

Privacy Policy

This Privacy Policy is issued on behalf of Dunn Regulatory Associates (“DRA”) (“we”, “us” or “our”), a part of the Acacium Group.

This Privacy Policy covers how we collect, use, share and process your Personal Information, provides certain information that is legally required and lists your rights in relation to your Personal Information.

Dunn Regulatory Associates, LLC is committed to protecting the confidentiality and privacy of information entrusted to it. As part of this fundamental obligation, DRA is dedicated to the appropriate protection and use of personal information that has been collected by or provided to us through our website (collectively, the “Online Services”).

Please review this Privacy Statement to learn more about how we collect, use, share and protect the personal information that we have obtained. By using DRA’s website, you consent to the collection and processing of your information as set forth in this Privacy Statement, now and as amended by us from time to time.

What information do we collect?

Dunn Regulatory Associates (“DRA”) collects information that can identify an individual or relates to an identifiable individual (“Personal Information”) to provide services to you and to operate our business. The type of Personal Information we collect depends on the situation. We collect Personal Information by different methods depending on whether the individual is a prospective or existing client, supplier, vendor, or website user.

The following provides examples of the type of information that we collect in a variety of contexts and how we use that information.

Context	Types of Information (Examples)	Primary Purpose for Collection and Use
Contact data	We may collect information about data subjects such as name and contact details (email, phone number, etc.) in order to communicate and facilitate the provision of our services with our clients or potential clients.	Order to carry out the client’s engagement with DRA

Services data	Personal data may be provided to us by clients to the extent required to perform the services. DRA may also acquire personal data from a third party at the direction of our client as required to perform services.	
Marketing information:	We may collect information to respond to inquiries regarding our services or to provide you with information, reports, or updates.	
Website visitor information:	<ul style="list-style-type: none"> • When you visit our website, we may collect information about your visit such as your IP address and the pages you visited and when you use our services we may collect information on how you use those services. • For security purposes. For example, we may use your data to protect DRA and its third parties against security breaches and to prevent fraud and violation of DRA's applicable agreements (where the processing is necessary for our legitimate business interests). <p>Whenever we process your personal data for our legitimate interests, we make sure to consider and balance any potential impact on you and your rights under data protection laws. Our legitimate business interests do not automatically override your interests - we will not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You have the right to object to this processing if you wish.</p>	

How do process the information we collect?

Personal data is processed both manually and electronically in accordance with the above-mentioned purposes and in compliance with current regulations. We permit only authorized DRA employees and Third-Party processors to have access to your information. Such employees and Third-Party processors are appropriately designated and trained to process data only according to the instructions we provide them.

How do we store the data we collect?

DRA will retain personal data for a reasonable period, taking into account legitimate business needs to capture and retain such information. Information will also be retained for a period necessary to comply with state, local, federal regulations, or country specific regulations and requirements.

Why might we share your information with third parties?

We may share data with Acacium Group and its group of companies. We do not share personal information with unaffiliated third parties, except as stated in this Privacy Policy, including as necessary for our legitimate professional and business needs, to carry out your requests, as required or permitted by law or professional standards, or otherwise with your consent.

In some instances, DRA may share personal information about you with third-party service providers and vendors working on our behalf. These third parties include providers of administrative, website hosting, data analysis, data back-up and security management services. Each such third party is required to safeguard personal information in accordance with its contractual obligations and data protection legislation applicable to its provision of services.

DRA may disclose personal information in order to respond to lawful requests of government or law enforcement agencies, including to meet national security or law enforcement requirements or where disclosure is required by applicable laws, court orders, or government regulations. In the event that the ownership of DRA or their assets changes as the result of a merger, acquisition, or sale of assets, information owned or controlled by DRA may be transferred to another company. Information may also be shared in connection with the consideration, negotiation, or completion of a corporate transaction in which we are acquired by or merged with another company or we sell, liquidate, assign or transfer all or a portion of our assets. These disclosures may also be needed for data privacy or security audits and/or to investigate or respond to a complaint or security threat. DRA does not sell personal information to any third parties. Also, DRA will not transfer the personal information you provide to any third parties for their own direct marketing use.

DRA may also share personal data between entities within our corporate group for several reasons, including:

- **Service Delivery & Operational Efficiency:** Ensuring smooth operations by sharing data for administrative, HR, IT, finance or customer service purposes.
- **Regulatory Compliance & Risk Management:** Meeting legal obligations, conducting internal audits, and managing risks across the organization.
- **Security & Fraud Prevention:** Protecting against security threats, cyber risks, and fraud by implementing centralized monitoring and threat detection.
- **Research & Analytics:** Using aggregated or pseudonymized data to improve products, services, and customer experiences.

