SERVICE HIVE

DATA PROTECTION & PRIVACY POLICY

A GDPR-Aligned Policy for Market Research Operations

CLASSIFICATION	Confidential — Vendor Onboarding & Internal Use
DOCUMENT VERSION	1.0
EFFECTIVE DATE	11 July 2026

Service Hive • Virar West, Maharashtra, India • service-hive.pro

Document Control

Document Title	Data Protection & Privacy Policy (GDPR-Aligned)
Document Owner	Data Protection Lead, Service Hive
Applies To	Service Hive, its employees, recruiters, moderators, transcribers, translators, field partners and sub-processors
Classification	Confidential — Internal & Client Vendor-Onboarding Use
Version	1.0
Effective Date	11 July 2026
Next Scheduled Review	11 July 2027
Approved By	Founder & Director, Service Hive

Revision History

Version	Date	Author	Summary of Changes
0.1	27 Jun 2026	Service Hive Compliance Team	Initial draft prepared for internal review.
1.0	11 Jul 2026	Service Hive Compliance Team	Reviewed, approved and issued as the official Data Protection & Privacy Policy.

This Policy is reviewed at least annually, and sooner following a material change in applicable law, Service Hive's service offering, or a significant data protection incident. See Section 22, Policy Governance.

Table of Contents

1. Introduction

Service Hive is a market research data delivery company that plans, fields, and delivers qualitative and quantitative research on behalf of research agencies, consultancies, and corporate clients around the world. In the course of that work we collect and process personal data belonging to survey and interview respondents, panel members, business contacts, employees, and vendor partners.

This Policy explains how Service Hive protects that personal data and sets a single, consistent standard for everyone who works with us — employees, recruiters, moderators, transcribers, translators, and any field or technology partner we engage — across every market we operate in. It is written to align with the EU General Data Protection Regulation (GDPR) and is intended to give our clients, respondents, and partners confidence in how personal data entrusted to Service Hive is handled, from the first recruitment call through to secure data delivery and disposal.

This Policy should be read together with Service Hive's Information Security Policy, its standard Data Processing Agreement (DPA), and the project-specific Data Processing Record completed for each study (Appendix A).

2. Purpose

This Policy exists to:

- Set out Service Hive's commitment to processing personal data lawfully, fairly, and transparently;
- Give staff, recruiters, moderators, and field partners clear, practical rules to follow at every stage of a research project;
- Support due diligence and vendor-onboarding reviews carried out by enterprise clients before they commission work from Service Hive;
- Reduce the regulatory, contractual, and reputational risk associated with handling respondent and client data; and
- Provide a consistent reference point that sits above, and is implemented through, the project-level procedures and templates in the Appendices.

3. Scope

This Policy applies to Service Hive and to every individual and organisation that processes personal data on Service Hive's behalf, including employees, freelance recruiters and interviewers, moderators, transcribers, translators, panel and sample providers, and technology vendors.

It applies wherever Service Hive processes personal data of a data subject located in the European Economic Area (EEA) or the United Kingdom, personal data belonging to an EEA/UK resident regardless of where the processing takes place, or personal data processed in connection with providing research services to a client established in the EEA/UK — consistent with the extraterritorial scope of GDPR Article 3.

Service Hive also applies the core principles of this Policy as a baseline operating standard across all the markets it works in — including India, the UAE, Saudi Arabia, and other jurisdictions — as good practice, aligning where relevant with local frameworks such as India's Digital Personal Data Protection Act. Where a local law imposes a stricter requirement than this Policy for a given engagement, the stricter requirement governs that engagement.

The Policy covers personal data relating to respondents and panel members, client and business contacts, employees, and vendor personnel, collected through any research mode Service Hive fields — online surveys, telephonic interviews (CATI), in-person interviews (CAPI), and qualitative video or in-person interviews and focus groups.

4. Definitions

Consent: A freely given, specific, informed, and unambiguous indication of a Data Subject's agreement to the Processing of their Personal Data, given by a clear affirmative statement or action. Silence, pre-ticked boxes, or inactivity do not constitute valid consent.

Controller: The entity that determines the purposes and means of Processing Personal Data. Service Hive acts as Controller for its own recruitment and panel databases, and as Processor when executing a client-commissioned study to that client's instructions.

Data Subject: An identified or identifiable individual whose Personal Data is Processed — including respondents, panel members, business contacts, employees, and vendor personnel.

Fieldwork Partner: Any recruiter, interviewer, moderator, transcriber, translator, or local field agency engaged by Service Hive to help deliver a study.

