Data Processing Agreement and Schedules

Version 2026-10-30.1 | 30 October 2026 | CBX Media LLC

1. Parties, scope and duration

The controller is the Customer identified in the service order. The processor is CBX Media LLC, Shams Business Center, Sharjah Media City Free Zone, Sharjah, UAE, licence 2537521, represented by Laura Eva Bozic, General Manager. Privacy contact: privacy@marketing-aigency.com. This DPA is electronically concluded with the main agreement and applies to booked and activated modules, including the free trial and the free month of Performance Attribution, until return/deletion of customer data is complete. Where Customer processes for another controller, CBX acts as a subprocessor and Customer ensures the required authorisation.

CBX's own account, billing and website processing is separate. Customer data must not be used for CBX's own personal advertising, cross-customer profiling or model training.

2. Processing and instructions

Schedule A and the recorded module/account authorisations define purposes, persons and data. Operations comprise collection, transmission, normalisation/hashing, storage, matching, analysis, authorised advertising actions, export and deletion. GDPR special-category and criminal-offence data are excluded from the standard service. Detected prohibited content is restricted and addressed with Customer.

CBX acts only on documented instructions, including recipients and transfers, unless required by Union or Member State law; where permitted, CBX informs Customer before such processing. The agreement and recorded authorisations constitute initial instructions. Authorised workspace administrators or persons designated in writing may send further instructions to privacy@marketing-aigency.com. CBX promptly flags apparently unlawful instructions and suspends affected execution until lawfully resolved.

Customer is responsible for its collection grounds and notices. Ordering or activating a module is not visitor consent. Document 03 governs marketing attribution, conversion feedback and linked surveys. Hashes remain personal data. Attribution emails are temporarily received in plaintext, normalised and hashed; plaintext lead emails are not persistently stored for attribution.

3. Confidentiality and security

CBX restricts access to necessary authorised persons bound by confidentiality and implements Schedule B before affected processing begins. Measures may evolve with equivalent or greater protection; material changes are notified. No particular certification or completed penetration test is promised. Agreed controls and GDPR Article 32 remain binding.

4. Subprocessors

Customer generally authorises Schedule C providers for booked functions. CBX imposes equivalent data protection obligations and remains responsible for their performance. New/replacement providers are notified at least 30 days before access, stating function, data and locations. Customer may object on reasonable data-protection grounds. Affected access does not begin before resolution. If no reasonable solution exists, the affected service may end and prepaid fees for unperformed service are refunded. Urgent changes require suspension or express individual authorisation.

5. Assistance, incidents and audit

CBX assists with data subject rights and GDPR Articles 32–36, considering the processing and information available. Requests are forwarded without undue delay; identity and tenancy are verified before disclosure. Customer-related personal data breaches are notified without undue delay after awareness, targeting an initial, if necessary preliminary, notification within 24 hours. Missing details do not delay initial notification. Known scope, effects, measures and contact are provided and updated. Customer decides its statutory notifications.

CBX provides necessary evidence and permits audits, including inspections by Customer or a confidentially bound auditor. Reasonable notice and initial document review must not frustrate effective incident-driven audits.

6. Return, deletion and precedence

Customer chooses return followed by deletion or direct deletion where lawful. Document 04 governs formats, periods and backups. Legally required retention is separated, access-restricted and not used for other purposes. CBX confirms completion and any lawful residual retention.

Data of a cancelled add-on, and add-on data after a subscription ends, are kept blocked for 30 days and then deleted, as are the attribution data of Performance Attribution after the free month ends without a subscription or after the subscription ends; credentials of connected accounts without a paid plan, for example during and after the free trial or after a subscription ends, are deleted no later than 90 days after Customer's last login. Details are set out in document 04 section 2.

This DPA prevails on data protection issues; a valid transfer instrument prevails over it. Mandatory data subject rights, including GDPR Article 82, remain unaffected. Otherwise the main agreement’s liability provisions apply to the extent lawful. Electronic inclusion and acceptance are recorded with order ID and document version.

7. International processing and EU representative

Core infrastructure is intended to be in Frankfurt; necessary CBX remote access takes place from the UAE. Schedule C identifies international service providers and possible further processing. EU hosting does not mean exclusive EU processing.

Before the first affected transfer, CBX and Customer document the flow, roles, applicable transfer basis and necessary supplementary measures and supply the specific transfer schedule. Where SCCs 2021/914 apply to the particular importer processing, their unmodified official text and completed annexes are incorporated: Module 2 for controller-to-processor and Module 3 for processor-to-subprocessor. Clause 9(a): general authorisation with 30 days’ prior notice; no optional redress under Clause 11(a); Clauses 17/18: German law and German courts where permitted for the module. Party details derive from the service order and DPA; Schedule A describes transfers, B measures and C subprocessors. The competent authority under Clause 13 is specifically identified in the transfer record.

