

CrescoNet Global Privacy Policy

Last updated: 14 May 2026

1. About CrescoNet and this Policy

CrescoNet LLC and its affiliates (collectively, “CrescoNet”, “CrescoNet Group”, “we”, “us” or “our”) are a leading provider and integrator of highly resilient and secure, public and private LTE/5G multi-application networks and DER solutions for electric, water and gas utilities.

This Privacy Policy describes how we collect, use, disclose and otherwise process Personal Information when you visit or interact with our website at www.cresconet.com (the “Website”), engage with our sales and marketing activities, apply for a role with us, or receive our products or services (together with the Website, the “Services”). It applies to all CrescoNet Group companies unless a local CrescoNet affiliate has published a separate notice for its jurisdiction.

If you have entered into a contract with us, the terms of that contract take precedence over this Privacy Policy to the extent of any inconsistency, provided that nothing in any contract will operate to waive rights you have under applicable law.

2. Controller of Your Personal Information

Unless stated otherwise at the point of collection, the data controller (or equivalent under local law) for Personal Information processed through the Website is:

CrescoNet (USA) LLC
80 Liberty Ship Way, Unit 6
Sausalito, California, 94965
USA
Email: PrivacyOfficer@cresconet.com

For Personal Information relating to individuals resident in a jurisdiction where a local CrescoNet affiliate operates, that affiliate may act as the controller alone or jointly with CrescoNet.

3. Personal Information We Collect

“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 an identified or identifiable individual or household. In some jurisdictions this is referred to as “personal data” or “personally identifiable information” — we use “Personal Information” throughout this Policy to cover all of those.

The categories of Personal Information we collect, and examples of each, are set out in the table below:

Category	Examples	Sources
Identifiers	Name, postal address, email, phone, online identifiers, IP address, account username	You directly; your use of the Website; third-party sign-in providers

Commercial information	Records of products or services requested, purchased or considered	You directly; our business systems
Internet/network activity	Browsing history on the Website, interactions with pages and advertising, referring URL, device and browser information, time-zone setting	Cookies and similar technologies; analytics and advertising partners
Geolocation (approximate)	Approximate location derived from IP address	Cookies and analytics
Professional/employment	Job title, employer, business contact details, CV/résumé content if you apply for a role	You directly; recruitment platforms; references you provide
Audio/visual	Recordings of customer support calls where permitted by law; photos you submit	You directly; our support platforms
Inferences	Preferences and characteristics inferred from the above to personalise content and marketing	Derived by us or our service providers
Social network profile information	Name, image, posts, preferences made available by social network services you connect	Social network platforms where you authorise the connection
Account credentials	CrescoNet username and password, third-party access tokens	You directly

We do not knowingly collect the following, and if you believe we have, please contact us:

- Government-issued identifiers beyond what is strictly necessary for contracting or compliance
- Precise geolocation
- Contents of your private communications not directed to us
- Biometric or genetic data
- Health data
- Information about racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sex life or sexual orientation
- Criminal conviction or offence data

Sensitive Personal Information (California and certain other US states).

Some categories listed above (such as account credentials) are treated as “sensitive personal information” under the CCPA. We use and disclose such information only for the business purposes permitted under Cal. Civ. Code § 1798.121 and comparable provisions of other state laws, and we do not use or disclose it for purposes that would trigger a consumer’s right to limit under the CCPA. [CONFIRM WITH COUNSEL based on actual processing activities.]

Children.

The Services are not directed to children. We do not knowingly collect Personal Information from children under 13 (or the equivalent minimum age under local law — e.g. under 16 in the EU/UK unless member-state law specifies a lower age down to 13). In the US, several states require opt-in consent before selling or sharing the Personal Information of consumers aged 13–16; we do not knowingly sell or share the Personal Information of any consumer under 16 without the required

consent. If you become aware that a child has provided us with Personal Information, please contact us and we will take steps to delete it.

4. How We Use Personal Information

We process Personal Information for the purposes set out below. Where we rely on the GDPR or UK GDPR as the lawful basis for processing (because you are in the EU, UK or another jurisdiction that applies an equivalent framework), the legal basis is indicated in the right column.

