Data Protection
Impact Assessment

Transceve Ltd · Company No. 16191698

Version 1.0 · April 2026 · CONFIDENTIAL

1. Document Overview

Organisation	Transceve Ltd
Company number	16191698
Registered address	Allia Future Business Centre, Kings Hedges Road, Cambridge CB4 2HY
Data controller	Transceve Ltd
DPO / data lead	Damien Ribbans, Founder (damien@transceve.org)
Date of assessment	April 2026
Review date	April 2027 (or on material change to processing)
ICO registration	Application submitted April 2026
Status	Pre-launch — no real customer data processed at time of assessment

This DPIA has been prepared in advance of onboarding paying customers, in accordance with Article 35 UK GDPR.

It should be reviewed by a qualified DP solicitor before the first paying customer is onboarded and updated

annually or whenever a material change to processing activities occurs.

2. Purpose and Context of Processing

2.1 What Transceve does

Transceve is a SaaS platform that enables third sector organisations (charities, social enterprises, community organisations, and similar bodies) to measure the impact of their conversational practice. Organisations upload recordings, transcripts, or documents of sessions between their practitioners and service users. Transceve analyses these conversations using locally-hosted artificial intelligence

models and scores them against Self-Determination Theory's three Basic Psychological Needs (Autonomy, Competence, and Relatedness).

The platform produces BPN scores (1–9), confidence levels, qualitative utterance extractions, structural flags, and grant report drafts. All processing occurs within Transceve's own infrastructure — no conversation data is transmitted to any third-party AI provider.

2.2 Why this DPIA is required

A DPIA is required under Article 35 UK GDPR where processing is likely to result in a high risk to individuals. Transceve's processing meets the threshold because it involves:

- Systematic analysis of personal data using automated means (Article 35(3)(a))
- Processing of data relating to vulnerable individuals, including those in mental health, substance misuse, domestic abuse, youth work, and similar contexts
- Processing that may involve inferences about health or psychological wellbeing, which are special category data under Article 9 UK GDPR
- Large-scale processing of conversational data on behalf of multiple data controllers (the customer organisations)

---

3. Data Flows and Processing Activities

3.1 Data collected

Category	Examples	Source
Conversational content	Audio, video, transcripts, emails, documents containing spoken or written exchanges between practitioners and service users	Uploaded by customer organisation
Pseudonymous service user references	Reference codes (e.g. SU-REF-001) — no names or direct identifiers stored in Transceve	Assigned by customer organisation
Practitioner utterances	Extracted from conversation as part of diarisation and analysis	Derived from uploaded content
Service user utterances	Extracted from conversation — the participant voice is a core analytical output	Derived from uploaded content
Inferred psychological need scores	BPN scores (Autonomy, Competence, Relatedness) derived by AI analysis — potentially health-adjacent inferences	Generated by Transceve AI
Organisation account data	Org name, contact email, billing details, org profile content	Provided by customer on registration

Category	Examples	Source
User account data	Name, email address, hashed password	Provided by customer staff on registration
Audit log data	IP address, user agent, action type, timestamp for all actions	Collected automatically by Transceve
Usage data	Token consumption, file types, session counts	Collected automatically by Transceve

3.2 Special category data consideration

Transceve's position is that BPN scores are measures of conversational quality and practitioner effectiveness, not clinical assessments of individual health. They are scored at the session level and are pseudonymous. However, this position requires legal validation.

3.3 Data flow summary

- Customer uploads file to Transceve → stored on Hetzner Cloud server (Helsinki, Finland, EU)
- Whisper model transcribes audio/video on the same server — no external transmission
- pyannote diarises speakers on the same server — no external transmission
- Ethical LoRA pre-checks transcript for safeguarding concerns — on the same server
- transceve-bpns LoRA analyses transcript and generates BPN scores — on the same server
- Results stored in PostgreSQL database on the same server
- Customer accesses results via HTTPS — encrypted in transit
- Automated backups to Hetzner Object Storage (same jurisdiction)

No conversation data is transmitted outside Hetzner's EU infrastructure at any point. The sole third-party services receiving any data are SendGrid (email notifications — no conversation content) and the National Grid ESO carbon intensity API (no personal data).

