

ZIV MEDIA GROUP, LLC

DATA POLICY

Effective Date: [CONFIRM: insert publication date] **Last Updated:** [CONFIRM: insert date]

Drafting note (delete before publishing): Statements that say "Ziv Media requires" or "our policy is" are representations. Publish each only once it is true in practice (see the Launch Checklist in the Legal Analysis & Launch Package). Bracketed CONFIRM items must be resolved and the document reviewed by your attorney.

1. Purpose

1.1 This Data Policy describes how Ziv Media Group, LLC ("Ziv Media," "we," "us," or "our") sources, validates, enriches, licenses, sells, distributes, and otherwise handles lead and marketing data in the course of our business, and the standards we require of the sources that supply data and the Clients that receive it.

1.2 This Data Policy is separate from, and complements, our **Privacy Policy**, which explains how we collect and use personal information about website visitors, customers, and individuals generally and describes individual privacy rights. Where the two documents address the same subject, they are intended to be read consistently.

1.3 This Data Policy is a statement of practices and requirements. It does not by itself create a contract, a warranty, or rights in any third party (see Section 35).

2. Scope

This Data Policy applies to data and Leads that Ziv Media generates, acquires, processes, licenses, sells, or distributes, and to Clients, Sources, and vendors that supply or receive that data. It does not replace a signed agreement (for example, an insertion order, lead purchase agreement, data license, or data processing agreement), the Terms and Conditions that govern our website and services, or any legally required consent language shown on a lead form.

3. Definitions and Roles

3.1 Definitions.

- **"Data"** means information in any form that we generate, acquire, or process, including Leads, contact data, firmographic data, demographic data, behavioral and interest data, and marketing data.
- **"Personal Information"** has the meaning in our Privacy Policy and applicable law.
- **"Lead"** means a record indicating an individual's or business's interest in a product or service, with associated contact, source, timestamp, and consent information.
- **"Consent Record"** means the evidence of a consumer's consent associated with a Lead, including the disclosure language displayed, the date and time, the page or form version, the

consent action taken, the identifiers collected (such as IP address), and the identity of the Source.

- **"Source"** means any person from which we obtain Data, including publishers, affiliates, lead-generation partners, data vendors, and public sources.
- **"Client"** means a business that purchases, licenses, or receives Data or Leads from us.
- **"Suppression Data"** means records of opt-outs, revocations, Do-Not-Call listings, deletion requests, and similar do-not-contact or do-not-sell indicators.
- **"Sale," "Share," "business purpose," "service provider," "contractor," "third party," "data broker," and similar terms** have the meanings given by the applicable law.

3.2 Roles vary by activity. No single legal label applies to everything we do. Our role is determined by the facts and any written agreement.

Activity	How we are typically characterized	The recipient or counterparty
Collecting Leads through forms we operate and delivering them to Clients for payment	"Business" / "controller"; this is a sale of Personal Information	Client is a "third party"
Acquiring Data from Sources with which the individual has no direct relationship and licensing or selling it	"Data broker" where state law so defines; this is a sale	Client is a "third party"
Enriching, matching, or appending a Client's own file at the Client's direction under a compliant written agreement	"Service provider," "contractor," or "processor"	Client is the "business" or "controller"
Operating live-transfer or pay-per-call programs	Seller or transferor of calls and associated data; telemarketing laws may apply to us or the Client	Client receives the call
Our own business marketing	"Business" / "controller"	n/a

4. Data Categories

We may handle: **contact data** (name, email, telephone, postal address); **demographic and firmographic data** (employer, title, industry, company size, general characteristics); **interest and behavioral data** (service interests, form responses, site activity); **lead-source and consent data**; **call data** (call detail records and, where lawful and disclosed, recordings); and **derived data** (scoring or interest indicators). Different categories carry different legal treatment, and we apply the restrictions in Section 18 to categories that carry heightened risk.

5. Data Sources

We obtain Data from: (a) individuals who submit forms on sites we operate; (b) publishers, affiliates, and lead-generation partners; (c) data vendors and data providers; (d) publicly available sources; (e) Clients (for Client-provided data); and (f) our own website and communications. [CONFIRM: remove any source type you do not use.] We do not describe individual Sources by name in this Policy. Source information is confidential business information, but we maintain it so that we can document provenance.

