DATA PROCESSING AGREEMENT

Polser, Inc. — Processor Template — Version 2.1

Processor (Data Importer)	Polser, Inc., 1111B South Governors Avenue 6368, Dover, DE 19904, USA — legal@polser.io
Controller (Data Exporter)	[CUSTOMER LEGAL ENTITY NAME] [REGISTERED ADDRESS] [DATA PROTECTION CONTACT EMAIL]
Effective Date	[DATE]
Governing Agreement	[MASTER SERVICE AGREEMENT / ORDER FORM] dated [DATE]
Version	2.1 — June 2026

This DPA covers EU GDPR and UK GDPR. For international transfers, Polser holds certification under the EU–US Data Privacy Framework (DPF) and UK Extension. Supplementary SCCs and UK IDTA are available in Schedule 1.

1. Background and Scope

1.1 This Data Processing Agreement ("DPA") forms part of the agreement between Polser, Inc. ("Polser" or "Processor") and the Customer identified on the cover page ("Controller") for the provision of Polser's SaaS platform services (the "Agreement").

1.2 This DPA governs the processing of Personal Data by Polser on behalf of the Customer in connection with the provision of the Services. In the event of conflict between this DPA and the Agreement, this DPA shall prevail to the extent of the conflict on data protection matters.

1.3 The parties acknowledge that:

- the Customer is the Controller of Personal Data processed through the Services;
- Polser is the Processor, acting only on the documented instructions of the Customer;
- this DPA implements the requirements of Article 28 EU GDPR and, where applicable, the UK GDPR.

2. Definitions

Terms defined in the Agreement or in applicable Data Protection Law shall have the same meaning where used here. The following additional definitions apply:

Term	Definition
Data Protection Law	All applicable laws and regulations relating to the processing of Personal Data, including (as applicable): EU GDPR (2016/679); UK GDPR as defined in the Data Protection Act 2018; the UK DPA 2018; and national implementing legislation.
Personal Data	Any information relating to an identified or identifiable natural person that Polser processes on behalf of the Customer, as further described in Annex A.
Processing	Any operation performed on Personal Data, whether or not by automated means, as defined in applicable Data Protection Law.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
Subprocessor	Any third party engaged by Polser to process Personal Data on Polser's behalf in connection with the Services.
Supervisory Authority	The relevant data protection supervisory authority, including the UK ICO and/or relevant EU data protection authorities.
SCCs	The Standard Contractual Clauses for the transfer of personal data to third countries adopted by the European Commission under Decision 2021/914.
UK IDTA / UK Addendum	The ICO's International Data Transfer Agreement (IDTA) and/or the ICO's International Data Transfer Addendum to the EU SCCs.
DPF	The EU–U.S. Data Privacy Framework and its UK Extension, administered by the U.S. Department of Commerce, to the extent Polser is a certified participant thereunder.

3. Processing Details

3.1 The subject matter, duration, nature, and purpose of the processing, and the categories of Personal Data and Data Subjects, are set out in Annex A to this DPA.

3.2 Polser shall process Personal Data only to the extent necessary to provide the Services and strictly in accordance with the Customer's documented instructions. The Customer's instructions are set out in this DPA and the Agreement. The Customer may issue further written instructions during the term.

3.3 If Polser is required by applicable European Union, European Union Member State, or United Kingdom law to process Personal Data otherwise than in accordance with the Customer's instructions, Polser will notify the Customer before such processing (unless prohibited by law on grounds of public interest). Polser shall promptly notify the Customer if, in its reasonable opinion, an instruction infringes Data Protection Law.

3.4 The Customer warrants that it has a lawful basis under Data Protection Law for processing the Personal Data it submits to the Services and that its instructions to Polser are lawful. Polser's obligation to follow instructions is conditional on those instructions being lawful.

4. Polser's Obligations as Processor

4.1 Confidentiality

Polser shall ensure that persons authorised to process Personal Data on its behalf are subject to appropriate obligations of confidentiality with respect to the Personal Data.

