

Lawful Basis for Processing Professional Data

Client-Facing GDPR Compliance Brief

RampedUp provides business-to-business information services using professional and company information. Our privacy program is designed to support responsible use of business contact data, data accuracy, transparency, and meaningful privacy rights. Where the GDPR applies to a particular processing activity, RampedUp relies principally on legitimate interests under Article 6(1)(f), subject to the safeguards described below.

1. Nature of the Data We Process

RampedUp focuses on professional and business contact information used in B2B contexts. Typical data elements may include an individual's name, job title, employer, business contact details, professional profile information, and related company information.

The information is generally derived from publicly accessible professional and business sources, including company websites, press releases, professional directories, public business records, and other sources where individuals or organizations have made professional information available.

RampedUp's services are intended for business and professional use. We do not position ordinary employment or business contact information as sensitive personal data merely because it identifies an individual.

2. Principal Lawful Basis: Legitimate Interests

Where GDPR applies, RampedUp relies principally on Article 6(1)(f), which permits processing when it is necessary for legitimate interests pursued by the controller or a third party, provided those interests are not overridden by the data subject's interests or fundamental rights and freedoms.

RampedUp's legitimate interests include:

- providing accurate business-to-business information and data enrichment services;
- validating, maintaining, and updating professional and company information;
- supporting responsible business communications and commercial outreach;
- helping customers maintain accurate records and reduce outdated or incorrect business contact information;
- and
- supporting business identity resolution, company research, and related commercial data-quality functions.

Legitimate-interest assessment

RampedUp evaluates legitimate-interest processing using the established three-part framework: identifying a legitimate interest, assessing whether the processing is necessary for that interest, and balancing that interest against the rights, freedoms, and reasonable expectations of the individual.

Several characteristics of RampedUp's processing are relevant to that balance: the information is professional rather than private in nature; it is typically made publicly available in a business context; its use is limited to business-information purposes; and individuals are provided mechanisms to access, correct, or request removal of information.

3. Public Professional Data and the Article 9 Distinction

Ordinary employment and professional contact information - such as a person's employer, title, business email address, or professional biography - generally does not fall within the special categories of personal data governed by Article 9 of the GDPR.

Article 9 imposes a substantially higher level of protection on specified special categories of personal data. Even within that heightened regime, Article 9(2)(e) recognizes an exception where the data subject has manifestly made the relevant information public.

RampedUp does not rely on Article 9(2)(e) as the lawful basis for ordinary employment information. Rather, the provision provides useful context: the GDPR itself recognizes that affirmative public disclosure is relevant even within a category of data subject to heightened restrictions. For ordinary professional data, RampedUp's lawful-basis analysis remains grounded in Article 6(1)(f), with public professional disclosure considered as part of the necessity, proportionality, and reasonable-expectations analysis.

4. Accuracy and Data Quality

Article 5(1)(d) establishes accuracy as a core GDPR principle. It is not a separate lawful basis for processing, but it is directly aligned with RampedUp's data-quality objectives.

RampedUp's services are designed in part to reduce inaccurate, stale, or incomplete business information. Maintaining current professional information can help customers avoid relying on obsolete titles, employers, contact details, or company relationships.

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

Under Article 14(5)(b) of the GDPR, RampedUp does not provide individualized notice to data subjects where providing that notice would be impossible or would involve disproportionate effort and the statutory conditions for the exemption are satisfied. In those circumstances, RampedUp maintains appropriate safeguards, including making relevant privacy information publicly available and providing accessible privacy-request and opt-out mechanisms.

The proportionality analysis may take account of factors such as the number of data subjects, the age and nature of the data, the professional context in which the information was published, the practical burden of individualized notification, and the safeguards available to individuals. RampedUp's public privacy information and opt-out mechanisms are part of those safeguards.

Public availability is also relevant to the overall privacy and reasonable-expectations analysis, but RampedUp does not treat public availability, standing alone, as the Article 14(5)(b) exemption.

6. Data Subject Rights and Access Requests

RampedUp provides privacy mechanisms through which individuals can request access to, correction of, or removal of personal information associated with them, subject to applicable law and appropriate identity verification.

Where Article 15 applies, RampedUp provides the personal data identified in its systems together with the supplementary information required by applicable law. This may include available source information, relevant purposes of processing, categories of personal data, applicable retention information, and recipients or recipient information where required and identifiable.

The right of access is a right to personal data and specified information about its processing. It does not convert a privacy request into a requirement to provide internal legal memoranda, privileged advice, or a bespoke legal analysis of the controller's compliance program.