---

4. Lawful Basis for Processing

4.1 Controller/processor relationship

The customer organisation (charity, social enterprise etc.) is the data controller in respect of personal data contained in uploaded conversational content. Transceve acts as a data processor on the customer's instruction. This relationship is governed by Transceve's Data Processing Agreement (DPA).

For data Transceve collects directly (account data, audit logs, usage data), Transceve is the data controller.

4.2 Lawful basis by category

Data category	Lawful basis	Notes
Conversational content (as processor)	Customer's lawful basis — Transceve relies on customer's Article 6 basis	Customer responsible for ensuring lawful basis. Transceve's DPA requires customers to warrant this.
Service user references (pseudonymous)	Legitimate interests (Article 6(1)(f)) — service improvement and impact measurement	Pseudonymisation reduces privacy impact. Data subjects not directly identifiable by Transceve.
Account and contact data	Contract (Article 6(1)(b)) — necessary to provide the service	Standard SaaS account data.
Audit logs	Legitimate interests (Article 6(1)(f)) — security, fraud prevention, compliance	Retention: 12 months. Access restricted to Transceve admin.
Usage data	Contract (Article 6(1)(b)) — necessary for billing and service delivery	Aggregated — no conversation content included.
BPN score inferences (if special category)	Explicit consent (Article 9(2)(a)) OR substantial public interest (Article 9(2)(g)) — TO BE CONFIRMED WITH LEGAL ADVICE	This is the key legal risk. See Section 3.2.

5. Necessity and Proportionality

5.1 Is the processing necessary?

Yes. The core purpose of Transceve — enabling third sector organisations to objectively measure whether their conversations are working — cannot be achieved without analysing the conversational content itself. Aggregate outcome data alone does not reveal the conversational dynamics that drive or undermine psychological need satisfaction.

5.2 Data minimisation measures

- Service users are identified by reference codes only — Transceve never stores names, addresses, or direct identifiers
- Organisations maintain their own ID-to-name mapping outside Transceve
- Only the content necessary for analysis is processed — no metadata beyond what is inherent in the file
- Media files can be deleted by the customer at any time
- Token-based usage tracking is aggregated — no per-utterance billing data retained

5.3 Retention

- Uploaded media files: retained until deleted by the customer or organisation account closure
- Analysis results: retained for the life of the organisation account
- Audit logs: 12 months
- Account data: retained for duration of contract plus 6 years (legal obligation)
- Backups: 30-day rolling retention on Hetzner Object Storage

A formal retention policy document is in preparation and will be published in the Privacy Notice before commercial launch.

---

6. Risk Assessment

6.1 Risk register

Risk	Likelihood	Impact	Level	Mitigation	Residual
Unlawful access to conversational data by third parties	Low	High	Medium	HTTPS encryption in transit. Firewall — ports 80/443 only. No public database port. Strong secrets. Regular security updates.	Low
Data breach via Hetzner infrastructure compromise	Low	High	Medium	Hetzner ISO 27001 certified. EU jurisdiction (no US Cloud Act). Transceve data isolated in dedicated server. Encrypted backups.	Low
BPN scores classified as special category data without legal basis	Medium	High	High	Legal review commissioned before commercial launch. Pseudonymisation. Consent mechanism being designed. Public interest basis being assessed.	Medium
Customer uploads data without lawful basis for doing so	Medium	Medium	Medium	DPA requires customers to warrant lawful basis. Terms of Service place obligation on customer. Customer responsible for data subject rights.	Low
Safeguarding disclosure not acted upon	Low	High	Medium	Ethical LoRA pre-check flags safeguarding concerns. Flag displayed prominently in results UI. Trust page guidance on human review. Customer remains responsible for acting on disclosures.	Low

Risk	Likelihood	Impact	Level	Mitigation	Residual
AI hallucination produces inaccurate BPN scores	Medium	Medium	Medium	Structured prompts. Confidence scoring. Participant-only utterance attribution. Human review guidance on Trust page. LoRA trained on validated examples.	Low
Data subject exercises rights (erasure, access) — Transceve unable to respond	Medium	Medium	Medium	DPA passes primary rights obligation to customer. Transceve admin can delete org data. Pseudonymous references mean Transceve cannot identify data subjects directly.	Low
Employee / contractor accesses customer data inappropriately	Low	High	Medium	Transceve admin role has zero access to conversation content or analysis results by design. Full audit trail on all actions. Currently sole founder — risk increases as team grows.	Low

