Data Processing Agreement (Pro)

HumanDesign.ai Ltd · Version 1.0 · Effective 1 July 2026

1. Parties, scope and how this DPA applies

1.1 This Data Processing Agreement ("DPA") is between **HumanDesign.ai Ltd**, company number 14696719, registered at 128 City Road, London, EC1V 2NX, United Kingdom ("HumanDesign.ai", "we"), and the customer named in the order, account or signature block below ("Customer", "you").

1.2 It applies when you use HumanDesign.ai Pro (the "Services"): a HumanDesign.ai practitioner or professional account, where you enter, store or analyse the birth details, charts and session notes of your own clients, and use Bella (our AI assistant) on them.

1.3 This DPA forms part of the agreement under which you use the Services (the HumanDesign.ai Pro Terms of Service, the "Agreement"). It takes effect on the earlier of your acceptance of the Agreement online and your signature below, and lasts as long as we process Customer Personal Data for you. A signed copy is available on request from privacy@humandesign.ai.

1.4 This DPA does not cover personal data we process as an independent controller, such as your own account, login and billing details, usage analytics, fraud prevention and our communications with you. Our Privacy Policy covers those.

2. Definitions

2.1 **Data Protection Law** means all laws on personal data that apply to the processing under this DPA, including the UK GDPR and Data Protection Act 2018, the EU GDPR (Regulation 2016/679), and, where they apply to you, other national laws such as the Australian Privacy Act 1988 and US state privacy laws.

2.2 **Customer Personal Data** means personal data that you, or your clients or end users through you, submit to the Services, and that we process on your behalf. Annex 1 describes it.

2.3 **Sub-processor** means a third party we engage to process Customer Personal Data. Annex 3 lists them.

2.4 **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.

2.5 **SCCs** means the EU standard contractual clauses in Commission Implementing Decision (EU) 2021/914. **UK Addendum** means the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner under s119A Data Protection Act 2018. **DPF** means the EU-US Data Privacy Framework and its UK Extension.

2.6 Controller, processor, data subject, personal data, processing and supervisory authority have the meanings given in the UK GDPR and EU GDPR.

3. Roles and instructions

3.1 For Customer Personal Data, you are the controller (or a processor acting for your own controller) and HumanDesign.ai is your processor (or sub-processor).

3.2 We will process Customer Personal Data only on your documented instructions, unless the law requires otherwise; in that case we will tell you first unless the law forbids it. Your instructions are: the Agreement, this DPA, and your use

and configuration of the Services (including what you enter, which features you use, and what you ask Bella to do). We will tell you if we believe an instruction breaks Data Protection Law.

3.3 You are responsible for having a lawful basis, and any consent you need, to give us your clients' or users' data, and for the notices you give them. Birth details and charts are not special category data in themselves, but conversations and notes about clients can reveal health, religious or philosophical beliefs, or other sensitive matters. If you enter such data, you are responsible for having the condition you need to process it (for example explicit consent).

3.4 We will not sell Customer Personal Data, use it to build profiles for advertising, or use it to train or fine-tune any AI model. We may create aggregated, de-identified statistics about how the Services perform (for example error rates and response times), which do not identify you, your clients or your users.

4. Our obligations as processor

4.1 **Confidentiality.** Only personnel who need access to provide, support, secure or fix the Services may access Customer Personal Data, and only for those purposes. Everyone with access is bound by confidentiality obligations. This includes AI tools that our team uses to support and maintain the Services; those tools are listed in Annex 3 and are subject to the same limits.

4.2 **Security.** We will put in place and maintain the technical and organisational measures in Annex 2, which are appropriate to the risk. We may update them, but not so that overall protection is reduced.

4.3 **Assistance.** Taking into account the nature of the processing and the information available to us, we will help you, at your reasonable request, to meet your obligations on security, breach notification, data protection impact assessments and prior consultation with a supervisory authority.

4.4 **Records.** We will keep the records of processing that Data Protection Law requires of a processor.

4.5 **Investigating faults.** When we investigate a fault that affects you, we will use logs and metadata first. We will only look at the content of Customer Personal Data when that is needed to fix the fault, keep the look to what is necessary, and not copy it outside the Services and the Sub-processors in Annex 3.

5. Sub-processors

5.1 You give general authorisation for us to use the Sub-processors listed in Annex 3, and to add or replace Sub-processors under this clause.

5.2 We will impose on each Sub-processor, by written contract, data protection obligations that protect Customer Personal Data at least as well as this DPA. We remain liable to you for each Sub-processor's performance of those obligations.

5.3 We will publish the current list at https://pro.humandesign.ai/subprocessors and give you at least **14 days'** notice by email of any new or replacement Sub-processor, before it processes Customer Personal Data.

5.4 You may object on reasonable data protection grounds within that notice period. We will then discuss it in good faith. If we cannot offer a reasonable alternative (for example, not using the feature that relies on that Sub-processor), you may terminate the affected Services by written notice, and we will refund any prepaid fees for the period after termination.

5.5 In an emergency, for example where a Sub-processor fails or a security issue requires an immediate change, we may replace a Sub-processor with shorter notice. We will tell you as soon as we can, and your right to object still applies.

