beenet

TEMPLATE V1.0

ENTERPRISE TRUST, SECURITY & REGULATORY COMPLIANCE

GDPR ARTICLE 28 EXECUTION TRACK

DATA PROCESSING ADDENDUM

Data Processing Agreement

GDPR Article 28 — Controller / Processor Terms

PARTIES & KEY TERMS	
CONTROLLER **[Customer legal name — full registered legal entity name]**	PROCESSOR **TAKISOFT 2.0 (trading as BeeNet)**
REGISTERED ADDRESS [Customer registered address]	REGISTERED ADDRESS 200 rue de la Croix Nivert, 75015 Paris, France
EFFECTIVE DATE [Date, on countersignature]	TERM Co-terminous with the underlying Service Agreement

PREAMBLE

This Data Processing Agreement forms part of the agreement for use of the BeeNet platform between Customer and TAKISOFT 2.0. It sets out the terms under which BeeNet processes personal data that Customer's organization submits to or generates within BeeNet — messages, attendance, grades, homework and related records — solely on Customer's documented instructions, per GDPR Article 28.

EU / UK GDPR — ART. 28

Data Processing Agreement covering sub-processors, transfers and security measures.

COPPA SCHOOL OFFICIAL / GDPR-K

Pupil data processed solely on the school's instructions, never for commercial purposes.

1. SUBJECT MATTER AND DURATION

BeeNet processes personal data on Customer's behalf to provide the BeeNet communication and school-management platform, as described in the Service Agreement. This DPA applies for the duration of the Service Agreement and for as long afterward as BeeNet retains Customer's personal data under Section 9 (Deletion and return).

2. NATURE AND PURPOSE OF PROCESSING

Hosting, storage, transmission, and display of the personal data Customer's organization submits to or generates within BeeNet, for the purpose of operating messaging, attendance, scheduling, homework, grading, transportation, and related school-administration features Customer has configured — never for BeeNet's own purposes (marketing, profiling, or resale).

3. CATEGORIES OF PERSONAL DATA

Account and identity data (name, email, phone, organization membership, guardian relationships), authentication/security data (device identifiers, login history), communication content (messages, attachments, channel membership, and the text of SMS and WhatsApp messages sent by Customer or received as SMS replies), and school-submitted educational data (attendance, behavior notes, grades, homework, transportation, daily recaps). Special category data: none collected by design beyond what Customer itself submits into notebooks/behavior notes, which remains Customer's own data under Customer's instructions.

4. CATEGORIES OF DATA SUBJECTS

Pupils/students, parents/guardians, instructors/teachers, organization administrators, and (where the transportation module is used) drivers.

5. PROCESSOR OBLIGATIONS

a. Process only on documented instructions from Customer, including regarding international transfers, unless required otherwise by EU or member state law (in which case BeeNet informs Customer first, unless prohibited).

b. Ensure confidentiality of any person authorized to process the data, under a duty of confidentiality (contractual or statutory).

c. Implement appropriate technical and organizational security measures per GDPR Article 32 — see Annex 3.

d. Respect the conditions for engaging sub-processors in Section 6.

e. Assist Customer, insofar as possible given the nature of processing, in responding to data-subject rights requests via privacy@beenet.app.

f. Assist Customer with its Article 32–36 obligations (security, breach notification, DPIAs, prior consultation with supervisory authorities), taking into account the information available to BeeNet. Customer's own supervisory authority for this purpose is its national data protection authority [name Customer's DPA here, e.g. CNPD for Luxembourg, ICO for the UK, CNDP for Morocco] — distinct from CNIL, BeeNet/TAKISOFT 2.0's own supervisory authority.

g. Delete or return all personal data at the end of the Service Agreement, per Section 9, and delete existing copies unless EU/member-state law requires retention.

h. Make available the information necessary to demonstrate compliance with this Article and allow for and contribute to audits, including inspections, conducted by Customer or an auditor Customer mandates. Audits may be conducted no more than once per 12-month period (or following a breach affecting Customer's data), on at least 30 days' written notice, during normal business hours, with the auditor bound to confidentiality. BeeNet may first offer a current third-party audit report (Annex 4); Customer may still require an inspection for anything that report doesn't resolve. Each party bears its own audit costs, unless the audit finds a material breach of this DPA, in which case BeeNet bears Customer's reasonable costs.

i. Notify Customer without undue delay after becoming aware of a personal data breach affecting Customer's data, describing its nature, likely consequences, and measures taken or proposed. BeeNet targets initial notification within 72 hours of becoming aware — an operational target, distinct from BeeNet's own separate Article 33 duty to notify its own supervisory authority within 72 hours.

j. Immediately inform Customer if, in BeeNet's opinion, an instruction infringes GDPR or other applicable EU or member-state data protection provisions (Art. 28(3), final sentence).