To ensure that intra-group data sharing is lawful, transparent, and secure, we have established an intra-group data sharing agreement between group entities that define purpose, scope, and legal basis for data sharing.

We do not share personal information with unaffiliated third parties, except as stated in this Privacy Policy, including as necessary for our legitimate professional and business needs, to carry out your requests, as required or permitted by law or professional standards, or otherwise with your consent.

Residents of European Union and United Kingdom

For residents of the European Union (and United Kingdom), DRA is the data controller responsible for your personal information collected pursuant to this Privacy Policy. Our digital operations are conducted in the United States. Regardless of where you live, you consent to have your personal data transferred to, processed and stored in the United States, and allow DRA to use and collect your personal information in accordance with this Privacy Policy.

In addition, residents of certain countries, including European Union member states (and the United Kingdom), have some or all of the following rights with respect to personal information collected from and about them on the Online Services: the right to request access to, and the correction, erasure, and/or restriction of processing of, such personal information; in some instances, the right to object to the processing of such personal information; in some instances, the right to request that DRA export, in a structured, commonly used, and machine readable format, and transmit to another controller, such personal information; and the right to withdraw, at any time, any consent to the processing of such personal information. To exercise these rights, please contact DRA via email at Privacy.Team@acaciumgroup.com.

Additional Disclosures for California Residents

This section applies to any California residents about whom we have collected personal information, including through use of our website, by utilizing our services, or by communicating with us electronically.

For purposes of this section, “personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer or household. Personal information does not include publicly available information or information that has been de-identified.

Information we collect

The types of personal information we collect about you will depend on your relationship DRA. For example, in many cases, we may collect personal information from our business clients during the course of an engagement to provide services to our clients, and our collection and use of personal information is governed by our contract with that entity.

We may collect the following categories of personal information:

- **Identifiers**, which may include real name and alias; postal address; unique personal identifier; online identifiers as detailed below; email address; telephone number; and/or other similar identifiers.
- **Commercial information**, which may include services purchased, obtained, or considered; account balances, payment history, or account activity; bank account and other information relating to your financial institution; and/or other purchasing or consumer histories or tendencies.
- **Professional or employment-related information**, which may include information regarding your current employers; job title and responsibilities; and
- **Geolocation data**: we do not collect any geolocation data

Purposes and Sources of Collection

We may collect or use personal information for the following purposes:

- Auditing and compliance with policy, procedures, laws, regulations, and professional standards;
- Billing, payment, and fulfillment;
- Protect against fraud and other malicious or illegal activity;
- Customer and client communications;

- Customer and client relationship management;
- General business administration;
- Provision and performance of the services;
- Internal analytics and benchmarking;
- Marketing our services;
- Financial reporting and accounting;
- Administer, maintain, and improve the website and services; and
- Systems and data security.

We may collect personal information from the following sources:

- Our clients and customers and prospective clients and customers or their authorized representatives, including via documentation, forms, communications and interactions with us, and through our website
- Government entities and databases, such as anti-fraud databases, sanctions lists, and court judgments; and
- Publicly available sources.

Disclosures of Information

Categories of Third Parties With Whom We Share Information

We may share personal information as described in this Privacy Policy, including with the following categories of third parties:

- **Technical and Operational Service Providers and Business Partners.** We may engage third parties to perform certain functions on our behalf. To do so, we may disclose personal information to our third-party business partners and service providers in order to maintain and operate the websites and provide, improve, and personalize the services, including to fulfil requests for the services and for other technical and processing functions, such as sending e-mails on our behalf, fulfilling orders, and technical support. We may also share personal information to service providers or other third parties to detect, protect against, and respond to security incidents or other malicious, deceptive, illegal, or fraudulent activity or other threats.
- **Government Entities.** We may share personal information with government entities and agencies, regulators, law enforcement, and other third parties, including to provide the services, comply with applicable laws and regulations, to respond to a subpoena, search warrant, or pursuant to legal process, and to establish or exercise our legal rights or for fraud- or crime-prevention purposes.

- **Professional Service Firms.** We may share personal information with other professional service firms in connection with our legal, regulatory, and professional obligations and to establish or exercise our rights and defend against claims, including, for example, auditors, law firms, and consultants.