Panel / Panelist: Service Hive's proprietary database of individuals who have opted in to be contacted about future research opportunities, and the individual members of that database.

Personal Data: Any information relating to an identified or identifiable natural person, including names, contact details, professional details, recordings, and any online identifier.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Processing: Any operation performed on Personal Data, including collection, recording, storage, use, transmission, or erasure.

Processor: A person or organisation that Processes Personal Data on behalf of a Controller under documented instructions.

Pseudonymisation: Processing Personal Data so that it can no longer be attributed to a specific Data Subject without additional, separately held information — for example, replacing a respondent's name with a code such as “R1” in a transcript.

Screener: The structured questionnaire used to determine a prospective respondent's eligibility for a study, and through which recruitment consent is captured.

Special Category Data: Personal Data revealing racial or ethnic origin, health, genetic or biometric data, sex life or sexual orientation, religious or philosophical beliefs, political opinions, or trade union membership, and data relating to criminal convictions or offences.

Sub-processor: Any third party engaged by Service Hive to Process Personal Data as part of delivering a study, such as a transcription vendor, translation partner, or panel-sampling company.

Supervisory Authority: An independent public authority responsible for monitoring the application of GDPR in an EU member state.

5. GDPR Principles

Service Hive Processes Personal Data in line with the following principles, and must be able to demonstrate that compliance on request:

- **Lawfulness, fairness and transparency:** Personal Data is Processed on a documented lawful basis, and Data Subjects are told clearly what will happen to their data.
- **Purpose limitation:** Personal Data is collected for the specific, explicit purpose stated in the relevant study or panel registration, and is not reused for an incompatible purpose.
- **Data minimisation:** Only the Personal Data genuinely needed for the stated research purpose is collected.
- **Accuracy:** Personal Data is kept accurate and, where necessary, up to date; inaccurate data is corrected or erased without undue delay.
- **Storage limitation:** Personal Data is kept in identifiable form for no longer than necessary — see Section 15, Data Retention.
- **Integrity and confidentiality:** Personal Data is Processed securely, using appropriate technical and organisational measures — see Section 14, Security Measures.
- **Accountability:** Service Hive documents its Processing activities, decisions, and safeguards so that compliance can be demonstrated to clients and Supervisory Authorities.

6. Roles & Responsibilities

Founder & Director: Holds ultimate accountability for data protection at Service Hive and formally approves this Policy.

Data Protection Lead (DPL): Owns day-to-day compliance. Coordinates breach response, maintains the Records of Processing Activities, reviews screeners and consent language, approves studies involving Special Category Data or minors, and is the single point of contact for Data Subjects, clients, and Supervisory Authorities on privacy matters. Contactable at privacy@service-hive.pro.

Project / Study Managers: Confirm that each project's data flows, consent script, and retention plan comply with this Policy before fieldwork begins, and complete the project's Data Processing Record (Appendix A).

Recruiters & Interviewers: Obtain and accurately log respondent consent, follow approved screening scripts, and handle respondent data only as instructed for the study.

Moderators, Transcribers & Translators: Handle recordings, transcripts, and translations under the confidentiality and data-handling terms in their engagement agreement, whether employed directly or engaged as a Fieldwork Partner.

IT / Systems Administration: Maintains access controls, encryption, and backup arrangements for the systems Service Hive uses to store and transmit Personal Data.

All Personnel: Complete mandatory data protection training before handling Personal Data, and report any suspected Personal Data Breach to the DPL within 24 hours of becoming aware of it.

7. Lawful Basis for Processing

Service Hive identifies and documents a lawful basis under GDPR Article 6 before Processing begins for any activity. The bases most commonly relied on are:

- **Consent:** The primary basis for recruiting and interviewing respondents, and for recording interviews — see Section 8, Consent Management.
- **Contract:** Used to Process client contact details and respondent honorarium details necessary to perform a research services contract.
- **Legal obligation:** Used where Processing is required to meet a statutory obligation, such as retaining incentive-payment records for tax and finance purposes.
- **Legitimate interests:** Used narrowly — for example, to prevent duplicate or fraudulent survey participation and to protect data quality — and only where this does not override the Data Subject's own interests and rights.

The lawful basis for each study is recorded in that study's Data Processing Record (Appendix A) before fieldwork is authorised.

8. Consent Management

Consent is captured through plain-language screener wording, read aloud or displayed to the respondent before any substantive question is asked, and is logged with a timestamp and the method of collection.