Purpose	Legal basis (EU/UK)
Provide the Website and Services you request; create and administer your account; respond to enquiries	Performance of a contract; legitimate interests
Bill for Services and manage payments	Performance of a contract; legal obligation
Communicate with you about the Services, including service notices and security alerts	Performance of a contract; legitimate interests; legal obligation
Send marketing communications about products, services and events	Consent (where required) or legitimate interests (where permitted)
Measure and improve the Website and Services, including analytics and product development	Legitimate interests; consent where required for non-essential cookies
Personalise content and (where permitted) deliver targeted advertising	Consent (where required) or legitimate interests (where permitted)
Recruitment and assessment of job applicants	Steps to enter into a contract; legitimate interests; consent where required
Security, fraud prevention, system administration and protecting rights	Legitimate interests; legal obligation
Comply with law; respond to lawful requests; establish, exercise or defend legal claims	Legal obligation; legitimate interests
Corporate transactions (mergers, acquisitions, financings, reorganisations, asset sales)	Legitimate interests

We will only use Personal Information for the purposes for which it was collected, a compatible purpose, or as otherwise permitted or required by law. If we need to use Personal Information for an unrelated purpose, we will notify you and, where required, seek your consent.

Automated decision-making and profiling.

We do not use Personal Information to make decisions that produce legal or similarly significant effects about you solely on the basis of automated processing.

5. How We Share Personal Information

We share Personal Information with the following categories of recipients:

- CrescoNet Group companies, to operate our business and provide the Services.
- Service providers and processors that perform services on our behalf, including cloud hosting, data storage, analytics, IT support, customer relationship management, marketing automation, email delivery, payment processing and professional advisers (lawyers, accountants, auditors).
- Advertising and analytics partners (e.g. Google, LinkedIn, Meta) in connection with online advertising and measurement. Some of these sharing activities constitute “sharing” for cross-context behavioral advertising under the CCPA (see Section 9).

- Other third parties at your direction, including when you use a social sign-in or authorise us to connect to another service.
- Government authorities, regulators, courts and law enforcement, where required by law, legal process, or to protect rights, property or safety.
- Counterparties to a corporate transaction, such as a proposed or completed merger, acquisition, financing, reorganisation or sale of assets. In such a transaction we will use reasonable efforts to require that Personal Information continues to be handled consistently with this Policy.

We do not sell Personal Information for monetary consideration.

Under the CCPA, certain disclosures to advertising partners in connection with cross-context behavioral advertising may nonetheless be considered “sharing” or “sale”. We provide California residents with the right to opt out of such sharing — see Section 9. [CONFIRM WITH COUNSEL after reviewing actual ad-tech stack — Google Ads, LinkedIn Insight Tag and Meta Pixel may constitute “sale” and/or “sharing” under CCPA.]

The categories of Personal Information disclosed to service providers and contractors, and to third parties, in the preceding 12 months are set out in Section 3 (all categories). We do not use or disclose sensitive personal information for purposes that would trigger a right to limit under the CCPA.

6. International Data Transfers

CrescoNet is a global organisation. Personal Information we collect may be transferred to, stored in, and processed in the United States and other countries where we, our affiliates or our service providers operate. Those countries may have data protection laws that differ from those in your country of residence.

Where we transfer Personal Information out of the European Economic Area, United Kingdom, Switzerland, or another jurisdiction that restricts international transfers, we rely on one or more of the following safeguards:

- Adequacy decisions of the European Commission, UK Government or equivalent body;
- The European Commission’s Standard Contractual Clauses (2021), the UK International Data Transfer Agreement or Addendum, and the Swiss Addendum, as applicable, together with any supplementary measures required following Schrems II;
- Certification under the EU–US Data Privacy Framework, UK Extension, and Swiss–US Data Privacy Framework [CONFIRM WITH COUNSEL whether CrescoNet LLC is or intends to be DPF-certified];
- Other transfer mechanisms recognised under applicable law; or
- Your explicit consent or another derogation, where appropriate.

You may request a copy of the relevant transfer safeguards by contacting us using the details in Section 13.

7. How Long We Retain Personal Information

We retain Personal Information only for as long as necessary for the purposes for which it was collected, including to satisfy any legal, accounting, tax, regulatory or reporting requirements, to resolve disputes and to enforce our agreements. When deciding how long to retain information we

consider its nature and sensitivity, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process it, whether those purposes can be achieved by other means, and applicable legal requirements.