4.2 Security

Polser shall implement and maintain appropriate technical and organisational measures (TOMs) to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. A summary of Polser's current TOMs is set out in Annex B and at polser.io/trust. Polser may update its TOMs from time to time, provided that any updates do not materially reduce the overall level of security afforded to Personal Data.

4.3 Subprocessors

4.3.1 The Customer provides general written authorisation for Polser to engage Subprocessors. Polser's current list of Subprocessors is set out in Annex C and maintained at polser.io/trust. In the event of any conflict or discrepancy between the static list in Annex C and the dynamic list maintained at polser.io/trust, the online directory shall take legal precedence as the definitive record of approved Subprocessors.

4.3.2 Polser will provide at least 30 days' prior written notice before engaging a new Subprocessor or replacing an existing one. Such notice shall be delivered by direct email to the Customer's data protection contact identified on the cover page of this DPA, and/or via Polser's subprocessor change notification service (accessible at polser.io/trust), to which the Customer may subscribe to receive automated email alerts. During that period, the Customer may reasonably object to the change in writing, setting out the grounds for objection. Polser will work in good faith to address legitimate data protection concerns. If the parties cannot resolve the objection within 30 days, either party may terminate the relevant services on written notice, without liability for early termination fees on account of the data protection objection alone. The financial consequences of any such termination, including in respect of prepaid fees, shall be governed by the Agreement; provided, however, that if the Customer terminates under this clause due to a legitimate, documented data protection objection to a new Subprocessor, Polser shall issue a pro-rata refund of any prepaid, unearned fees calculated from the effective date of termination through the end of the then-current prepaid subscription term.

4.3.3 Polser shall impose data protection obligations on each Subprocessor that are substantially equivalent to those in this DPA. Polser remains fully liable to the Customer for the acts and omissions of its Subprocessors to the extent Polser would be liable if it had performed the processing directly.

4.4 Assistance with Data Subject Rights

4.4.1 Polser shall, taking into account the nature of the processing and insofar as reasonably practicable and technically feasible, assist the Customer by implementing appropriate technical and organisational measures to enable the Customer to respond to Data Subject rights requests under Data Protection Law (including rights of access, rectification, erasure, restriction, portability, and objection). Such assistance is provided at no additional charge where it is fulfilled through Polser's standard platform tooling and self-service features. Polser shall be entitled to charge the Customer at its standard professional rates where responding to Data Subject requests requires manual engineering intervention that goes materially beyond Polser's standard platform capabilities, or where the underlying Data Subject requests are manifestly unfounded or excessive within the meaning of applicable Data Protection Law.

4.4.2 Polser shall notify the Customer promptly (and in any event within 3 Business Days) if it receives a Data Subject request relating to Personal Data processed on the Customer's behalf. Polser shall not respond to such requests directly without the Customer's prior written authorisation.

4.5 DPIAs and Prior Consultation

Upon the Customer's reasonable written request, Polser shall provide, at no additional charge, such information and standard compliance documentation as is reasonably available and necessary to assist the Customer in conducting a data protection impact assessment (DPIA) or in complying with a prior consultation requirement under Data Protection Law (including, for example, completing standard security questionnaires or providing pre-existing compliance documentation). Polser shall be entitled to charge for such assistance at its standard professional rates only where the Customer requests bespoke documentation, custom security architecture assessments, or manual engineering resource that go materially beyond Polser's standard compliance outputs.

4.6 Records

Polser shall maintain records of its processing activities in relation to the Services as required by Article 30(2) EU GDPR and/or equivalent UK law, and shall make the portion of such records relating strictly to the Customer's processing available to the Customer on reasonable written request.

5. Personal Data Breach Notification

5.1 Polser shall notify the Customer without undue delay, and in any event within 48 hours, upon becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA.

5.2 Such notification shall include, to the extent available at the time:

- a description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records affected;
- the name and contact details of Polser's data protection contact;
- the likely consequences of the breach;
- the measures taken or proposed to address the breach and mitigate its effects.

5.3 Where not all information is available at the time of initial notification, Polser shall provide further information in follow-up communications without undue delay.