- Recording (audio or video) always requires its own, separately captured consent — it is never bundled into general study consent.
- Sharing raw recordings or unredacted transcripts with a client requires an additional, specific consent, obtained and logged before the interview begins.
- Respondents may withdraw consent at any point, including mid-interview, without affecting any incentive already earned for time given. On withdrawal, active processing stops and, where requested, the recording and responses collected are deleted.
- Screeners never use pre-ticked boxes or default-in language, and every screener includes plain-language wording a respondent can understand without legal training.
- Where Service Hive sources respondents through a third-party panel provider, that provider's consent and opt-in mechanism is reviewed by the DPL before the panel is used.

9. Special Category Data

Some studies legitimately require questions that touch on Special Category Data — for example, health-related consumption habits or occupational safety incidents. Service Hive only collects such data where it is directly relevant to the study's stated research objective, and only with the respondent's explicit, specifically-worded consent captured in the screener.

- Any study expected to collect Special Category Data requires DPL sign-off before fielding, including a documented assessment of whether a Data Protection Impact Assessment is needed.
- Special Category Data is minimised and, wherever the research design allows, aggregated or anonymised in client deliverables.
- Special Category Data is never reused for a purpose beyond the study it was collected for without fresh, specific consent.

10. Children's Data

Service Hive does not knowingly recruit or interview anyone under 18 without verifiable consent from a parent or legal guardian. For EEA-based respondents under 16, guardian consent is required in line with GDPR Article 8, and, where the study design calls for it, the guardian is present during the interview.

Any study that targets minors as respondents requires prior written sign-off from the DPL and uses a child-appropriate consent or assent script reviewed before fielding.

11. Data Controller Responsibilities

Where Service Hive determines the purposes and means of Processing — principally its own recruitment and panel database — it acts as Controller and:

- Maintains a clear, accessible privacy notice for panel members and prospective respondents;
- Carries out a Data Protection Impact Assessment before any higher-risk Processing activity, such as adopting new recruitment technology, large-scale collection of Special Category Data, or systematic profiling;
- Maintains Records of Processing Activities covering its panel and recruitment operations;
- Builds data protection into the design of its screeners, panel systems, and recruitment tools by default; and
- Puts appropriate safeguards in place before transferring Personal Data internationally — see Section 16.

12. Data Processor Responsibilities

Where Service Hive is engaged by a client to execute fieldwork and deliver data to that client's specification, it acts as Processor and:

- Processes Personal Data only on the client's documented instructions;
- Signs a Data Processing Agreement with the client before a project begins, covering the categories of data, duration, nature and purpose of Processing, and Service Hive's obligations;
- Flows equivalent data-protection obligations down to any Sub-processor or Fieldwork Partner, and does not engage a new Sub-processor without the client's prior general or specific written authorisation — see Section 18;
- Assists the client in responding to Data Subject requests, Personal Data Breaches, and Data Protection Impact Assessments relevant to the project; and
- Returns or securely destroys Personal Data at the end of the engagement, at the client's choice, in line with the project's Data Processing Record.

13. Data Subjects' Rights

Data Subjects can exercise the following rights by writing to privacy@service-hive.pro. Service Hive verifies the requester's identity, responds within one month (extendable by a further two months for complex requests, with the Data Subject informed of the extension), and does not charge a fee for a standard request.

- **Right of access:** To confirm whether Personal Data is being Processed and receive a copy of it.
- **Right to rectification:** To have inaccurate or incomplete Personal Data corrected.
- **Right to erasure:** To have Personal Data deleted where it is no longer needed, consent is withdrawn, or Processing was unlawful.
- **Right to restrict Processing:** To limit how Personal Data is used while a dispute over its accuracy or lawfulness is resolved.
- **Right to data portability:** To receive Personal Data provided to Service Hive in a structured, machine-readable format, where Processing is based on consent or contract and carried out by automated means.
- **Right to object:** To object to Processing based on legitimate interests, including profiling for data-quality purposes.
- **Rights related to automated decision-making:** Service Hive does not use fully automated decision-making that produces a legal or similarly significant effect on a Data Subject.

Where Service Hive holds the data as Processor for a client, the request is forwarded to that client without undue delay and Service Hive supports the client in resolving it.

14. Security Measures

Service Hive applies technical and organisational measures appropriate to the sensitivity of the Personal Data it handles, including:

- Role-based access control, so Personal Data is only visible to the people who need it to do their job;

- Encryption of recordings, transcripts, screener responses, and client deliverables both in transit and at rest;
- Transfer of Personal Data only through approved, encrypted channels or secure client data rooms — never over unsecured email or consumer messaging apps;
- Physical and device security requirements for recruiters and interviewers working in the field;
- Time-limited, access-controlled links for sharing recordings and deliverables;
- Periodic access reviews and a mandatory password / multi-factor authentication policy for internal systems;
- Security due diligence on vendors and Fieldwork Partners before they are onboarded; and
- A documented incident-response process, tested periodically — see Section 17, Personal Data Breaches.

