KRY10 GROUP
DATA PRIVACY POLICY

Welcome to Kry10 Group's data privacy policy.

This data privacy policy covers the usage and protection of personal data by Kry10 Group, which comprises the following legal entities (collectively referred to as **Kry10**, **we**, **us** or **our**):

Entity	Jurisdiction	Primary Role
Kry10 Holdings	United States	Parent company
Kry10 NZ	New Zealand	NZ operations
Kry10 Corporation	United States	US operations; DPF certificate holder
Kry10 Pty Ltd	Australia	Australian operations
Kry10 UK Ltd	United Kingdom	UK operations

Kry10 respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from) or contact us via email or phone and share your data with us. It also tells you about your privacy rights and how the law protects you.

1. Important information and who we are

Purpose of this privacy policy

This privacy policy aims to give you information on how Kry10 collects and processes your personal data through your use of this website, our social media channels and other platforms provided by us, including any data you may provide through this website when you complete any forms on our site or send any information to us as well as any data that you provide to us in person, via email or on the phone. It is important that you read this privacy policy so that you are fully aware of how and why we are using your data.

We do not collect any data relating to children.

We are the controller and responsible for your personal data. If you have any questions on this policy, including any questions about this policy or how we handle your personal data, or if you wish to exercise your legal rights under *Your legal rights*, please contact us using the details under *Privacy Contacts.*

Your duty to inform us of changes

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

Our website may include links to third-party websites. We do not control, and are not responsible, for the content or practices of these websites. The inclusion of such links does not imply our endorsement of these websites, their content, their owners, or their practices. This privacy policy does not apply to these other websites. These websites are subject to their own privacy and other policies. We recommend reviewing the privacy policies of any third-party websites you visit.

2. The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes first and last name, username and password.
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account and payment card details.
- **Transaction Data** includes billing information and payment details (processed via PCI – compliant third-party payment processors).
- **Technical Data** includes internet protocol (IP) address, device identifiers, browser and operating system information, telemetry, diagnostics, your login data, time zone setting and location, and other technology on the devices you use to access this website.
- **Usage Data** includes information about how you use our website and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We do not collect any **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes processing personal data for the purpose of:
  - providing and maintaining our services to you.
  - notifying you about changes to our services.
  - providing client support.
  - gathering analysis or valuable information so that we can improve our services.
  - monitoring the usage of our services.
  - detecting, preventing and addressing technical issues.
  - providing you with news, special offers and general information about other services which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information.
  - entering a promotion, competition, prize draw and you contact us, or we contact you.
- **Indirect interactions.** We may contact you indirectly via our social media platforms for the purpose of entering a promotion, competition or prize draw and notifying you if you are a winner. This may include actions such as tagging you on our posts or liking your posts.
- **Automated technologies or interactions.** As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our cookie policy for further details.
- **Third parties or publicly available sources.** We will receive personal data about you from various third parties and public sources as set out below:

  Technical Data from the following parties:

  (a) analytics providers such as Google;

  (b) advertising networks such as Google;

  (c) search information providers such as Google; and

  (d) marketing platform providers such as Mailchimp.

Cookies

We use cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site. A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to

your computer's hard drive. We use the strictly necessary cookies which are essential to provide you with services available through the website and to enable you to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these cookies, the services that you have asked for cannot be provided, and We only use these cookies to provide you with those services.

You can manage your cookie preferences at any time by using our cookie banner. You may accept all cookies, disable cookies where possible to do so or adjust settings by category. You can also control cookies through your browser settings, including blocking or deleting cookies. How to do this depends by browser. Please note that disabling certain cookies may affect the functionality and performance of the website and some features may not work as intended.