7. Technical and Organisational Security Measures

7.1 Technical measures

- HTTPS enforced for all connections — HTTP redirects to HTTPS
- TLS 1.2 and 1.3 only — weak cipher suites disabled
- Let's Encrypt SSL certificate — auto-renewing
- Security headers on all API responses: CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy
- Firewall: inbound ports 22 (SSH), 80 (HTTP), 443 (HTTPS) only — database and internal services not publicly exposed
- All AI models run locally — no conversation data transmitted externally
- Passwords hashed with bcrypt
- JWT tokens with configurable expiry (default 8 hours)
- Full audit trail: every action logged with user ID, IP address, user agent, timestamp
- WCAG 2.1 AA — 0 axe-core violations at launch

7.2 Organisational measures

- Data Processing Agreement with all customer organisations
- Privacy Notice, Terms of Service, and Cookie Policy published at /legal
- ICO registration submitted April 2026
- Transceve admin role designed with zero access to customer conversation data

- Ethical constitution (Governing Social Contract v2, March 2026) governing all AI design decisions
- Constitutional AI pre-check (transceve-ethical LoRA) screens every transcript before analysis
- Staff data protection training — to be formalised as team grows

7.3 Infrastructure

- Hetzner Cloud, Helsinki, Finland — EU jurisdiction, no US Cloud Act exposure
- 100% renewable energy
- EU-UK adequacy decision in force (renewed December 2025, valid to December 2031)
- Daily encrypted database backups to Hetzner Object Storage — 30-day rolling retention
- Single-server deployment at launch — GPU server to be added on Hetzner approval

---

8. Consultation

8.1 Internal consultation

As a sole-founder company at pre-launch stage, internal consultation has been conducted by Damien Ribbans in his capacity as founder, data lead, and de facto DPO. This DPIA has been prepared with reference to the ICO's DPIA guidance and the UK GDPR.

8.2 External consultation

REQUIRED BEFORE COMMERCIAL LAUNCH: This DPIA must be reviewed by a qualified data protection solicitor

before the first paying customer is onboarded. Key areas requiring legal input:

- Whether BPN score inferences constitute special category data under Article 9
- Appropriate lawful basis if special category data is engaged
- Adequacy of the DPA for processor obligations
- Retention policy completeness
- Whether ICO consultation under Article 36 is required

8.3 Data subject consultation

Data subjects in this context are service users whose conversational data is uploaded by customer organisations. Direct consultation with data subjects has not been conducted at this stage. Customer organisations are responsible for ensuring their service users are informed of data processing through their own privacy notices, and that any necessary consent is obtained.

Transceve's Privacy Notice and Trust page provide transparency about the analytical processing that occurs. This will be supplemented by guidance to customer organisations on what to tell service users.

---

9. Decisions and Sign-Off

9.1 Summary of key decisions

Decision	Status	Owner / deadline
Obtain legal advice on BPN score special category question	REQUIRED before commercial launch	External DP solicitor — before first paying customer
Formalise data retention policy	In preparation	Damien Ribbans — before commercial launch
Publish updated Privacy Notice covering BPN inferences	Pending legal advice	Damien Ribbans — after legal review
Design consent mechanism if special category basis required	Pending legal advice	Development team — after legal review
ICO registration	Submitted April 2026	Damien Ribbans — complete
Staff data protection training policy	Not yet formalised	Damien Ribbans — before first hire
Annual DPIA review	Scheduled April 2027	Damien Ribbans
Review on material change to processing	Ongoing	Damien Ribbans

9.2 Sign-off

Name	Role	Date
Damien Ribbans	Founder / Data Lead, Transceve Ltd	April 2026
[DP Solicitor name]	External reviewer	[To be completed]

---

10. Version History

Version	Date	Author	Changes
1.0	April 2026	Damien Ribbans	Initial draft — pre-commercial launch

This document is confidential and intended for internal use and legal review only. It should not be shared with customers in its current form pending completion of legal review.