

Last Updated: October 20, 2025

RampedUp – Data Collection & Privacy Brief

RampedUp complies with the EU-U.S. Data Privacy Framework (DPF), including the UK Extension and the Swiss-U.S. DPF. We commit to cooperating with and adhering to the guidance of the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC).

Lawful Basis for Processing Personal Data

RampedUp processes personal data under the following lawful bases as established by the General Data Protection Regulation (GDPR):

- **Article 6(1)(f)** – Processing is necessary for the purposes of our legitimate interests, including delivering business-to-business (B2B) services, validating contact data, and supporting responsible outreach, where such interests are not overridden by the data subject's rights or freedoms.
- **Article 9(2)(e)** – The data has been manifestly made public by the data subject. Even in the case of special category data, this article permits lawful processing if the subject has made the data publicly available. Employment-related data, which is not special category data, may therefore be processed under an even lower threshold.
- **Article 5(1)(d)** – We support data accuracy for our clients by ensuring personal data is accurate and up to date, minimizing risk caused by outdated or incorrect information.

Legitimate Interest and Public Data Use

We process business contact and firmographic information about professionals, such as name, job title, employer, work email or phone (where publicly provided), and company details, sourced from publicly available websites and public sources. We do this to help our customers keep their business records accurate.

All data subjects are professionals, and the use of their contact data is restricted to business purposes. The privacy impact is minimal, and the interests of both RampedUp and its clients (e.g., promoting products/services) are legitimate and reasonable. We do not intentionally collect special-category data.

The use of accurate contact data for commercial communication is consistent with the reasonable expectations of the data subjects and necessary for lawful business operations.

Exemption from Individual Notice – Article 14(5)(b)

Under Article 14(5)(b) of the GDPR, RampedUp does not notify individual data subjects when:

- The data was manifestly made public by the data subject
- Notification would involve disproportionate effort given the scale and nature of the data
- The data poses minimal impact on an individual's private life

Our activities support business transparency and contact accuracy. All data is derived from public sources such as company websites and press releases. We provide full transparency through our privacy policy and offer a public opt-out portal at:

<https://basic.rampedup.io/app/donotsell>

Terms of Service - Legal Basis for Collection Public Data

Terms of Service (ToS) that “disallow” scraping do not, by themselves, make scraping publicly available web pages unlawful under U.S. computer-crime law. In *Van Buren v. United States*, the U.S. Supreme Court held that the Computer Fraud and Abuse Act (CFAA) is violated only when someone accesses areas of a computer system that are off-limits to them - such as content protected by a pay wall or log-in - not simply when they use publicly available information in a way the website owner dislikes.

Building on that interpretation, the Ninth Circuit in *hiQ Labs, Inc. v. LinkedIn Corp.* reaffirmed that accessing and scraping data from publicly available web pages does not constitute “unauthorized access” under the CFAA, because there are no authentication or access-control gates to cross.

RampedUp has been advised that our data collection practices are lawful and consistent with this legal framework. We only collect information from web pages that are publicly available and do not require a login, paywall, or other form of authorization to view.

In addition, RampedUp abides by the permissions published by website owners and respects the crawling and indexing preferences they specify. As a result, our sourcing is limited to data that does not require authorization to access and is gathered in a manner that respects both technical access rules and applicable law.

International Registries

- **Data Privacy Framework Registration Number: 48066**
Organizations participating in the EU-U.S. DPF may receive personal data from the European Union / European Economic Area in reliance on the EU-U.S. Organizations participating in the UK Extension to the EU-U.S. DPF may receive personal data from the United Kingdom and Gibraltar in reliance on the UK Extension to the EU-U.S.
- **Privacy Shield Registration Number: a2zt0000000PL5uAAG**
RampedUp participates in the U.S.-EU Privacy Shield Framework. All personal data received from EU and Swiss sources is protected in accordance with these standards.

Domestic Registries

- **California Data Broker Registration Number: 538248**
The California Privacy Protection Agency (CPPA) manages California's Data Broker Registry.
- **Oregon Data Broker Registration Number: 00344**
Oregon's Department of Consumer and Business Services manages the state's data broker registry.
- **Texas Data Broker Registration Number: 20250186**
The Texas Data Broker Registry is managed by the Texas Secretary of State.
- **Vermont Data Broker Registration Number: 0409326**
The Vermont Secretary of State manages the state's data broker registry.