4. How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where it is necessary for our recognised legitimate interests (**RLIs**). These are different to legitimate interests. RLIs apply where there are public interest reasons for processing (such as preventing or detecting crime, safeguarding individuals, responding to emergencies, supporting national or public bodies when they confirm it is necessary for their official functions). RLIs are legally recognised within data protection law. Where we rely on an RLI, we will ensure the use is strictly necessary and only use or share the minimum data required.
- Where we need to comply with a legal obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal grounds, we are relying on to process your personal data where more than one ground has been set out in the table below:

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a client or supplier	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your services including: (a) managing and maintaining client relationships (b) managing payments, fees, and charges (c) collecting and recovering money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
(a) notifying you about changes to our terms or privacy policy (b) asking you to leave a review or take a survey	(a) Identity (b) Contact (c)Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how client use our services)
To enable you to complete a survey	(a) Identity (b) Contact (c) Usage (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how clients use our services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests and RLIs (for running our business, provision of administration and IT services, network security and to prevent fraud) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Usage (d) Marketing and Communications (e) Technical	Necessary for our legitimate interests (to study how clients use our services, to develop them, to grow our business and to inform our marketing strategy)

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To use data analytics to improve our website, services, marketing and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of clients for our services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Marketing and Communications	Necessary for our legitimate interests (to develop our services and grow our business)

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

Promotional offers from us

We may use your Identity, Contact, Technical and Usage Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased services from us and you have not opted out of receiving that marketing.

Third-party marketing

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at any time.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. International Transfer of Data

Your personal data may be collected, transferred, and stored by us in the US, our home jurisdiction, as well as in our offices or affiliates located in other countries where we operate, including the UK, Australia and New Zealand. This may also include countries that do not provide the same level of data protection as your home jurisdiction. We are committed to ensuring that your personal data is handled in accordance with applicable data protection laws, including but not limited to the UK General Data Protection Regulation (**UK GDPR**), the Data Protection Act 2018 (**DPA**) and the Data (Use and Access) Act 2025 (**DUAA**) in the UK, the EU General Data Protection Regulation (**EU GDPR**), the Privacy Act 1988 in Australia, the Privacy Act 2020 and Privacy Amendment Act 2025 in New Zealand, the California Consumer Privacy Act (**CCPA**) and Washington My Health My Data Act in the US and other applicable global privacy regulations.

To safeguard your personal data during international transfers, we have implemented robust measures, including:

1. **Data Sharing Agreement**
   We have established a data sharing agreement between our legal entities and affiliates to ensure that your data is adequately protected, irrespective of where it is processed. This agreement is designed to meet the requirements of global privacy laws, including the EU GDPR's provisions for cross-border data transfers.
2. **Standard Contractual Clauses (SCCs):**
   For transfers originating from the European Economic Area (**EEA**) or the UK to countries outside these regions, we rely on SCCs approved by the European Commission. These legally binding clauses provide safeguards to ensure your data receives an equivalent level of protection.
3. **Adequacy Decisions:**
   Where applicable, we may transfer personal data to countries deemed by the European Commission to provide an adequate level of protection.
4. **Supplementary Measures:**
   In cases where data is transferred to jurisdictions without adequacy decisions, we implement additional safeguards such as data encryption, pseudonymization, and strict access controls to protect your information.
5. **Compliance with Local Laws:**
   All data transfers comply with local data protection laws, such as the UK GDPR, the DPA and the DUAA in the UK, the EU GDPR, the Privacy Act 1988 in Australia, the Privacy Act 2020 and Privacy Amendment Act 2025 in New Zealand, the CCPA and Washington My Health My Data Act in the US and other applicable global privacy regulations.
6. **Compliance with Data Privacy Framework:**

   Kry10 Corporation and Kry10 Holdings complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. Kry10 Corporation and Kry10 Holdings has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF

Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/

7. **FTC enforcement**

   Kry10 Corporation is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC) with respect to its compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF.

8. **Liability for onward transfers**

   Kry10 Corporation is responsible for personal data it receives under the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and then transfers to a third party acting as its agent. Kry10 Corporation remains liable under the DPF Principles if that agent processes the data in a way that doesn't comply with the Principles, unless Kry10 Corporation proves it is not responsible for the event that caused the damage.

EU Representative

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Kry10 commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF in the context of the employment relationship.

As Kry10 processes the personal data of individuals of the European Union in our role as either "Data Controller" or "Data Processor" we have appointed DataRep as our EU representative in accordance with Article 27 of the EU GDPR. The EU representative acts on our behalf in relation to its obligations under the EU GDPR and is available to data subjects and supervisory authorities for any issues relating to the processing of personal data.