15. Data Retention

Retention periods are set project by project in the Data Processing Record (Appendix A), applying the following defaults unless the client contract or applicable law requires otherwise:

- **Interview recordings:** Deleted or anonymised within 90 days of project close-out, unless the client contractually requires a longer period or requests earlier deletion.
- **Transcripts:** Anonymised transcripts are retained for up to 12 months for quality assurance and audit purposes, then securely deleted, unless the client contract specifies otherwise.
- **Screening data of non-selected candidates:** Deleted within 30 days of the fieldwork window closing, unless the individual has separately consented to remain in Service Hive's panel database.
- **Incentive and payment records:** Retained for the period required by applicable finance and tax law in the relevant jurisdiction.
- **Panel database records:** Retained until the panelist withdraws consent or opts out, subject to periodic re-permissioning to confirm the panelist still wishes to remain listed.

Personal Data that has reached the end of its retention period is deleted or destroyed using a secure method that prevents reconstruction or further Processing.

16. International Transfers

Service Hive fields studies across multiple countries — including India, the UAE, and Saudi Arabia — and regularly delivers data to clients headquartered in the EEA, UK, and elsewhere. Where Personal Data is transferred outside the country in which it was collected, Service Hive puts appropriate safeguards in place before the transfer occurs, including:

- Standard Contractual Clauses with clients and Sub-processors where required;
- A transfer impact assessment of the destination country's data protection framework before a new cross-border transfer arrangement is set up;

- Data minimisation and pseudonymisation of transcripts and datasets wherever the research design allows before cross-border delivery; and
- Clear notice to respondents in the consent script where their data will be transferred outside their home country.

17. Personal Data Breaches

A Personal Data Breach at Service Hive might include, for example, a lost recorder or laptop containing unencrypted interview recordings, a data-delivery file sent to the wrong recipient, or unauthorised access to the panel database.

- Any employee, recruiter, or Fieldwork Partner who suspects a Personal Data Breach must report it to the DPL within 24 hours of becoming aware of it.
- The DPL assesses the risk to affected Data Subjects and, where Service Hive is acting as Controller and the breach is likely to pose a risk, notifies the relevant Supervisory Authority within 72 hours of becoming aware of it.
- Where Service Hive is acting as Processor, it notifies the affected client Controller without undue delay so the client can meet its own notification obligations.
- Where a breach is likely to result in a high risk to affected individuals, those individuals are notified directly, in clear language, without undue delay.
- Every breach, however small, is logged in the Personal Data Breach Report (Appendix D), recording its cause, impact, and the remedial action taken.

18. Third-Party Processors

Service Hive works with a range of Sub-processors and Fieldwork Partners — freelance moderators, transcription and translation vendors, panel and sample providers, cloud storage and software vendors, and courier services used for incentive fulfilment.

- Each new Sub-processor is assessed for data protection and security practice before being onboarded;
- A written data processing agreement or confidentiality undertaking is in place before any Sub-processor accesses Personal Data;
- Service Hive maintains a Sub-processor / Fieldwork Partner Register (Appendix C), reviewed periodically;
- Clients are given prior notice, and the opportunity to object, before Service Hive engages a new Sub-processor on their project; and
- Sub-processor arrangements are reassessed periodically and whenever the scope of work changes materially.

19. Respondent Panel Management

Service Hive's proprietary respondent panel, and the partner panels it draws on for additional sample, sit at the centre of its recruitment operations and are managed under this Policy as follows:

- Every panel source has a documented consent and legal basis; where a partner panel provider supplies respondents, Service Hive reviews that provider's consent practices before use.
- Panel registration collects only the profiling fields needed for current and reasonably foreseeable eligibility screening, and a panelist's separate consent is obtained before they are contacted about future studies.
- Panelists can update their profile, pause participation, or request full deletion of their panel record at any time by writing to privacy@service-hive.pro.
- Limited technical identifiers, such as a hashed phone number or device identifier, are used strictly to prevent duplicate participation and protect data quality — never for profiling or marketing unrelated to research eligibility.
- Incentive-fulfilment details, such as bank or UPI information, are stored separately from research response data and are accessible only to the finance or operations staff responsible for processing payment.
- Panelists are periodically re-permissioned to confirm they still wish to remain in Service Hive's database.