Legitimate Interests Assessment

Summary of processing

- **Purpose(s):** Provide customers with fresh, accurate B2B contact and company intelligence to (a) maintain CRM quality, (b) identify decision-makers, (c) support B2B outreach compliance (suppression and dedupe), and (d) analyze markets and competition.
- **Data subjects:** Business professionals acting in a professional capacity (employees, executives, founders, practitioners). Children are not targeted.
- **Data categories (typical):** Name, job title/role, employer, email address, work phone / direct dial phone, LinkedIn URL, company HQ & locations, industry/NAICS/SIC, employee counts, revenue bands, company URLs, and similar firmographics. No intent to process special-category data; RampedUp policy prohibits collection/use of sensitive attributes.
- **Sources:** Public web pages (company "About/Team/Contact/Directory" pages, press releases, filings, professional profiles where publicly published by the subject or employer), business registries, and other open-web signals.
- **Activities:** Discover → extract → normalize → verify/validate → deduplicate → enrich/match to customer records → deliver via UI/API/Flat File; maintain suppression lists and opt-outs.
- **Recipients/roles:** RampedUp acts as (a) **controller** for its master reference graph and prospecting platform; and (b) **processor** when performing customer-directed matching/enrichment against the customer's own records.
- **Sub-processors:** <https://rampedup.io/sub-processors>
- **International transfers:** Data may be hosted/processed in the U.S./EU/UK using SCCs and vendor transfer safeguards; vendor DPF participation is required where applicable.

- **Retention:** Reference graph: rolling refresh; stale/unverified records suppressed within 24 months (default) and deleted within 36 months unless re-verified. Customer-provided match logs retained 12 months for audit, then minimized/anonymized.

Purpose test — legitimate interest exists

Our interest (specific & lawful): Building and maintaining a high-quality B2B contact/firmographic dataset so businesses can keep CRMs clean, identify relevant decision-makers, and perform proportionate B2B outreach. This supports market transparency, reduces misdirected email/phone traffic, and enables opt-outs/suppression to function correctly.

Reasonable expectations: Business professionals generally expect their employer-published profile (name, title, work contact data) to be discoverable and used for professional interactions, lead qualification, and verification.

Necessity test — proportionate means

- Public-source discovery and normalized enrichment are the most effective, least-intrusive way to achieve the purpose at B2B scale.
- Less intrusive alternatives (e.g., asking each individual for consent prior to indexing public work details) are impracticable and would undermine data accuracy and suppression-list integrity.
- Minimization measures ensure this practice by limiting our collections to only the fields we process and nothing more.

Balancing test — interests vs. rights & freedoms

Professional context only; public/enterprise sources; no special-category data; strict field minimization; refresh & accuracy controls; per-record suppression and global opt-out; downstream use contractually bound to lawful-use terms; security and access controls; transparency via notice and subject-rights portal.

Safeguards (implemented):

- **Minimization:** Strict contact identifiers; blocklists for sensitive terms.
- **Accuracy & refresh:** Recrawl/re-verify cadence; decay rules; stale record suppression; audit trails.
- **Opt-out & suppression:** One-click global opt-out; immediate suppression in master graph; propagation to customers via suppression feeds/flags.
- **Transparency:** Public privacy notice naming “legitimate interests” and B2B uses; clear contact channel; DSAR workflow.
- **Security:** Role-based access, encryption in transit/at rest, logging, least-privilege admin, vendor due diligence.

- **Downstream controls:** Customer Terms/DPA restrict use to lawful purposes; prohibit sensitive inferences or discriminatory uses.

Outcome: On balance, RampedUp's legitimate interests are **not overridden** by the risks to individuals' rights and freedoms, given the professional context and safeguards.

Decision & Actions

- **Lawful basis:** Article 6(1)(f) Legitimate Interests.
- **Proceed?** Yes, with safeguards above.
- **Mitigations (owners & due dates):**
 - Confirm/automate 24-month stale-record suppression (Eng) • Dec 15, 2025
 - Apply Vendor Risk Assessment (Eng) • Dec 15, 2025
 - Quarterly audit of opt-out propagation to all exports/APIs (Ops) • Starting Q1 2026
- **Review triggers:** Material change in data sources, product scope, or legal guidance; new processing of non-public data sources; expansion to new jurisdictions; introduction of automated decision-making beyond lead discovery.
- **Decision Making AI Policy:** <https://rampedup.io/ai-policy>

Data-subject rights & objection-handling SOP (internal)

1. **Intake:** Route requests from privacy@ or <https://basic.rampedup.io/app/donotsell>
2. **Verify identity:** Lightweight verification using email confirmation.
3. **Locate record(s):** Search master graph by name + employer + email/phone/LinkedIn.
4. **Fulfill request:**
 - **Access:** Provide source categories, data fields, purposes, recipients, retention, and transfer info.
 - **Rectification:** Correct fields; keep change log.
 - **Erasure/Restriction:** Suppress record globally (do not delete source URLs from audit logs).
 - **Objection (Art. 21):** If objecting to legitimate-interests processing for direct marketing or related enrichment, **cease processing for that person**, add to suppression, and push suppression to customer export/API feeds.
5. **Confirm to requester:** Within one month (extendable where complex).
6. **Prevent re-ingestion:** Add hashed identifiers (email/phone/LI path) to the suppression ledger checked during crawl/ingest.
7. **Audit:** Log request ID, handler, timestamps, actions, and propagation status.

Customer & vendor contract hooks (short list)

- **Customers (Controllers):** Must use data only for lawful purposes; comply with privacy legislation; honor objections and opt-outs; use suppression feeds; no sensitive-attribute use.

- **Vendors (Sub-processors):** Security, confidentiality, breach notice, SCCs/transfer safeguards; no secondary use; delete/return upon termination; annual assessments.