5.4 Polser shall cooperate reasonably with the Customer in connection with any regulatory notification or communication to Data Subjects that the Customer determines is required. The Customer is responsible for all required notifications to Supervisory Authorities and Data Subjects. Polser shall not make public statements or notifications regarding a Personal Data Breach without the Customer's prior written consent, except where required by applicable law.

6. International Data Transfers

6.1 Where the Services involve a transfer of Personal Data from the EEA or the UK to Polser in the United States, the parties agree that such transfers are made subject to the following transfer mechanisms, applied in the following order of priority:

6.1.1 EU–US Data Privacy Framework (DPF) and UK Extension — Primary Mechanism

Polser is a certified participant in the EU–U.S. Data Privacy Framework and the UK Extension to the EU–U.S. Data Privacy Framework, as administered by the U.S. Department of Commerce. The Customer's transfer of Personal Data to Polser is made under, and subject to, Polser's DPF certification to the extent that certification covers the processing in question. The Customer may verify Polser's current certification status at dataprivacyframework.gov/list.

6.1.2 Standard Contractual Clauses / UK IDTA — Fallback

To the extent that the DPF or UK Extension is invalidated, suspended, or does not cover a particular transfer, the parties agree to rely on the following supplementary transfer mechanism:

- For transfers from the EEA: the EU SCCs (Module 2: Controller to Processor) as adopted by Commission Decision 2021/914, as incorporated into Schedule 1 to this DPA.

- For transfers from the UK: the ICO UK IDTA or UK Addendum to the EU SCCs, as incorporated into Schedule 1 to this DPA.

6.2 The parties agree that Schedule 1 (incorporating the EU SCCs and UK Addendum) is hereby pre-executed and incorporated into this DPA. Schedule 1 shall apply automatically and immediately to any transfer of Personal Data from the EEA or UK to the United States to the extent that such transfer is not covered by a valid adequacy decision or the DPF. No further signature or manual activation is required for Schedule 1 to take effect.

6.3 Polser shall promptly notify the Customer if it ceases to be certified under the DPF or UK Extension, in which case the parties acknowledge that the pre-executed mechanisms in Schedule 1 shall automatically govern such transfers seamlessly and without interruption.

7. Audit and Compliance

7.1 Polser shall, upon the Customer's reasonable written request and at reasonable intervals (not more than once per calendar year unless there are reasonable grounds to suspect a material breach of this DPA), provide the Customer with such information as is reasonably necessary to demonstrate Polser's compliance with this DPA.

7.2 Polser shall, as its primary method of demonstrating compliance, make available to the Customer the following upon written request:

- Certifications and reports: relevant summaries of third-party audits, ISO certifications, penetration test reports, or equivalent (subject to appropriate redactions); or, where no third-party audit has been conducted, a completed information security questionnaire or written summary of Polser's security practices prepared by Polser's technical team.
- Security questionnaire: a completed industry-standard security questionnaire (such as the one provided by the Customer) within a reasonable timeframe.

7.3 Where the Customer demonstrates in writing that the information provided under clause 7.2 is insufficient to satisfy a specific regulatory audit requirement and that a physical inspection is required by applicable Data Protection Law, Polser shall permit such inspection subject to:

- at least 30 days' prior written notice;
- the Customer entering into a confidentiality agreement covering information obtained during the audit;
- the audit being conducted by the Customer's internal compliance personnel or a mutually approved, independent third-party certified auditor, such approval not to be unreasonably withheld or delayed;
- such auditor not being a direct or indirect competitor of Polser, and Polser having the right to object to any proposed auditor on reasonable grounds of conflict of interest or competitive sensitivity;
- such auditor entering into a direct confidentiality agreement with Polser covering all information obtained during the audit, prior to commencing the inspection;
- the audit being conducted during normal business hours with minimum disruption to Polser's operations;
- the Customer bearing all costs of any such physical audit, unless the audit is initiated following a confirmed Personal Data Breach caused by Polser, or reveals a material breach of this DPA by Polser, in which case Polser shall bear its own reasonable costs of facilitating the audit.