6. SUB-PROCESSORS

Customer authorizes BeeNet's engagement of the sub-processors listed in Annex 2, each bound by data-protection terms no less protective than this DPA (general authorization under Art. 28(2)). Where a sub-processor fails to fulfil its data protection obligations, BeeNet remains fully liable to Customer for that sub-processor's performance, per Art. 28(4).

BeeNet will give Customer at least 30 days' advance notice of any intended addition or replacement of a sub-processor (or, for urgent security/operational reasons, as much notice as practicable), during which Customer may object on reasonable grounds. If the parties cannot resolve an objection, either party may terminate the Service Agreement solely as to the affected processing, on written notice, without penalty.

7. INTERNATIONAL TRANSFERS

Where a sub-processor is located outside the EU/EEA (see Annex 2), transfers rely on the Standard Contractual Clauses' Module 3 (Processor-to-Processor, Commission Decision 2021/914) — or the sub-processor's own EU-U.S. Data Privacy Framework certification where applicable — plus supplementary technical measures (encryption in transit, data minimization) — per beenet.app/privacy §8.

8. DATA SUBJECT REQUESTS

If BeeNet receives a request directly from a data subject relating to Customer's data, BeeNet will not respond directly (other than to confirm receipt) and will promptly forward the request to Customer, who remains responsible for the substantive response as Controller.

9. DELETION AND RETURN

On termination of the Service Agreement, BeeNet will, at Customer's choice, delete or return all personal data, except where EU or member-state law requires continued storage (e.g. billing records, 7 years, French commercial law).

10. LIABILITY

As set out in the Service Agreement's Limitation of Liability clause.

11. GOVERNING LAW

France, unless the parties agree to a different governing law or dispute-resolution forum in the Order Form or an amendment to this DPA.

ANNEX 1 — PROCESSING DETAILS

Subject matter, duration, nature, purpose, data categories and data subjects are as stated in Clauses 1–4 above.

Reused verbatim from beenet.app/privacy §7. This annex must always match the live public page exactly at signature time — do not let this table drift from it.

PROVIDER	PURPOSE	DATA LOCATION
Microsoft Azure (Microsoft Ireland Operations Ltd.)	Application hosting, SQL database, blob storage, Redis cache, Service Bus, Notification Hubs, Communication Services (transactional email), Application Insights, Key Vault, Log Analytics	EU: Azure West Europe (Netherlands); geo-redundant database backups and file storage replicated to the paired region North Europe (Ireland)
Cloudflare, Inc. (USA)	CDN, WAF, DDoS protection, DNS	Global edge network, EU data-residency configuration
Twilio Inc. (USA)	Delivery of SMS login codes (Twilio Verify API); invitations by WhatsApp or SMS (WhatsApp messages are passed on to Meta, see next row); account-creation SMS; SMS notifications (emergency alerts by default, plus categories Customer enables) and SMS campaigns sent by Customer; receipt of SMS replies from recipients (including STOP opt-outs)	Twilio global network. Data: phone number; recipient's role, organization name and inviter's name (invitations, account-creation SMS); full text of SMS/WhatsApp messages, which may contain personal data written by Customer; text of recipients' SMS replies
Meta Platforms Ireland Limited (WhatsApp Business Platform)	Delivery of invitations sent by WhatsApp (relayed through Twilio). Applies only when an invitation goes out by WhatsApp; SMS invitations go through Twilio only	Meta global infrastructure; transfers to Meta Platforms, Inc. (USA) under the EU-U.S. Data Privacy Framework, or otherwise SCCs Module 3 (Meta Data Transfer Addendum). Data: recipient's phone number, inviter's name, organization name, role, invitation text
Google LLC (USA)	Firebase Cloud Messaging (Android push), Play Integrity API, Google Maps Platform (bus tracking)	Google global infrastructure
Apple Inc. (USA)	Apple Push Notification service, App Attest	Apple global infrastructure
Cloudflare, Inc. (Turnstile) (USA)	Bot protection on the public demo request form (website only)	Global

BeeNet does not use third-party analytics or advertising SDKs in the mobile app.