6. Data Acquisition

6.1 We acquire Data only from Sources that we reasonably believe collected it lawfully. Our standards require each Source to (a) identify itself and the origin of the Data, (b) collect Data through disclosures that are truthful and consistent with law, (c) provide Consent Records where the Data may be used for telephone, text, or other marketing that requires consent, and (d) honor opt-outs and deletion requests.

6.2 We may decline, quarantine, or delete Data that does not meet these standards, and we may terminate a Source that does not.

6.3 Data obtained from a Source may be subject to that Source's terms and restrictions, which can limit how we or our Clients may use it.

7. Data Verification and Validation

We may apply technical and manual checks to Data, including format and syntax checks, de-duplication, telephone and email validity checks, address standardization, comparison against suppression and Do-Not-Call lists, and fraud and bot-traffic screening. These checks reduce, but do not eliminate, errors and invalid records, and we do not represent that any record is accurate, current, or reachable (see Sections 9 and 35).

8. Data Enrichment, Matching, and Append

8.1 We may enrich or append Data using other lawfully obtained Data, match records across datasets, and standardize fields. We do this to improve the operation and routing of Leads and to deliver services to Clients.

8.2 When we perform enrichment or append services on a Client's own file, we process that file only as the Client directs under a written agreement and do not merge it into our own datasets or use it for other purposes unless the agreement or the law permits.

8.3 We do not use enrichment or matching to determine eligibility for credit, insurance, employment, housing, or other purposes restricted by Section 18.

9. Data Accuracy and Quality

Data is compiled from many Sources, can change quickly, and may contain errors. We use commercially reasonable efforts to maintain data quality, including correcting records we learn are inaccurate. We do not guarantee accuracy, completeness, freshness, exclusivity, deliverability, contact rate, or conversion. Return, rejection, and credit rights for Leads and calls, if any, are governed exclusively by the Client's signed agreement and our Terms and Conditions.

10. Data Licensing, Sale, and Brokerage

10.1 We sell and license Data. We deliver Leads and Data to Clients in exchange for payment. Under California and other state privacy laws, that is a "sale" of Personal Information. Under Nevada law, we also treat our transfers of covered information for monetary consideration as potential "sales" and honor verified requests accordingly.

10.2 Terminology. We use the following terms consistently:

- **Sale:** disclosing Personal Information to a third party for monetary or other valuable consideration, as law defines it.
- **Licensing:** granting a Client a limited right to use Data under an agreement while we retain our rights in the Data, subject to law and any Source restrictions.
- **Sharing:** disclosing Personal Information for cross-context behavioral advertising. We describe our website practices in the Privacy Policy [CONFIRM: ad-tech status].
- **Business-purpose disclosure:** disclosure to a service provider or contractor under a contract that limits use of the information.
- **Brokerage:** acquiring Data from Sources and making it available to Clients.

10.3 Rights granted to Clients are limited. A Client receives only the rights stated in its agreement, and may not use Data for purposes inconsistent with this Policy, the agreement, or the law.

11. Lead Generation and Consent Standards

11.1 Privacy notice, consent, and contract are different things. Our Privacy Policy is a notice. It does not create or prove consent to be contacted. Consent to receive telephone calls, text messages, or email marketing is captured at the point of collection through a lead-form disclosure, evidenced by a Consent Record. Client obligations are set by signed agreements. We keep these documents separate on purpose.

11.2 Consent requirements at the Source. For any Lead that may be used for automated or prerecorded calls, text messages, or other telemarketing for which the law requires prior express written consent, we require that the Source: (a) present a clear and conspicuous disclosure at the point where the consumer provides the telephone number; (b) state that consent is not a condition of purchase; (c) obtain the consumer's affirmative action and electronic or written signature; (d) identify the sellers, or the categories or listing of sellers, that may contact the consumer in a manner that is consistent with law and not misleading [CONFIRM with counsel: the FCC's one-to-one consent rule was vacated and removed, but disclosures must still be clear and specific enough to establish consent]; and (e) capture and preserve a Consent Record.

11.3 No substitute for consent. We do not treat the existence of a record, a purchased list, an inquiry, or a business relationship as consent unless the law so provides.

11.4 Revocation. A consumer may revoke consent by any reasonable means. We treat a revocation received through any channel as a suppression event, and we require Sources and Clients to do the same.