Disclosures of Personal Information for Business or Commercial Purposes

We may have disclosed the following types of personal information to third parties for a business or commercial purpose in the previous twelve (12) months:

- Identifiers
- Commercial information
- Information relating to Internet activity or other electronic network activity
- Professional or employment-related information
- Other personal information not listed above and described in California Civil Code 1798.80(e)

International Transfers

As a multi-national company, we transmit information between and among our affiliates. We also maintain relationships with service providers who are based in foreign countries. As a result, your information may be processed in a foreign country where privacy laws may be less stringent than the laws in your country. Nonetheless, where possible we take steps to treat Personal Information using the same privacy principles that apply pursuant to the law of the country in which we first received your information. By submitting your Personal Information to us you agree to the transfer, storage and processing of your information in a country other than your country of residence including, but not necessarily limited to, the United States. If you would like more information concerning our attempts to apply the privacy principles applicable in one jurisdiction to data when it goes to another jurisdiction you can contact us using the contact information below.

How do we safeguard your information?

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

In the event that we are required by law to inform you of a breach to your Personal Information we may notify you electronically, in writing, or by telephone, if permitted to do so by law.

How long do we keep your information for?

We will retain your personal information for as long as required to provide services or complete the transaction also after you no longer wish to engage our services.

We retain your personal information so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy or applicable laws and regulations that may apply in a particular jurisdiction.

Cookies

You can set your browser to refuse some or all cookies, or to indicate when a cookie is being sent to your computer. However, this may prevent our websites or services from working properly. You can also set your browser to delete cookies every time you finish browsing. For more information about how to manage browser cookies, please follow the instructions provided by your browser.

Communications Opt-Out

We may periodically send you messages or notifications of your account statuses, and marketing communications. All such material will have information on how to opt out of receiving those messages.

Additional Information for California Residents

If you are a California resident, the following privacy disclosures apply to you in addition to the rest of the Privacy Policy. For purposes of this section, "Personal Information" means information that identifies, relates to, describes, and is reasonably capable of being associated with, or could be linked, directly or indirectly, with a particular individual or household.

California Sensitive Information Disclosure

We may collect the following categories of sensitive Personal Information (as defined under California law): social security, driver's license, state identification card, or passport number; account log-in, financial account, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, or union membership; health-related information; information concerning sex life or sexual orientation. This information is collected in order to assess your eligibility for employment, provide certain benefits, comply with applicable laws and regulations, for diversity and inclusion programs, manage our business, or provide you with services and for security purposes. Note that we do not use such information for any purposes that are not identified within the California

Privacy Rights Act Section 1798.121. We do not “sell” or “share” sensitive Personal Information for purposes of cross-context behavioral advertising.

Your California Privacy Rights

California residents have the following rights:

- **Access to Your Information.** You may request access to your Personal Information, including a copy of the information we have about you.
- **Deletion of Your Information.** You may request that we delete your Personal Information, subject to certain exceptions.
- **Correction of Your Information.** You may ask us to correct information that is inaccurate or incomplete. Note that we may keep historical information in our backup files as permitted by law.
- **Opt Out of Sharing of Your Information for Purposes of Cross-Context Behavioral Advertising.** You may opt-out of the sharing of your Personal Information for purposes of cross-context behavioral advertising.

Please note, not all of the rights described above are absolute, and they do not apply in all circumstances. In some cases, we may limit or deny your request because the law permits or requires us to do so, or if we are unable to adequately verify your identity. We will not discriminate against individuals who exercise their privacy rights under applicable law.

If you would like to exercise any of these rights, please send an email with the subject line, “California Privacy Rights” to Privacy.Team@acaciumgroup.com or call us at (866) 877-1514.

To protect your information, we must be able to verify your identity before we can process your request to exercise any of the foregoing privacy rights. We may conduct the verification process by email or phone, and we may ask you to provide information such as your name, contact information, and any additional relevant information based on your relationship with us.

California residents may designate an authorized agent to submit requests to exercise certain privacy rights on their behalf. If you are an authorized agent submitting a request on behalf of a California resident, you must provide us with a copy of the signed permission you have been given indicating that you are able to act on that person’s behalf.

“Do Not Track” disclosure

We do not currently recognize the “Do Not Track” signal.

Contact Us

If you have any questions or concerns about this Privacy Policy or the information practices of our Services, please email us Privacy.Team@acaciumgroup.com or call us at (866) 877-1514.

You may also write us at:

Dunn Regulatory Associates, LLC
8609 Westwood Center Drive, Ste. 110
Vienna, VA 22182

If you need to access this Privacy Policy in an alternative format due to having a disability, please contact us at the appropriate address above.

Changes to Privacy Policy

Dunn Regulatory Associates, LLC (“DRA”) may change this Privacy Policy from time to time due to changes in relevant law or our business practices. When changes are made to this Privacy Policy, we will post the changes on this website, and they will become immediately effective when posted. You can check the “Last Updated” legend at the bottom of this page to see when this Privacy Policy was last revised.

Last updated and effective date: November, 2025