7.4 The Customer shall treat all information obtained through the audit process as Polser's confidential information.

8. Data Return and Deletion

8.1 Upon termination or expiry of the Agreement, or upon the Customer's earlier written request, Polser shall, at the Customer's written election, either:

- securely delete or destroy all Personal Data processed under this DPA; or
- return to the Customer (in a commonly used, machine-readable format via Polser's standard self-service platform export features) all Personal Data then held by Polser on the Customer's

behalf. Any custom or bespoke data extraction requests requiring manual engineering resources shall be subject to a mutually agreed professional services statement of work.

8.2 Polser shall complete such deletion, destruction, or return within 60 days following the termination date or receipt of the Customer's written instruction, and shall provide written certification to the Customer upon completion.

8.3 Notwithstanding clause 8.1, Polser may retain Personal Data to the extent required by applicable Union, Member State, or UK law (such as statutory tax or corporate record-keeping obligations), provided that Polser shall isolate such retained data, continue to apply the protections of this DPA to it, notify the Customer of the retention obligation to the extent permitted by law, and securely delete it as soon as the statutory retention obligation expires.

8.4 Polser uses AWS DynamoDB point-in-time recovery (PITR) as its primary backup mechanism. Following deletion of Personal Data, residual copies may be retained within the PITR recovery window for up to 35 days; such residual copies are subject to the protections of this DPA and are automatically purged upon expiry of that recovery window in the ordinary course of Polser's infrastructure operations.

9. Term

9.1 This DPA commences on the Effective Date and remains in force for the duration of the Agreement and until all Personal Data has been deleted or returned pursuant to clause 8.

9.2 Obligations that by their nature should survive termination (including clauses 5, 7, and 8) shall survive termination of this DPA.

10. Liability

10.1 Each party's liability under or in connection with this DPA is subject to the exclusions and limitations of liability set out in the Agreement. Nothing in this clause or the Agreement shall limit or exclude either party's liability to Data Subjects or Supervisory Authorities under the fallback Standard Contractual Clauses incorporated into Schedule 1. Nothing in this DPA is intended to reduce or exclude either party's liability for:

- death or personal injury caused by negligence;
- fraud or fraudulent misrepresentation;
- any other liability that cannot be excluded or limited under applicable law.

10.2 The parties agree that in the event of a claim by a Data Subject or a Supervisory Authority arising from a breach of this DPA, liability between the parties shall be apportioned to reflect the degree of responsibility of each party for the damage caused, in accordance with Article 82 EU GDPR.

11. General

11.1 This DPA, together with the Agreement and its Annexes, constitutes the entire agreement between the parties with respect to the processing of Personal Data in connection with the Services.

11.2 Polser may update this DPA to reflect changes in applicable Data Protection Law by providing the Customer with at least 30 days' prior written notice. If such update materially and adversely reduces the data protection protections afforded to the Personal Data, the Customer may object in writing within the 30-day notice period. The parties shall negotiate in good faith to resolve the objection; provided, however, that no termination right shall apply if the amendment is strictly required to comply with a mandatory change in applicable Data Protection Law or a binding order from a Supervisory Authority. If no agreement is reached within 30 days of the objection, either party may terminate the affected Services as its sole remedy, without liability for early termination fees. The financial consequences of any such termination shall be governed by the Agreement; provided that if the Customer terminates due to a legitimate objection to a material, adverse reduction in data protection, Polser shall issue a pro-rata refund of any prepaid, unearned fees for the terminated Services.

11.3 This DPA shall be governed by and construed in accordance with the laws applicable to the Agreement for general commercial matters; provided, however, that data protection matters arising

under this DPA shall be governed by the laws of Ireland (in respect of EU GDPR processing) or the laws of England & Wales (in respect of UK GDPR processing), as applicable, consistent with and without prejudice to the governing law provisions set out in Schedule 1. Any disputes arising under this DPA shall be subject to the dispute resolution provisions of the Agreement, save that disputes relating exclusively to data protection matters under the fallback SCCs or UK Addendum shall be resolved in accordance with Schedule 1.

11.4 If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

11.5 Notices under this DPA shall be in writing and sent by email: To Polser: legal@polser.io. To the Customer: the data protection contact identified on the cover page of this DPA.