Indicative retention periods are:

- Website visitor and analytics data: typically 14 to 26 months from collection.
- Marketing contacts: for as long as you remain subscribed and for a reasonable period thereafter (no longer than 3 years) for suppression-list purposes.
- Customer account and transaction records: for the duration of the relationship and up to 7 years thereafter, or longer where required for tax, audit or regulatory reasons.
- Recruitment records: typically 12 months after the end of the recruitment process, unless you consent to longer retention for future opportunities.
- Security logs and incident records: typically 12 to 24 months.

8. Your Privacy Rights

Depending on where you live, you may have some or all of the following rights. We respond to requests within the timeframes required by applicable law (generally 45 days under US state laws, with a possible 45-day extension; 30 days under the GDPR, extendable by two months for complex requests).

- Right to know / access: confirm whether we process Personal Information about you and obtain a copy of it, including (under CCPA) information beyond the preceding 12 months where we have retained it.
- Right to correct / rectify inaccurate Personal Information.
- Right to delete / erase Personal Information, subject to legal exceptions.
- Right to data portability: receive your Personal Information in a structured, commonly used, machine-readable format, and, where technically feasible, have it transmitted to another controller.
- Right to opt out of targeted advertising, sale, or sharing of Personal Information.
- Right to opt out of certain profiling that produces legal or similarly significant effects.
- Right to limit the use and disclosure of sensitive personal information (California).
- Right to withdraw consent at any time where we rely on consent, without affecting the lawfulness of processing before withdrawal.
- Right to object to processing based on legitimate interests, and to direct marketing.
- Right to restrict processing in certain circumstances.
- Right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects.
- Right to appeal: if we decline a request, you may appeal (required in several US states including Colorado, Connecticut, Virginia, Texas and others).
- Right to lodge a complaint with your local data protection authority (EU/UK/EEA) or with the California Privacy Protection Agency or your state Attorney General (US).
- Right to non-discrimination for exercising your rights.

To exercise any of these rights, contact us using the details in Section 13, or use the request mechanisms on our Website. We will take reasonable steps to verify your identity before acting on your request. You may also use an authorised agent, subject to verification.

9. US State Privacy Rights Notice

This section provides additional disclosures for residents of US states with comprehensive privacy laws in effect as of the date at the top of this Policy, including California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia. [CONFIRM WITH COUNSEL which of these states CrescoNet meets the applicability thresholds for — some of the obligations below only apply if thresholds are met, but publishing the rights framework is common practice.]

Categories, sources, business purposes and recipients.

See Sections 3, 4 and 5.

“Sale” and “Sharing”.

We do not sell Personal Information for monetary consideration. We do “share” Personal Information, as that term is defined under the CCPA, with advertising and analytics partners in connection with cross-context behavioral advertising. The categories shared are: identifiers, internet/network activity information, approximate geolocation, and inferences. You have the right to opt out of this sharing.

How to exercise your rights:

- Use the “Your Privacy Choices” / “Do Not Sell or Share My Personal Information” link in the Website footer.
- Email us at PrivacyOfficer@cresconet.com.
- Use the request form at [INSERT URL].
- We honour Global Privacy Control (GPC) and other recognised Universal Opt-Out Mechanisms when sent from a browser or device. When we process an opt-out preference signal we will display confirmation on the Website.

Sensitive Personal Information.

See Section 3. If in the future we use or disclose sensitive personal information for purposes that would trigger the right to limit, we will provide a “Limit the Use of My Sensitive Personal Information” link and notice at the point of collection.

Non-discrimination.

We will not discriminate against you for exercising any of your privacy rights.

Appeals (Colorado, Connecticut, Virginia, Texas and other states with an appeal right).

If we decline your request, you may appeal by replying to the response email or by contacting us at PrivacyOfficer@cresconet.com. We will respond to appeals within the timeframe required by your state’s law (typically 45 or 60 days). If your appeal is denied, you may contact your state Attorney General.

Financial incentives.

We do not offer financial incentives in exchange for Personal Information.