If importer processing is already subject to GDPR Article 3 and therefore outside those SCCs, another applicable effective basis is established before processing. Without a required valid basis the affected transfer does not start; if protection ceases, the transfer is suspended and Customer informed. Contract acceptance or technical activation alone does not satisfy this prerequisite. Only lawfully available functions may be activated; the main agreement’s rules on ending the free trial without cost and on cancellation remain applicable.

Official SCC text: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. The general selections here alone do not constitute a complete transfer record. The specifically agreed transfer schedule is supplied with Customer’s savable contract documents.

DIS-CONNECT GmbH, Gerwigstraße 29, 76131 Karlsruhe, Germany, info@dis-connect.de, acts solely as EU representative for privacy enquiries and regulatory correspondence. It receives only necessary case information, not general access to ad accounts, databases or attribution. Representation does not replace transfer safeguards.

Schedule A: Processing by booked module

Module	Individuals and data	Purpose / duration
Advertising/Reporting	account holders, users and contacts; account/campaign names, tokens, metrics, proposals, approvals and actions	management, analysis and authorised execution during use; document 04 periods
Attribution/Customer matching	visitors, leads and buyers; sanitised origin, click IDs, time, transient email/hash, consent, agreed purchase/revenue marker	attribution and measurement on documented grounds; raw data maximum 90 days
Conversion feedback	consenting visitors/leads; hash, click ID, event ID, time, sanitised source URL	specifically authorised platform and purpose in account configuration; document 04
Surveys	buyers; answers, expressly authorised order fields, optional attribution linkage	voluntary source research; raw data maximum 90 days
AI assistant/agents	users and persons in permitted content; inputs, campaign context, outputs	analysis, suggestions and authorised actions; normally 90 days, saved projects according to purpose
Optional speech	users; audio, transcript, language	transcription; audio at CBX transient only, transcript treated like chat

Unbooked or unauthorised functions receive no corresponding customer data. Content is minimised. Processing is ongoing according to use or event-driven according to authorised events.

Schedule B: Binding technical and organisational measures

- TLS in transit; appropriate at-rest encryption and AES-256-GCM for platform tokens; separate key access, no production secrets in browser or repository.
- Individual administrative accounts with multi-factor protection, necessary privileges, periodic review and prompt revocation; encrypted, updated and locked administrative devices.
- Tenant isolation through database policies and server authorisation, especially privileged service access; input validation, abuse controls and relevant mutation logs.
- No plaintext lead emails in persistent attribution or error logs; sanitised URLs and parameters; no sensitive form contents in advertising events.
- Purpose-specific consent before collection/transmission, covering withdrawal, retries and queued events; general storage permission alone is insufficient.
- Server enforcement of customer roles, authorised actions and entered budget limits; logging and stop/access-revocation facilities. Only Customer increases its ceiling.
- Encrypted backups, bounded rotation under document 04, documented recovery procedures and regular restore tests; deletion markers reapplied after restore.
- Incident/data-subject procedures, provider controls and at least annual and incident-driven review. Implementation and findings are recorded internally and evidenced on justified request.

Schedule C: Providers by function

Provider / address	Function / data	Processing and conditions
Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	database/auth/storage; module and account data	core project Frankfurt; international support/subprocessors; supabase.com/legal/dpa
Vercel Inc., 440 N Barranca Avenue #4133, Covina, CA 91723, USA	hosting/functions; requests, transient content, operational logs	EU functions, international CDN/support; vercel.com/legal/dpa
Anthropic, PBC, 548 Market St, PMB 90375, San Francisco, CA 94104, USA	model API; necessary campaign context, inputs/outputs	international processing under API terms, no permission to train on customer content; anthropic.com/legal/data-processing-addendum
Eleven Labs Inc., 169 Madison Ave #2484, New York, NY 10016, USA	optional transcription; audio/transcript	activated speech only; contract, retention and transfers secured before access
GitHub, Inc., 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA	automated jobs and encrypted backups; necessary job/log data	international processing, minimised logs, rotation under document 04

Authorisation does not permit unprotected transfers. CBX binds providers before access and records actual processing countries including remote access. Section 4 governs changes. Customer-directed Meta, Google and TikTok recipients are identified by function and actual account; applicable platform terms additionally govern joint or independent controllership. CBX's own payment/accounting providers are not technical subprocessors of customer attribution.

UAE customers

For UAE customers, these contractual safeguards also apply to booked processing under applicable UAE data-protection law. References to GDPR rights bind the parties contractually where applicable and do not displace mandatory UAE law or competent authorities. The main agreement determines governing law subject to mandatory rules and any prevailing transfer instrument.