Reused from beenet.app/privacy §12.

ENCRYPTION

- **In transit** — TLS 1.2+ for all connections, HSTS preload enforced, Certificate Transparency monitored.
- **At rest** — Azure SQL Transparent Data Encryption (TDE), Azure Blob Storage encryption, Key Vault HSM-backed key management.
- **OTP codes** — salted SHA-256 hashing with constant-time comparison.

ACCESS CONTROLS

- Role-based access control (RBAC) on all data.
- Managed identities for service-to-service authentication (no shared passwords).
- Private network endpoints for all data stores (no public internet access to databases).
- Multi-factor authentication enforced for administrators.
- Progressive lockout on failed login attempts.

MOBILE SECURITY

- Device-bound refresh tokens (cannot be used from a different device).
- Device integrity attestation (Play Integrity / App Attest).
- Secure storage via Android Keystore and iOS Keychain.
- Automatic session expiration.

OPERATIONAL & ADMINISTRATOR ACCESS

- Regular security audits and dependency vulnerability scanning.
- Immutable audit logs for all administrative actions.
- Incident response procedures aligned with GDPR notification requirements.
- Admin access to org data is logged, minimum-scope, and forbidden for SuperAdmin accounts.

Message encryption notice: messages are encrypted at rest and in transit; BeeNet does not currently offer end-to-end encryption. Authorized administrators within Customer's organization, and in limited audited support scenarios BeeNet administrators, may technically access message content.

TAKISOFT 2.0 holds no first-party security certification of its own. What is true and independently verifiable is that every sub-processor in Annex 2 holds current third-party certifications, checked 2026-09-30 — reverify before each signature, as these lapse and renew.

SUB-PROCESSOR	CERTIFICATIONS HELD
Microsoft Azure	ISO/IEC 27001, SOC 1/2/3 Type 2, ISO 27017, ISO 27018, ISO 27701, PCI DSS, and others (Microsoft Learn: Azure compliance offerings)
Twilio	ISO/IEC 27001, ISO 27017, ISO 27018, SOC 2 (Type I; Type II reports available on request) (Twilio Trust Center)
Cloudflare	ISO 27001 (since 2019), ISO 27701, ISO 27018, SOC 2 Type II, PCI DSS Level 1 (Cloudflare Trust Hub)
Meta Platforms Ireland Limited (WhatsApp Business Platform)	Meta states it holds SOC 2 Type II and ISO 27001 reports for the WhatsApp Cloud API (Meta for Developers: WhatsApp data privacy & security). Applies to WhatsApp senders that run on Cloud API.
Google LLC (Firebase / Play Integrity / Maps)	ISO/IEC 27001:2022, SOC 1/2/3, ISO 27017, ISO 27018 (Google Cloud compliance)
Apple Inc. (used for APNs / App Attest)	ISO/IEC 27001, ISO/IEC 27018 covering Apple's internet services generally. Apple's certification page names example in-scope services (Apple School Manager, Apple Business Manager) but doesn't explicitly enumerate APNs/App Attest — treat as "falls under Apple's general scope," not a service-specific guarantee, until confirmed directly with Apple.

Disclaimer: *this annex describes the sub-processors' own, self-reported and independently published certifications — BeeNet does not audit or independently verify them, and does not warrant their continued accuracy. Reverify each row before relying on it; certifications lapse and renew.*

Signed by authorized representatives of both Parties, this Agreement takes effect on the date last signed below.

FOR AND ON BEHALF OF THE CONTROLLER

Name & title Date

FOR AND ON BEHALF OF THE PROCESSOR

TAKISOFT 2.0

Name & title Date

BEFORE SIGNING

This template is provided for informational purposes and to speed up procurement review. BeeNet recommends each party have this Agreement reviewed by its own legal counsel before execution, and complete the Controller's legal name, registered address and effective date above.