6. International transfers

6.1 **Where data is stored.** We store Customer Personal Data in the European Union: our primary servers are with Hetzner in Helsinki, Finland, and our encrypted backups are in Cloudflare R2 using its EU jurisdiction. HumanDesign.ai Ltd is a UK company, and our team may access the data from the UK and other countries under the safeguards in this clause.

6.2 **Transfers from you to us.** Where EU GDPR applies to you, transfers to HumanDesign.ai in the UK rely on the European Commission's adequacy decision for the UK. If that decision ceases to apply, the SCCs (Module 2, controller to processor, or Module 3, processor to processor, as fits your role) are incorporated into this DPA, with the options set out in 6.5.

6.3 **Transfers to Sub-processors.** Some Pro features send Customer Personal Data to Sub-processors outside the UK and EU, mainly in the United States. Today these are: AI chat on Google Gemini models, memory notes, conversation summaries and text embeddings (OpenAI, Google, Anthropic), web search (Perplexity), and the daily briefing (Google). Annex 3 lists each one with its location. For each such transfer we rely on at least one of: (a) an adequacy decision, including the DPF where the Sub-processor is certified under it; or (b) the SCCs (Module 3) and, for UK data, the UK Addendum, entered into with the Sub-processor. We will assess the risks of each transfer and keep that assessment available to you on request.

6.4 **Customers outside the UK and EU.** If you are in another country (for example Australia), you acknowledge that Customer Personal Data is stored in the EU and processed in the UK, EU and United States as described in Annex 3, and you are responsible for telling your clients or users about this where your law requires it.

6.5 **SCC options.** Where the SCCs apply between you and us: Clause 7 (docking) applies; Clause 9 option 2 (general authorisation, with notice as in clause 5.3); Clause 11 optional wording does not apply; Clauses 17 and 18: the law and courts of Ireland; Annexes I to III are completed by Annexes 1 to 3 of this DPA. For UK transfers the UK Addendum applies, with Table 4 allowing either party to end it as permitted there.

6.6 We will not describe AI processing under this DPA as EU-only unless every AI Sub-processor in Annex 3 processes Customer Personal Data in the EU.

7. Personal Data Breaches

7.1 We will notify you without undue delay, and in any event within **48 hours** of becoming aware of a Personal Data Breach affecting Customer Personal Data. We will notify the email address on your account and any privacy contact you give us.

7.2 The notice will include, as far as we know at the time: what happened, the categories and approximate number of data subjects and records, the likely consequences, and the steps we have taken or propose. Where we don't have all of this at once, we will send it in stages without undue delay.

7.3 We will take reasonable steps to contain and investigate the breach and reduce its effects, and will cooperate with you on any notice you must give to a supervisory authority or to data subjects. Unless the law requires us to, we will not notify your clients, users or your supervisory authority on your behalf without your agreement.

7.4 Our notice is not an admission of fault or liability.

8. Data subject requests, audits, return and deletion

8.1 **Data subject requests.** If one of your clients or users contacts us directly about Customer Personal Data, we will pass the request to you without undue delay and will not answer it ourselves except to confirm we have passed it on. The Services let you view, export and delete client charts, conversations and notes. Where you need more help to answer a request, we will give reasonable assistance.

8.2 **Information and audits.** We will make available the information reasonably needed to show that we meet this DPA, including written answers to security questionnaires (no more than once a year unless there is a breach) and any third-party certifications or reports we hold. If that is not enough, or a supervisory authority requires it, you or an independent auditor bound by confidentiality may audit our compliance once per year, on at least **30 days'** written notice, during business hours, at your cost, and in a way that does not expose other customers' data. Audits of Sub-processors are met by the reports those Sub-processors make available.

8.3 **Return.** During the term you can export Customer Personal Data through the Services. If you need help, we will provide a reasonable export in a common machine-readable format.

8.4 **Deletion.** Within **30 days** after the Agreement ends, or earlier on your written request, we will delete Customer Personal Data from our live systems, including saved client charts, conversations, notes, AI memory items, and logs that contain it. Copies in encrypted backups are deleted as the backups expire, within **90 days**, and are not restored in the meantime except to recover from a failure. We may keep data where the law requires us to, and will keep it protected and process it only for that purpose. We will confirm deletion in writing on request.

8.5 Sub-processors that hold copies (for example AI providers' short-term abuse-monitoring logs) delete them on their own retention schedules.

9. Liability, term, law and precedence

9.1 **Liability.** Each party's liability under this DPA is subject to the limits and exclusions in the Agreement. In any case, each party's total liability arising out of or in connection with this DPA is capped at the fees you paid for the Services in the 12 months before the event giving rise to the claim, and that cap is shared with, not added to, the cap in the Agreement. Nothing limits liability that cannot be limited by law, or either party's liability to data subjects under Data Protection Law.

9.2 **Term.** This DPA lasts as long as we process Customer Personal Data for you, and the clauses on confidentiality, deletion and liability survive termination.