Execution

This DPA is entered into as of the Effective Date set out on the cover page. Each party warrants that the signatory below has authority to enter into this DPA on its behalf.

POLSER, INC. (Processor / Data Importer)	**[CUSTOMER LEGAL ENTITY NAME] (Controller / Data Exporter)**
Signature: Printed Name: Title / Role: Date:	Signature: Printed Name: Title / Role: Date:

ANNEX A — Processing Details

Instructions: This Annex must be completed by the parties before the DPA is executed. Fields marked [Customer to specify] require the Customer's input.

Subject Matter	Provision of the Polser SaaS platform for customer communication and support automation via the WhatsApp Business API, as described in the Agreement.
Duration of Processing	For the duration of the Agreement and until all Personal Data is deleted or returned pursuant to Clause 8.
Nature of Processing	Storage, transmission, retrieval, organisation, and automated processing of Personal Data to enable WhatsApp Business API communication services (e.g. sending and receiving messages, managing conversation threads, analytics).
Purpose(s)	To provide the services described in the Agreement. Polser processes Personal Data solely on the Customer's behalf and strictly in accordance with the Customer's instructions.
Categories of Personal Data	May include: name, phone number, WhatsApp ID, message content, device identifiers, conversation metadata, and any other personal data included by the Customer or End Users in communications processed through the platform. [Customer to specify applicable categories]
Categories of Data Subjects	End Users of the Customer's WhatsApp Business channels (e.g. customers, leads, students, patients, or other individuals who communicate with the Customer via WhatsApp). [Customer to specify]
Special Category Data	None anticipated by design. To the extent that End Users incidentally include special category data within unstructured free-text communications via the WhatsApp Business API, such data is processed by Polser as a technical conduit only. Customer warrants it has an appropriate legal basis under Article 9 GDPR for any such processing and has implemented suitable safeguards.
Authorised Customer Contact	[Customer to insert name/role authorised to give processing instructions]
Applicable Jurisdiction(s)	[Customer to select: ☐ EU GDPR ☐ UK GDPR ☐ Both]

ANNEX B — Technical and Organisational Security Measures (TOMs)

The following describes Polser's primary technical and organisational measures. Current documentation is also available at polser.io/trust. Polser may update these measures from time to time.

Measure	Description
Access Control	Role-based access controls (RBAC); multi-factor authentication (MFA) required for all staff accessing production systems; principle of least privilege enforced; access revoked immediately upon termination.
Encryption	Data encrypted in transit using TLS 1.2+; data encrypted at rest using AES-256 or equivalent; backups encrypted.
Pseudonymisation	Applied where technically feasible and where the purpose of processing can be fulfilled.
Infrastructure Security	Hosted on AWS (eu-west-1, Ireland), whose data centres are ISO 27001 certified. Network segmentation, firewalls, and intrusion detection systems in place.
Availability & Resilience	Redundant architecture with automated failover; regular backups with tested restore procedures; documented business continuity and disaster recovery plans.
Vulnerability Management	Regular vulnerability scanning and penetration testing; patch management programme; responsible disclosure policy.
Personnel Measures	All staff with access to Personal Data are subject to contractual obligations of confidentiality and data protection in their employment contracts. Access is granted on a role-based, least-privilege basis with MFA enforced, and is revoked promptly upon exit. A formal security awareness training programme is in development.
Incident Response	Documented incident response plan; breach detection and logging mechanisms; 48-hour notification capability, consistent with the obligation in Clause 5.1.
Subprocessor Controls	Subprocessors subject to data processing agreements with substantially equivalent security requirements.
Audit & Logging	Access logs maintained and retained for a minimum of 12 months; reviewed regularly for anomalies.

ANNEX C — Approved Subprocessors

The current, up-to-date list of Subprocessors is maintained at polser.io/trust. Polser provides 30 days' notice of material changes in accordance with Clause 4.3.