11.5 Records. We retain Consent Records, and the underlying evidence, for as long as legally required and for the period during which claims related to the contact could be brought. See Section 26.

11.6 Not legal advice to Clients. Clients are independently responsible for their own compliance (Sections 29 and 33).

12. Lead Distribution; Do-Not-Call and Suppression

12.1 Distribution. We deliver Leads to Clients through the methods and on the terms stated in their agreements (for example, real-time posting, batch files, or email). Whether a Lead is exclusive or shared is determined by the Client's order or agreement.

12.2 Suppression before delivery. Where applicable to the program, we check Leads against our internal suppression list and applicable Do-Not-Call data [CONFIRM: National DNC subscription and state lists] before delivery, and we do not intentionally deliver a Lead we know to be suppressed for the channel at issue.

12.3 Clients' independent scrub obligation. Clients must scrub against the National Do-Not-Call Registry, applicable state registries, and their own internal lists, before contacting any individual, whether or not we have also done so.

12.4 Suppression Data. We maintain Suppression Data to honor opt-outs, and retain it even after deleting other Data about the individual, as permitted by law, so that we do not re-add the individual.

13. Live Transfers and Pay-Per-Call

13.1 In live-transfer or pay-per-call programs, a consumer's call or interest is connected to a Client. Information provided on the call may be passed to the Client.

13.2 Call recording. If we record calls, we announce the recording at the start of the call [CONFIRM: recording practices] because some states (including Nevada, as of our last review, and California) require consent from all parties. Recordings are Personal Information and are handled under this Policy and the Privacy Policy. We may share recordings with Clients, consistent with the consent and notice provided.

13.3 Billing. What qualifies as a billable call, connected duration, and rejection windows are set by the Client's agreement, not by this Policy.

13.4 Transferred calls remain subject to telemarketing and call-recording laws; the party that places or receives the call, as applicable, is responsible for its compliance.

14. B2B Data

Data about individuals in their professional capacity (for example, work email or business telephone) can still be Personal Information. We apply the Privacy Policy and this Policy to it where applicable law covers it. Some Do-Not-Call and similar rules treat business-to-business calling differently, but those exceptions are limited, and calls to a mobile telephone may remain subject to the TCPA even when made for a business purpose. Clients must determine the applicability of those rules.

15. B2C and Consumer Data

Data about individuals in their personal capacity is subject to consumer privacy, telemarketing, and consumer-protection laws. We apply the consent standards in Section 11 and the restrictions in Section 18 to it, and we honor consumer rights as described in the Privacy Policy.

16. Publicly Available Data

We use publicly available data only to the extent the law permits and consistent with the terms of the source. Whether data counts as "publicly available" is defined by law and varies. Data being accessible does not mean it can be used for any purpose, and we do not collect it by methods that violate a site's terms or applicable law.

17. Third-Party and Vendor Data

We require data vendors and Sources, by contract where possible, to represent that they collected the Data lawfully, to provide provenance information on request, to cooperate with deletion and opt-out requests, and to notify us of complaints, claims, or regulatory inquiries involving the Data. Third-party Data may be subject to the vendor's terms. We are not responsible for a vendor's independent violation of law, and we may suspend or stop using Data we have reason to believe was unlawfully collected.

18. Restricted Data and Restricted Purposes

18.1 Restricted Data. Unless approved in writing following legal review, we do not intentionally acquire, accept, or deliver: government-issued identification numbers (including Social Security numbers); financial account, card, or credential data; precise geolocation; health, medical, or genetic information; biometric information; data revealing race, ethnicity, religion, sexual orientation or life, or immigration status; or Data about individuals we know to be under 18. [CONFIRM: this is a business decision, and it determines how the Privacy Policy treats sensitive information.]

18.2 Not a consumer reporting agency. Ziv Media does not intend to be a consumer reporting agency, and our Data is not a "consumer report." We do not furnish Data to be used, in whole or in part, to determine eligibility for credit, insurance, employment, housing, or any other purpose covered by the Fair Credit Reporting Act. Clients may not use Data for those purposes.

18.3 Deletion on discovery. If Restricted Data enters our systems, we will isolate and delete it, or handle it only as permitted by law.