9.3 **Precedence.** If this DPA conflicts with the Agreement, this DPA wins on data protection matters. If it conflicts with the SCCs or UK Addendum, those win.

9.4 **Changes.** We may update this DPA to reflect changes in Data Protection Law or the Services, with at least 30 days' notice, provided the update does not reduce the protection of Customer Personal Data. Annex 3 is updated under clause 5.

9.5 **Governing law.** Except where the SCCs require otherwise, this DPA is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

9.6 **Contacts.** Privacy notices to us: privacy@humandesign.ai. Notices to you: the email address on your account, or the privacy contact you give below.

Signatures (only needed for a signed copy; online acceptance of the Agreement also binds you)

	HumanDesign.ai Ltd	Customer
Name		
Title		
Date		
Signature		
Privacy contact email	privacy@humandesign.ai	

Annex 1: Description of processing

Item	Pro accounts
Data subjects	The Customer's clients, prospects and the people whose charts they look at (for example partners or family members of clients)
Categories of personal data	Names or labels the Customer gives; date, time and place of birth; computed chart data; session notes; questions and answers in Bella conversations about those people; AI-generated memory notes, titles and summaries; files the Customer uploads
Sensitive data	Not required by the Services. Conversations and notes may reveal health, religious or philosophical beliefs or other special category data if the Customer enters it (see clause 3.3)
Nature of processing	Storage, chart calculation, AI analysis and chat, memory extraction, summarising, search, display, export, deletion
Purpose	To provide the Pro features the Customer uses
Frequency	Continuous while the account is active
Duration and retention	Until the Customer deletes the data or the Agreement ends, then clause 8.4
Sub-processors	Annex 3
Competent supervisory authority	UK Information Commissioner's Office for HumanDesign.ai; for EU customers, the authority named under SCC Clause 13

Annex 2: Technical and organisational measures

Area	Measure
Hosting	Dedicated server operated by HumanDesign.ai at Hetzner in Helsinki, Finland; data centre physical security provided by Hetzner (ISO 27001 certified).
Encryption in transit	All web and app traffic uses HTTPS (TLS). Admin access to servers runs through an encrypted tunnel.
Encryption of backups	Backups are encrypted before they leave the server and stored in Cloudflare R2 in its EU jurisdiction.
Network access	No public SSH port. Server administration only through an authenticated tunnel with key-based login. Reverse proxy with connection caps and per-IP rate limits; abusive sources are blocked.

Area	Measure
Separation of customer data	Database row-level security restricts each account to its own records.
Access control	Production access is limited to the founder, named engineering staff and the AI tools they operate (Annex 3). Credentials are rotated after any suspected exposure.
Availability and resilience	Disks mirrored (RAID 1). Continuous database archiving with 7 retained base backups; host backups kept 90 days. Daily checks that backups succeed, with alerts on failure.
Monitoring	Service health and error monitoring with alerts to the operations team; reverse proxy and application logs.
AI providers	AI providers are used through their business APIs. A gateway in front of AI calls is set not to store prompt or response bodies.
Personnel	Confidentiality obligations for all staff and contractors; access removed when no longer needed.
Incident response	Breach handling under clause 7, with records of each incident kept.
Data minimisation	The Services do not require names or contact details of clients; Customers can use labels instead.

Annex 3: Sub-processors

Current as of 1 July 2026. Rows marked "outside EU" rely on the safeguards in clause 6.3.

Sub-processor	What it does with Customer Personal Data	Location	Transfer safeguard
Hetzner Online GmbH	Hosts the servers, database and file storage	EU (Helsinki, Finland)	Inside EU
Cloudflare, Inc.	Network, DNS and attack protection; admin tunnel; AI gateway that routes AI calls (logs metadata only, not prompts); encrypted backups in R2	Global network; backups in EU	DPF and SCCs
Google LLC (Gemini API)	Runs the Gemini models behind Bella chat and the daily briefing; text embeddings	Outside EU (US and global)	DPF and SCCs
OpenAI, L.L.C. / OpenAI Ireland Ltd	Extracts memory notes, writes conversation summaries and titles, text embeddings; AI assistant used by support staff to read and triage support tickets	Outside EU (US)	DPF and SCCs
Anthropic PBC	Fallback model for summaries; AI assistant used by engineering staff to investigate and fix faults (clause 4.5)	Outside EU (US)	SCCs
Amazon Web Services EMEA SARL (Bedrock)	Runs Claude models on some Bella paths	EU	Inside EU
Perplexity AI, Inc.	Web search, only when a Bella answer uses search; receives the search query	Outside EU (US)	SCCs
Google LLC (Google Workspace)	Support email inbox, only for data the Customer sends to support	Outside EU (US and global)	DPF and SCCs
Slack Technologies, LLC	Internal support notifications, which may include ticket titles and excerpts	Outside EU (US)	DPF and SCCs

Sub-processor	What it does with Customer Personal Data	Location	Transfer safeguard
Supabase, Inc.	Legacy database copy as of 1 Nov 2026, paused, no new data; being deleted	UK (London)	UK adequacy for EU data

Published at https://pro.humandesign.ai/dpa. Need a signed copy? Email privacy@humandesign.ai