Subprocessor	Location	Processing Activity	Transfer Mechanism
Amazon Web Services (AWS EMEA SARL)	Luxembourg / Ireland	Cloud infrastructure and hosting. All platform data in eu-west-1 (Ireland).	SCCs (AWS Service Terms) / UK Addendum
Meta Platforms Ireland Ltd	Ireland	WhatsApp Business API gateway. Message content, phone numbers, delivery metadata.	EU–US DPF + UK Extension / SCCs + UK Addendum
OpenAI Ireland Limited	Ireland	AI-assisted features. Engaged only when AI features are enabled by the customer.	SCCs + UK Addendum (OpenAI Business DPA)
ElevenLabs, Inc.	USA	Text-to-voice conversion. Engaged only when voice note features are enabled.	EU–US DPF + UK Extension / SCCs + UK Addendum
DeepL SE	Germany (EU)	Message translation. Engaged only when translation feature is enabled.	No transfer (EU-based)
Mixpanel, Inc.	USA	Product analytics. Pseudonymous identifiers only. No message content.	SCCs + UK Addendum (Mixpanel DPA)
PostHog, Inc.	USA / EU Cloud	Product analytics. EU Cloud (Frankfurt). Pseudonymous identifiers only.	EU hosting / SCCs + UK Addendum fallback
Okta, Inc. (Auth0)	USA	Authentication and identity management. Account identifiers and auth tokens.	SCCs + UK Addendum (Okta DPA)
650 Industries, Inc. (Expo)	USA	Mobile app infrastructure. Push notification routing only.	EU–US DPF + UK Extension / SCCs + UK Addendum
Google Ireland Ltd (Firebase)	Ireland	Android push notification delivery.	SCCs + UK Addendum (Firebase Terms)
Apple Inc. (APNs)	USA	iOS push notification delivery.	Apple Developer DPA / EU Transfer Agreement + UK Addendum

SCHEDULE 1 — Standard Contractual Clauses / UK IDTA (Fallback Transfer Mechanism)

Schedule 1 is pre-executed and automatically incorporated into this DPA by Clause 6.2. It takes effect dynamically if the DPF or UK Extension is suspended, invalidated, or does not cover a particular transfer. No separate signature is required.

Part 1: EU Standard Contractual Clauses (Module 2: Controller to Processor)

The parties agree to be bound by the EU SCCs adopted under European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (Module 2: Controller to Processor), hereby incorporated by reference and pre-executed as part of this DPA. The relevant completion details are as follows:

SCC Annex / Clause	Completion
Annex I.A – Parties	Data Exporter: as identified on the cover page. Data Importer: Polser, Inc., 1111B South Governors Avenue 6368, Dover, DE 19904, USA; legal@polser.io.
Annex I.B – Description of Transfer	As set out in Annex A to this DPA.
Annex I.C – Supervisory Authority	The supervisory authority of the Member State in which the data exporter is established.
Annex II – TOMs	As set out in Annex B to this DPA.
Annex III – Sub-processors	General authorisation granted; current list in Annex C and at polser.io/trust.
Clause 7 (Docking Clause)	Not included.
Clause 9 (Sub-processors)	Option 2: General written authorisation. 30 days' prior notice of changes.
Clause 11 (Redress)	Clause 11 is fully operative. The optional paragraph permitting data subjects to lodge complaints with an independent alternative dispute resolution body is omitted.
Clause 17 (Governing Law)	Laws of Ireland.
Clause 18 (Jurisdiction)	Courts of Ireland.

Part 2: UK International Data Transfer Addendum (UK Addendum to EU SCCs)

For transfers from the UK, the parties are bound by the UK Addendum to the EU SCCs issued by the ICO (Version B1.0, effective 21 March 2022, as updated from time to time), pre-executed as part of this DPA. The EU SCCs as completed in Part 1 of this Schedule form the Approved EU SCCs for the purposes of the UK Addendum. Either party may end the UK Addendum as set out in Section 19 thereof. As permitted by Section 11 of the UK Addendum, the governing law for transfers of Personal Data from the United Kingdom shall be the laws of England & Wales, and any disputes arising from the UK Addendum shall be subject to the exclusive jurisdiction of the courts of England & Wales.

Note on Execution: This Schedule is pre-executed and automatically incorporated by Clause 6.2. No separate signature is required. The completion details above form the operative Annex I, II, and III of the EU SCCs for the purposes of this DPA.