Public opt-out list

As an additional transparency and privacy safeguard, RampedUp makes a public opt-out list available at <https://rampedup.io/opt-out-list>. This resource provides a publicly accessible mechanism for identifying records that have been opted out or suppressed from RampedUp's data products, supporting downstream awareness of privacy choices.

RampedUp's public opt-out list complements its individual privacy-request processes and is intended to help ensure that opt-out preferences are reflected consistently across applicable data uses and disclosures.

7. Data Privacy Framework and International Transfers

RampedUp is an active participant in the Data Privacy Framework (DPF) program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce.

RampedUp evaluates cross-border transfer obligations separately from the question of whether a particular processing activity falls within GDPR territorial scope. Where an applicable transfer mechanism or contractual safeguard is required, RampedUp's privacy and contractual processes are intended to support the relevant transfer requirements.

The DPF Program enables eligible U.S.-based organizations to certify their compliance pursuant to the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF.

Our certification can be found on their website here: <https://www.dataprivacyframework.gov/participant/7816>

Do Not Sell – Subject Access Request Portal

RampedUp is registered with several states within the United States as a data broker:

- California Data Broker Registration Number: 538248
- Oregon Data Broker Registration Number: 00344
- Texas Data Broker Registration Number: 20250186
- Vermont Data Broker Registration Number: 0409326

In compliance with the laws of California, Texas, Vermont, and Oregon, the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, RampedUp commits to provide, correct, limit, or eliminate data associated with Individuals or Organizations by completing the Subject Access Request form.

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

8. Public Web Collection and Terms of Service

RampedUp collects professional and business information from web pages that are publicly accessible without a login, paywall, password, or other authentication barrier. Website terms of service may govern the relationship between a website operator and users of its services, but a terms-of-service restriction does not, by itself, convert access to an otherwise publicly available web page into unauthorized access under the federal Computer Fraud and Abuse Act (CFAA).

In *Van Buren v. United States*, 593 U.S. 374 (2021), the U.S. Supreme Court interpreted the CFAA's 'exceeds authorized access' language using an access-based approach: the statute is concerned with obtaining information from areas of a computer system that a person is not entitled to access, rather than merely using information for a purpose that the system owner disfavors.

The Ninth Circuit applied the same access-control distinction in *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022). In that case, the court held that accessing publicly available LinkedIn profile information did not constitute access 'without authorization' under the CFAA where the information was available to the general public and no authentication gate had to be bypassed.

These decisions address the CFAA and should not be read to mean that every method or use of web scraping is exempt from other potentially applicable laws, contractual obligations, intellectual-property rights, privacy requirements, or state-law restrictions. RampedUp's collection practices are designed around publicly accessible business information and do not depend on circumventing login requirements, paywalls, passwords, or comparable technical access controls.

RampedUp also respects published technical crawling and indexing preferences used by website owners. Accordingly, our sourcing practices are intended to remain limited to information that can be accessed without authorization barriers and to operate consistently with applicable technical access rules and law.

9. Territorial Scope and Reservation of Position

RampedUp is a U.S.-based business. The fact that a record concerns a person who is European, an EU citizen, or located in Europe does not by itself determine whether the GDPR applies to RampedUp's processing.

For a controller or processor not established in the European Union, Article 3 generally requires an additional territorial nexus, such as processing related to offering goods or services to data subjects in the Union or monitoring

their behavior in the Union. Where processing is carried out in the context of an EU establishment, Article 3 may apply regardless of where the underlying systems or servers are located.

Accordingly, RampedUp's provision of privacy rights, access tools, correction mechanisms, or other GDPR-aligned safeguards should not be interpreted as a concession that the GDPR applies to every RampedUp record or processing activity involving a person located in Europe. RampedUp may provide such protections as a matter of privacy practice while separately reserving its position regarding territorial applicability in any particular case.

10. Practical Privacy Commitments

- Professional and company information is used for legitimate B2B information purposes.
- Data quality and accuracy are core operational objectives.
- Individuals are provided practical mechanisms to access, correct, or request removal of information.
- RampedUp evaluates lawful basis, transparency, and cross-border transfer requirements according to the processing activity involved.
- RampedUp does not treat voluntary cooperation with a privacy request as a blanket admission of GDPR territorial jurisdiction.

Reference Framework

This brief reflects RampedUp's general privacy and compliance position and is intended to explain its approach in a concise, client-facing format. It is based on Regulation (EU) 2016/679 (GDPR), European Data Protection Board guidance concerning Article 3 territorial scope and Article 6(1)(f) legitimate interests, and the U.S. Department of Commerce Data Privacy Framework program materials.

This document is informational and describes RampedUp's general compliance approach. Specific obligations may depend on the facts of a particular processing activity, contractual relationship, jurisdiction, or data-subject request.