10. Cookies and Similar Technologies

We and our service providers use cookies, pixels, SDKs, local storage and similar technologies on the Website to:

- Make the Website function (strictly necessary);
- Remember your preferences (functional);
- Measure how the Website is used and improve it (analytics); and
- Deliver and measure advertising about CrescoNet on other platforms (advertising / targeting).

On your first visit, and at intervals thereafter, you will see a cookie banner allowing you to accept, reject, or manage non-essential cookies. You can change your choices at any time via the “Cookie Preferences” link in the Website footer. You can also control cookies through your browser settings and through opt-out preference signals (see Section 9).

A current list of the cookies we use, their purposes, durations and providers is available in our [Cookie Policy](#).

11. Marketing Communications

We may send you electronic marketing communications about our products, services and events where permitted by law, either with your consent or on the basis of a “soft opt-in” where that is allowed in your jurisdiction and you have not objected.

You can opt out of marketing at any time by:

- Using the unsubscribe link in any marketing email;
- Updating your preferences in your account (if applicable); or
- Contacting us at PrivacyOfficer@cresconet.com.

Opting out of marketing does not affect service or transactional communications necessary to provide the Services.

12. Security and Data Breaches

We maintain reasonable and appropriate administrative, technical, physical and organisational safeguards designed to protect Personal Information from loss, misuse, unauthorised access, disclosure, alteration or destruction. These include, where appropriate, encryption in transit and at rest, access controls, network monitoring, penetration testing, and employee training.

No security measures are perfect. In the event of a Personal Information breach that triggers notification obligations under applicable law, we will notify affected individuals and relevant regulators as required.

13. Contact Us and Complaints

If you have any questions or concerns about this Policy, or wish to exercise any of your rights, please contact our Privacy Officer:

By email: PrivacyOfficer@cresconet.com

If you are in the EU, UK or EEA, you have the right to lodge a complaint with your local supervisory authority. If you are in a US state with comprehensive privacy legislation, you may contact your state Attorney General or, in California, the California Privacy Protection Agency. In Australia, you may contact the Office of the Australian Information Commissioner (OAIC). In New Zealand, you may contact the Office of the Privacy Commissioner. We ask that you contact us first so that we have an opportunity to address your concerns.

14. Regional Notices

14.1 European Economic Area, United Kingdom and Switzerland

The legal bases on which we process Personal Information are set out in Section 4. You have the rights listed in Section 8, which you may exercise free of charge, subject to the conditions and exceptions in the GDPR / UK GDPR / Swiss FADP. Transfers outside the EEA, UK or Switzerland are described in Section 6.

14.2 United States — State-Specific Rights

See Section 9 and the rights in Section 8. Additional state-specific rights are available on request.

14.3 Australia

We handle Personal Information in accordance with the Australian Privacy Principles under the Privacy Act 1988 (Cth). You may request access to and correction of Personal Information we hold about you, and you may complain about a breach of the APPs by contacting our Privacy Officer. If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner.

14.4 New Zealand

We handle Personal Information in accordance with the Privacy Act 2020 and the Information Privacy Principles. You may contact our Privacy Officer to access or correct your Personal Information, or to make a complaint. If you are not satisfied with our response, you may contact the Office of the Privacy Commissioner.

14.5 Canada

We handle Personal Information in accordance with PIPEDA and applicable provincial laws, including Quebec's Law 25.

14.6 Other Jurisdictions (APAC, Latin America, Middle East)

Where we are subject to other data protection laws (including Singapore PDPA, Thailand PDPA, Indonesia PDP Law, Philippines DPA, Vietnam PDPD, Malaysia PDPA, Japan APPI, Korea PIPA, Brazil LGPD, UAE PDPL, Saudi PDPL and others), we handle Personal Information in accordance with those laws. Specific local notices may be published by CrescoNet affiliates where required.

15. Links to Other Sites

The Website may contain links to third-party websites. We are not responsible for the privacy practices of those sites. When you follow a link to a third-party site, you should read that site's privacy notice.

16. Changes to this Policy

We may update this Policy from time to time to reflect changes in our practices or legal requirements. We will post the updated Policy on the Website and update the "Last updated" date at the top. If changes are material, we will use reasonable efforts to notify you, for example by email or via a notice on the Website, before the changes take effect. Your continued use of the Services after the effective date of the revised Policy constitutes acceptance of it, except where further action is required to make changes effective under applicable law.