures described in Annex 2.
- Assist the Controller in responding to data-subject rights requests, including access, rectification, erasure, and portability, to the extent reasonably possible.
- Notify the Controller without undue delay - and within 72 hours of confirmation - of any personal-data breach affecting the Controller's data.
- Make available to the Controller the information necessary to demonstrate compliance with Article 28 of the GDPR.
- Delete or return the personal data at the end of the service, except where EU or French law requires further storage (for example, accounting retention).

4. Sub-processors

The Controller authorises Olyteck to engage the sub-processors listed in Annex 3. Each is bound by a written contract imposing data-protection obligations equivalent to those in this DPA.

Olyteck gives at least 30 days' notice before adding or replacing a sub-processor that materially handles Controller personal data. Notice is given by e-mail and on the public Trust Center.

5. International transfers

Application data and backups are processed and stored exclusively in the European Union. Where a sub-processor operates outside the European Economic Area, the transfer is governed by the European Commission's Standard Contractual Clauses (Decision 2021/914), Module Two (controller to processor), incorporated by reference into this DPA. Additional technical safeguards including encryption in transit and access control apply in every case.

6. Security of processing

Olyteck implements the technical and organisational measures set out in Annex 2 of this DPA, designed to ensure a level of security appropriate to the risk to the rights and freedoms of natural persons.

7. Audit cooperation

Olyteck makes available to the Controller documentation reasonably necessary to demonstrate compliance with this DPA, including the Security and Architecture Documentation, the most recent external penetration-test summary (redacted), and the Information Security Policy executive summary. On reasonable notice, and not more than once per year, the Controller may request additional information; in-person audits are arranged by mutual agreement and may be replaced by independent third-party reports.

8. Return and deletion of data

On termination, Olyteck deletes the Controller's tenant configuration, findings, and audit data within 30 days of confirmation, except for billing records that Olyteck is required to retain under French and EU accounting law. A deletion confirmation is provided on request.

Annex 1 - Description of the processing

Subject matter	Operation of Olyteck Cyber for the Controller
Nature and purpose	Read configuration metadata from Microsoft 365 via Microsoft Graph; evaluate against security checks; present findings to the tenant administrator
Duration	Term of the Controller's subscription
Categories of data subjects	End users of the Controller's Microsoft 365 tenant referenced in findings
Categories of personal data	Administrative identifiers (user principal name, display name, group memberships, sign-in metadata)
Sensitive data	None - the product is not designed to host special-category data

Annex 2 - Technical and organisational measures

- Encryption in transit: TLS 1.2 or TLS 1.3 with modern cipher suites for all public endpoints.
- Encryption at rest: AES-256 disk encryption or provider-managed equivalent for all persistent storage and backups.
- Authentication: end-user authentication delegated to Microsoft Entra ID with the Controller's own multi-factor and conditional-access policies.
- Access control: principle of least privilege; named operator accounts; access reviewed quarterly; audit logging of administrative actions.
- Secure development: private repository with branch protection, peer code review on every change, automated dependency-vulnerability scanning.
- Vulnerability management: continuous internal scanning, periodic external penetration testing, documented severity-based remediation service levels.
- Logging: append-only security event log retained at least 12 months.
- Backups: daily encrypted backups in the European Union with a 30-day rolling window.
- Incident response: documented process with 72-hour notification of personal-data incidents in line with GDPR Article 33.
- Personnel: confidentiality commitments on hire; security awareness training; multi-factor authenticated workstations.

Annex 3 - Authorised sub-processors

Sub-processor	Service	Region
Microsoft Corporation	Microsoft Entra ID and Microsoft Graph (Controller's own M365 tenant)	Controller-controlled
EU cloud hosting provider	Infrastructure-as-a-service hosting	European Union (France)
Stripe Payments Europe, Ltd.	Card payment processing and subscription billing	European Union / Ireland

Sub-processor	Service	Region
Microsoft 365 (Exchange Online)	Transactional and notification e-mail delivery	European Union
Cloudflare, Inc.	DNS and edge protection for the public marketing surface	Global (with EU PoPs)

An up-to-date sub-processor list is also published at cyber.olyteck.com/trust.

Issued as-is

This DPA is issued by Olyteck and may be relied upon as-is during prospect evaluation and procurement. A counter-signed copy is provided on customer request as part of the contracting paperwork.