19. Client-Provided Data

Data a Client provides to us remains subject to the Client's rights and the Client's agreement. We act on it as directed by the agreement. The Client is responsible for having the rights and legal basis (including notices and consents) to provide it to us. We do not accept Client-provided Data that includes Restricted Data unless approved in writing.

20. Data Disclosure and Sharing

We disclose Data to: Clients; service providers (hosting, CRM, lead-routing, call-tracking, communications, payment, identity-verification, fraud-prevention, and security providers); professional advisors; legal and regulatory authorities where required or permitted; and counterparties in a business transaction. We do not disclose Data to unrelated third parties for their own independent marketing outside the Client relationships and Source relationships described in this Policy, except as permitted by law or disclosed to you.

21. Data-Broker Status and Registration

21.1 Where we acquire Personal Information from Sources with which individuals have no direct relationship with us and sell it, we may be a "data broker" under California law and under the laws of other states. [CONFIRM — SELECT: "We are registered as a data broker with the California Privacy Protection Agency [and in the following states: ____]" OR "We will register before engaging in this activity in any state that requires it."]

21.2 **California DROP.** California residents can submit deletion requests to registered data brokers through the state's Delete Request and Opt-out Platform. As a registered data broker, we access the platform at least as often as California law requires, process requests within the required time, and direct our service providers and contractors to do the same.

21.3 Information about our registration is available in the state registry.

22. Marketing Use

We use Data to market our own services to businesses, subject to law and your opt-out. Clients use Data to market their own products and services. Neither this Policy nor our Privacy Policy constitutes consent to marketing; consent, where required, is captured as described in Section 11.

23. Opt-Outs

23.1 An individual may opt out of the sale or sharing of Personal Information, and of marketing, by emailing [CONFIRM: privacy email], using our online form [CONFIRM: URL], using an opt-out preference signal such as Global Privacy Control, or, for California residents, through DROP.

23.2 We add the individual to our Suppression Data and process the opt-out promptly, within the time the law requires. We require Clients who receive the opt-out information from us to honor it, and we will pass opt-outs to Clients where feasible. We cannot retract Data a Client has lawfully received before the opt-out, but we will notify Clients of the opt-out as required by law and our agreements.

24. Data Correction

We will correct inaccurate Personal Information in our records when a verified request or other information shows it to be inaccurate, as the law requires. We may notify Clients of material corrections as provided in their agreements. Our correction obligations extend to our records only.

25. Data Deletion

25.1 We honor verified deletion requests as the law requires. We may retain or decline deletion where an exception applies, including to keep Suppression Data and Consent Records, to comply with law, to complete a transaction, to detect security incidents or fraud, to establish or defend legal claims, or where deletion is not feasible or is not required by the applicable law.

25.2 Deletion does not require us to recall Data already lawfully delivered to Clients, but we will direct our service providers and contractors to delete as required and will notify Clients as required by law or contract.

26. Data Retention

We retain Data only as long as reasonably necessary for the purposes described in this Policy and the Privacy Policy, considering: the type of Data; our legal, tax, and recordkeeping obligations; the period during which claims may be brought; our contractual obligations; fraud-prevention and security needs; and the need to maintain Suppression Data. Consent Records and Suppression Data are retained longer than other Data because they document compliance and prevent re-contact. When Data is no longer needed, we delete or de-identify it.

27. Data Security

We use reasonable administrative, technical, and physical safeguards appropriate to the nature of the Data and the risks involved, including access controls, vendor oversight, and incident response procedures [CONFIRM that each is true]. No system is completely secure, and we do not guarantee that Data will never be accessed or disclosed without authorization. Where the law requires, we notify affected individuals, Clients, and regulators of security incidents.

28. Third-Party Providers

We use third-party providers for hosting, CRM, communications, call tracking, lead routing, analytics, payment processing, identity verification, fraud prevention, and professional services. We require providers that handle Personal Information on our behalf to protect it and use it only for our purposes, as the law requires. We are not responsible for the independent practices of third parties that are not our service providers.

29. Client Responsibilities

Each Client is independently responsible for its compliance with law and must:

1. Use Data only for lawful purposes permitted by its agreement, and not for any purpose in Sections 18 or 34.
2. Comply with the TCPA, the Telemarketing Sales Rule, CAN-SPAM, state telemarketing and "mini-TCPA" laws, state privacy laws, and any rules specific to its industry.
3. Scrub against Do-Not-Call and internal lists before contacting individuals, and honor revocations and opt-outs.
4. Not call, text, or email individuals in a manner that exceeds the consent shown in the Consent Record, or at times prohibited by law.