For more details on your rights, you can contact the National Data Protection Authority in your country or the European Commission *https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en*

If you want to raise a question to Kry10 or otherwise exercise your rights in respect of your personal data, you may do so by:

- Sending an email to DataRep at datarequest@datarep.com quoting Kry10 UK Ltd in the subject line
- Contacting us on our online webform at www.datarep.com/data-request or
- Mailing your inquiry to DataRep. Please contact us for a relevant address.

PLEASE NOTE: when mailing inquiries, it is ESSENTIAL you mark your letters for "DataRep" and not Kry10 UK Ltd or your inquiry may not reach DataRep. On receiving your correspondence, Kry10 will request evidence of your identity to ensure your personal data and information connected with it is not provided to anyone other than you.

If you have any concerns about how DataRep will handle your personal data, please refer to their privacy policy *www.datarep.com/privacy-policy*.

6. Disclosures of your personal data

We may share your personal data with third parties for the purposes set out in the table *Purposes for which we will use your personal data* above. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

7. Data security

Unfortunately, the transmission of information via the internet is not completely secure. Although we will take reasonable steps to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk.

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

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. Data retention

How long will you use my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting, or other requirements.

In some circumstances you can ask us to delete your data: see *your legal rights* below for further information.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

9. Use Of Artificial Intelligence (AI) Technologies

We use approved third-party AI technologies, operating under data processing agreements with model training disabled and data retention protections enabled, to help us triage, summarise, and

draft responses to your enquiries and correspondence. A member of our team reviews any AI-assisted response before it is sent. These providers act as our processors and do not use your information for their own purposes. The purposes for which AI technologies will be used include, but are not limited to:

- Data Analysis and Insights: AI tools will analyse data to provide insights that help us improve our services and tailor them to client needs.
- Security and Fraud Prevention: AI tools will be used to detect and prevent fraudulent activities, ensuring the safety and integrity of our systems.
- Personalisation: AI tools will assist in personalising client experiences by recommending content or services based on client preferences and behaviour.

We are committed to using AI responsibly and ethically. To this end, we implement reasonable and appropriate controls to manage the use of AI technologies, including rigorous validation procedures to mitigate and prevent inappropriate bias in AI outputs. These measures ensure that the results generated by AI are fair, accurate, and aligned with the purposes for which they are intended.

Safeguards for AI Use and Your Rights

Your personal data will only be processed using AI technologies in ways that are lawful, transparent, and consistent with the purposes outlined in this privacy policy. To protect your rights, we apply the following safeguards when using AI technologies:

1. **Human Oversight**: AI-driven processes that could result in decisions with legal or similarly significant effects are subject to meaningful human oversight to ensure fairness, accuracy, and accountability.
2. **Bias Prevention**: We continuously assess and address potential biases in AI algorithms and models to ensure that outputs are equitable and inclusive.
3. **Data Protection**: All data processed using AI is handled securely and in compliance with applicable data protection laws.
4. **Transparency**: We strive to provide clear information about how AI Technology is used, the purposes of its use, and the potential impacts on you.

Limitations of AI Use

We do not use AI technologies to make decisions that have a significant legal effect on you without your explicit consent or appropriate safeguards, such as ensuring human review. Additionally, AI technologies are not used for profiling that would infringe upon your rights or freedoms under applicable privacy laws.

10. Glossary

Consent means when you freely provide a specific, informed and unambiguous indication of your wishes through a written statement or clear affirmative action, inter alia, to being contacted by our marketing teams, or being asked to participate in a market research project which would be collected on our behalf by us or our third-party recruiters.

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do 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 can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Recognised Legitimate Interest means a specified purpose for handling personal data that is in the public interest and covers situations, such as crime prevention, public security, national security or defence, safeguarding, emergencies or sharing personal information to help other organisations perform their public tasks or official functions. Although there is no requirement for us to assess whether a person's rights, freedoms or interests outweigh the recognised legitimate interest, we must consider whether the activity we want to do is necessary.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

11. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- If you want us to establish the data's accuracy.
- Where our use of the data is unlawful, but you do not want us to erase it.
- Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
- You have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

12. Data Protection Complaints

Kry10 is committed to protecting the personal data of its workforce and that of its clients and take all complaints seriously.