20. Market Research Specific Requirements

Anonymisation by default

Client deliverables identify respondents by a code (for example, “R1”, “R2”) rather than by name, unless the research design specifically calls for identified data — for example, named executive interviews in a B2B study — in which case that requirement, and the respondent's specific consent to it, is documented in the project's Data Processing Record.

Recording and transcription

Interviews are recorded only with explicit, separately captured respondent consent. Access to raw recordings is limited to the project team, and recordings are not shared with the client in raw form unless the engagement contract and respondent consent both specifically provide for it.

Screener design standards

Every screener includes a standard introductory block covering who is conducting the research, its purpose, how the data will be used, whether the session will be recorded, that participation is voluntary and can be withdrawn at any time, and how to reach Service Hive with a privacy question. New screeners are reviewed by the DPL before fielding.

Business and B2B respondent data

Named business contacts — for example, industry executives interviewed for a B2B study such as a value-chain assessment — remain individuals whose Personal Data is protected under GDPR wherever an EEA-linked person is identifiable. Service Hive extends the same consent, security, and retention safeguards to B2B respondent data as it does to consumer respondent data.

Multi-country and translation work

Local field partners and translators engaged for multi-country studies are bound by the same confidentiality and data-handling terms as Service Hive's core team, and are made aware of any country-specific consent or transfer requirements for the study.

Client-supplied sample

Where a client supplies its own sample list, Service Hive processes it only for the purposes of that project, does not retain it beyond the retention period documented for that project, and shares deliverables only through the client's specified secure channel.

21. Training & Awareness

- All new employees, recruiters, and long-term field partners complete data protection induction training before they are given access to Personal Data.
- All personnel who handle Personal Data complete refresher training at least annually.
- Project teams receive a study-specific briefing before fielding any project involving Special Category Data, minors, or a new market.
- The DPL maintains training completion records, and completion is required before assignment to a relevant project.

22. Policy Governance

- This Policy is owned by the Data Protection Lead on behalf of Service Hive's Founder & Director, who gives final approval.
- It is reviewed at least annually, and sooner following a material change in applicable law, Service Hive's service offering, or a significant data protection incident.
- Any exception to this Policy must be approved in writing by the DPL before it takes effect.
- This Policy operates alongside Service Hive's Information Security Policy and its client-specific Data Processing Agreements. Where a signed client DPA imposes a more specific requirement for a given engagement, that DPA governs the engagement.

23. Appendices

The templates below are completed for each project and retained by the Data Protection Lead as evidence of compliance with this Policy.

Appendix A — Project Data Processing Record (template fields)

Field	Description
Project name & client	Identifies the study and the commissioning client.
Countries involved	Every country in which respondents are recruited, interviewed, or the data is stored or delivered.
Data categories collected	The categories of Personal Data the screener and interview will collect.
Special Category Data (Y/N)	Whether the study is expected to collect Special Category Data, and the DPL sign-off reference if so.
Lawful basis	The GDPR Article 6 basis relied on for this project.
Recording (Y/N)	Whether interviews will be audio/video recorded, and how consent is captured.
Sub-processors used	Any transcription, translation, or panel providers engaged for this project.
Retention period	Agreed retention period for recordings, transcripts, and screening data for this project.
DPIA required (Y/N)	Outcome of the DPL's screening assessment for a Data Protection Impact Assessment.

Appendix B — Data Subject Request Log (template fields)

Date Received	Requestor	Request Type	Verification Method	Due Date	Status

Appendix C — Sub-processor / Fieldwork Partner Register (template fields)

Name	Role	Data Accessed	Country	Agreement Signed (Y/N)	Last Reviewed

Appendix D — Personal Data Breach Report (template fields)

Field	Description
Date / time discovered	When the breach was first identified.

Field	Description
Description	What happened, and how it was discovered.
Data affected	Categories and approximate number of Data Subjects and records affected.
Risk assessment	The DPL's assessment of risk to affected individuals.
Containment actions	Immediate steps taken to contain the breach.
Notification decision	Whether the Supervisory Authority, client, and/or Data Subjects were notified, and when.
Root cause	The underlying cause identified.
Preventive actions	Changes made to prevent recurrence.

Appendix E — Standard Respondent Consent Script Checklist

- States who is conducting the research and on whose behalf;
- Explains the purpose of the study in plain language;
- Explains what data will be collected and how it will be used and shared;
- Discloses whether the session will be recorded, and obtains separate consent for recording;
- Confirms participation is voluntary and can be withdrawn at any time without affecting any incentive already earned;
- Provides a contact point for privacy questions (privacy@service-hive.pro); and
- Is reviewed and approved by the Data Protection Lead before the screener is fielded.