5. Maintain its own records of its contacts and make them available as required by law.
6. Promptly notify us of, and cooperate regarding, complaints, opt-outs, deletion requests, claims, and regulatory inquiries involving Data.
7. Maintain reasonable security for Data and notify us of any security incident affecting it.
8. Not resell, sublicense, or transfer Data except as its agreement permits, and bind any permitted recipient to equivalent restrictions.

30. Client Compliance Monitoring and Suspension

We may request information about a Client's use of Data, review complaints, and suspend or terminate delivery, to the extent our agreements allow, where we reasonably believe a Client is violating law, this Policy, or its agreement. We may do so without liability, to the extent the law and agreements permit.

31. Regulatory Compliance and Cooperation

We cooperate with lawful requests from regulators and law enforcement and may disclose Data, Consent Records, and Source information as required or permitted by law. We may also notify Clients and Sources of regulatory inquiries to the extent permitted. We monitor changes in applicable law and update this Policy as needed.

32. Complaints and Requests

To submit a complaint, correction, deletion, opt-out, or other request, contact the Data & Privacy Contact in Section 37. We will acknowledge and respond within the time the applicable law requires. If we cannot resolve a complaint, you may contact your state attorney general or the relevant federal or state regulator. Submitting a request does not guarantee a particular outcome, and requests are subject to verification and legal exceptions as described in the Privacy Policy.

33. Downstream Use

33.1 Once a Client receives Data, the Client, not Ziv Media, decides how to use it, within its agreement and the law. We do not control, and are not responsible for, a Client's independent use or disclosure of Data that violates law, this Policy, or the Client's agreement, to the fullest extent the law permits.

33.2 Where a Client operates in a regulated vertical (for example insurance, Medicare or health-related products, mortgage or financial services, or legal services), the Client is solely responsible for vertical-specific rules, licensing, disclosures, and recordkeeping. We may refuse, condition, or discontinue Data deliveries for any vertical.

34. Prohibited Uses

Data may not be used, and no one may direct us to use or deliver it, to: (a) violate any law; (b) harass, threaten, defraud, or deceive any person; (c) contact anyone on a suppression list or who has revoked consent, in a manner the law prohibits; (d) determine eligibility for credit, insurance, employment, housing, or other purposes covered by the Fair Credit Reporting Act; (e) discriminate in violation of law; (f) target or market to children; (g) re-identify de-identified Data; (h) stalk, surveil, or locate a person for

harm; (i) build or supplement a consumer report; or (j) transfer Data to a sanctioned person or for an unlawful purpose.

35. No Warranties; No Contract; Relationship to Other Documents

35.1 No warranties. We make no representation or warranty, express or implied, regarding the accuracy, completeness, quality, exclusivity, deliverability, contact rate, performance, or conversion of any Data, Lead, or call, or about the lawfulness of a Client's use, except as expressly stated in a signed agreement.

35.2 No contract or third-party rights. This Policy is informational. It does not create contractual obligations, a fiduciary or agency relationship, or any right or remedy in any person. Nothing here limits any right an individual has under applicable law.

35.3 Hierarchy. For Clients, a signed agreement (insertion order, lead purchase agreement, data license, or data processing agreement) controls over this Policy where they conflict. Payment, returns, chargebacks, liability limitation, indemnification, governing law, and dispute resolution are governed by those agreements and our Terms and Conditions, not by this Policy.

36. Changes to This Data Policy

We may update this Policy to reflect changes in law, technology, or our practices. We will post the updated version with a new "Last Updated" date and, where required, provide further notice. We review it at least annually.

37. Contact Information

Ziv Media Group, LLC Data & Privacy Contact: [CONFIRM: name/title] Email: [CONFIRM: email] Address: [CONFIRM: business address]

38. Additional Provisions

38.1 United States focus. We operate in and for the United States and do not target individuals in the European Economic Area, the United Kingdom, or other regions with separate data-protection regimes.

38.2 Severability. If any part of this Policy is held unenforceable, the rest remains in effect to the extent the law permits.

38.3 Accessibility. If you need this Policy in an accessible format, contact us at the address above.