If a data subject believes Kry10 has not handled their personal information in accordance with applicable privacy laws or Kry10's Privacy Policy, they have the right to make a complaint, and Kry10 will work to resolve it promptly.

Step 1: Contact Kry10 First

Data subjects must give Kry10 the opportunity to resolve their concern before escalating to a regulator.

To raise a privacy complaint, data subjects must contact the Privacy and Data Protection Lead. Details are provided below:

Email: privacy@kry10.com

Subject line: Privacy Complaint

It must include:

- Full name and contact details
- A full description of the complaint

If the data subject is based in the United Kingdom, they may also write to Kry10 at:

Kry10 Ltd Annecy Court, Ferry Works, Summer Road Thames Ditton, Surrey, England, KT7 0QJ

Kry10 will acknowledge the complaint within 5 business days and aim to provide a full response within 30 days. If the complaint is complex and requires more time, Kry10 will inform the data subject.

Step 2: If The Data Subject Is Not Satisfied

If the data subject is dissatisfied with Kry10's response, or if Kry10 has not resolved the complaint within 30 days, the data subject can escalate to the relevant regulator for their location.

If the data subject is based in the United Kingdom, they are required to lodge their complaint with Kry10 through one of the means described in Step 1 before escalating to the ICO. The ICO expects individuals to raise their concern with the organisation first.

Location	Regulator	Website
New Zealand	Office of the Privacy Commissioner	privacy.org.nz
Australia	Office of the Australian Information Commissioner (OAIC)	oaic.gov.au
United Kingdom	Information Commissioner's Office (ICO)	ico.org.uk
European Union	Your national data protection authority, being the Data Protection Commission (DPC)	edpb.europa.eu
United States	Federal Trade Commission (FTC)	ftc.gov

Step 3: EU and UK Individuals — Independent Dispute Resolution

If the data subject is located in the EU or UK and their complaint relates to personal data transferred to Kry10 Corporation in the United States under the EU-U.S. Data Privacy Framework or its UK Extension, they may also submit their complaint free of charge to Kry10's independent recourse mechanism:

JAMS jamsadr.com/DPF-Dispute-Resolution

If the data subject's complaint remains unresolved after this process, they may invoke binding arbitration under the Data Privacy Framework Annex I procedure at dataprivacyframework.gov/Arbitration.

13. Privacy Contacts

For privacy enquiries, requests, or complaints, please contact the Privacy and Data Protection Lead for the Kry10 Group:

Privacy Officer Email: privacy@kry10.com

If you wish to file your complaint by email, please use the details below per entity.

Kry10 NZ (New Zealand)

Privacy Officer Email: privacy@kry10.com
Address: PO Box 5180, Wellington, 6140

Kry10 Corporation (United States)

Privacy Officer Email: privacy@kry10.com
Address: 600 1st Ave Suite 102 #2481, Seattle, WA 98104

Kry10 Pty Ltd (Australia) Privacy Officer

Privacy Officer Email: privacy@kry10.com
Address: Level 3, 55 Pyrmont Bridge Road, Pyrmont NSW 2009, Australia

Kry10 Ltd (United Kingdom)

Privacy and Data Protection Lead Email: privacy@kry10.com
Address: Annecy Court, Ferry Works, Summer Road, Thames Ditton, Surrey, England, KT7 0QJ

EU Representative

DataRep Email: datarequest@datarep.com
Address: 77 Camden Street Lower, Dublin, D02 XE80, Ireland

14. Compliance Verification

Kry10 Corporation verifies its compliance with the DPF Principles through self-assessment conducted on an annual basis, in accordance with the DPF Supplemental Principle on Verification.

Each other Kry10 Group entity conducts periodic privacy compliance reviews consistent with its local regulatory obligations.

15. Changes to the privacy policy

We keep our privacy policy under regular review. This version was last updated on 16th October 2026.