PRIVACY POLICY

(last modified in May 2024)

INTRODUCTION

This is the Caristo Privacy Policy. The Caristo Group comprises two separate legal entities; a parent company **Caristo Diagnostics Limited**, which based in the UK, and **Caristo Diagnostics, Inc**., which is based in the USA.

This policy is issued on behalf of the Caristo Group, so when we mention "Caristo", "we", "us" or "our" in this privacy notice, we are referring to the relevant company in the Caristo Group responsible for processing your data.

We respect your privacy and value your trust. We are committed to being transparent about how we collect, store and manage your personal data, where we decide the purpose and means of the information processing (as a Controller) or we otherwise process it (as a Processor) under the authorisation of another organisation. This privacy notice will also tell you about your rights when it comes to your data. We are committed to protecting your personal data in accordance with the UK General Data Protection Regulation (**UK GDPR**). We are also subject to the EU General Data Protection Regulation 2016/679 (**EU GDPR**) in connection with personal data we collect about individuals who reside in the European Economic Area (**EEA**) and such other laws in other jurisdictions as may be applicable from time to time.

We may collect your personal data when you visit our website or if you contact us with regards our services. This Privacy Policy will explain how we may use the personal data you provide to us when using our website and when you use our services.

Please note that this Privacy Policy does not apply to any patient personal data which customers share with us in connection with their use of our services. That information is subject to the privacy policies of the customer. If you have questions concerning how these customers collect and use your personal data, including how we process personal data on behalf of such customers, please contact the customer directly.

PRIVACY

1. Who we are

Caristo Diagnostics Limited is a controller and responsible for your personal data. We are a private limited company incorporated and registered in England and Wales under company number 11429590 with its registered office at New Barclay House, 234 Botley Road, Oxford OX2 0HP. Caristo Diagnostics, Inc., is a Delaware corporation whose address is c/o CT Corporation of 1209 Orange Street, Wilmington, Delaware 19801, USA.

2. DPO

We have appointed a Data Protection Officer (**DPO**) who is responsible for overseeing questions in relation to this policy. If you have any questions about this policy, or the information we hold about you, including any requests to exercise your legal rights, or to make a complaint, you can contact us and/or our DPO by post (to the above address) or by email to *privacy@caristo.com*.

Individuals within the EEA can contact our European representative by email to *euprivacy@caristo.com*.

3. How to raise questions, complaints or exercise rights

If you have any concerns about how we are handling your personal data, please do get in touch with us, or our representative, and we will do our best to resolve the issue quickly, thoroughly and proactively. Please use the Contact Us Form on our website or send an email to privacy@caristo.com

If we have been unable to resolve the issue to your satisfaction, you also have the right to make a complaint at any time to a competent supervisory authority such as the Information Commissioner's Office (**ICO**), the UK supervisory authority for data protection issues. Their website is: www.ico.org.uk, and their helpline phone number is 0303 123 1113.

4. Changes to this policy and your duty to inform us of changes

We keep our Privacy Policy under regular review; and it was last updated in May 2024.

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.

5. Third-party links on our website

Our website may include links to third-party websites, plug-ins and applications, and from time to time to academic publications or medical organisations. Clicking on those links or enabling those connections may allow those third parties to collect or share data about you. We do not control these third-party websites, and so are not responsible for their use of any personal data you provide to them, or for the third party's privacy notices or practices. When you leave our website, we encourage you to read the privacy and cookie policies of every such website you choose to visit.

6. The type of 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 name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.
- **Contact Data** includes email address, telephone numbers and physical address.
- **Professional Data** includes details about your job role, qualifications and company address.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website, which may be through cookies (see Cookies Policy).
- **Usage Data** includes information about how you use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and your communication preferences.

If you provide us with personal data relating to another person, you agree that you have obtained their consent to the disclosure, and to our use of it in accordance with this Privacy Policy.

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy.

Personal Health Information and/or other Special Categories of Personal Data

We do not routinely collect any Special Categories of Personal Data about you through our interactions with you over our website, through email, telephone or in person. Special Categories of Personal Data include 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. Additionally, we do not collect any information about criminal convictions and offences.

7. How your personal data is collected

We use different methods to collect data from and about you, including through direct interactions. You may give us your Identity Data and Contact Data by filling in forms (including the Contact Us form on our website) or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- enquire about or request and/or engage in our services; and/or

- request marketing to be sent to you; and/or
- visit our offices or engage with us at conferences and events; and/or
- supply our business with products or services; and/or
- engage with us for career development and recruiting activities; and/or
- give us feedback or contact us through any means for example social media, or other enquiry routes.

8. How we use your personal data

We will only use your personal data when we are permitted by data protection laws to do so. Most commonly, we will use your personal data in the following circumstances:

- where you have provided your explicit consent;
- to perform a contract with you, or take steps to enter into a contract with you at your request;
- 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; and/or
- where we need to comply with a legal obligation.

Purposes for which we will use your personal data

The below table sets out a description of the main ways we plan to process your personal data, and the lawful grounds we rely on to do so. We have also identified what our legitimate interests are where appropriate.

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 would like further information.

Purpose/Activity	**Type of data**	**Lawful grounds for processing including basis of legitimate interest**
To register your interest in our products and services	Identity, Contact and Professional	Legitimate interests
To enter into contract and comply with our contractual obligations in managing our services with you.	Identity, Contact and Professional	Performance of contract or to take steps to enter into contract with you
To manage our relationship with you, such as notifying you about changes to our terms, services or Privacy Policy	Identity and Contact	Necessary to comply with a legal obligation Performance of contract Necessary for our legitimate interests (for managing notifications)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	Identity, Contact and Technical	Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) Necessary to comply with a legal obligation

Purpose/Activity	Type of data	Lawful grounds for processing including basis of legitimate interest
To deliver relevant website content to you	Identity, Contact, Usage, Marketing and Communications and Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To respond to contact made by you through, for example social media, website forms and other enquiry routes	Identity, Contact	Legitimate business interest
To give you secure access to our offices or to engage with you at and after conferences and events (personal identifiers, and contact details)	Identity, Contact	Legitimate business interest
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	Technical, Usage	Necessary for our legitimate interests (to define types of customers for our products and 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 goods or services that may be of interest to you	Identity, Contact, Technical, Usage, Marketing and Communications	Necessary for our legitimate interests (to develop our products/services and grow our business)
To collect your details for recruitment with a view to your joining us as an employee. When you engage with us for career development and recruiting activities	Your professional qualifications, educational background and your public life when you communicate with us through our website or email, for careers purposes, or have otherwise made publicly available. (personal identifiers, contact details, CV, screening results, references)	Legitimate business interest and performance of a contract
To liaise with you as regards your supplying our business with products or services.	Names, roles and contact details (telephone, email, address), as may be provided by you or your organisation for engagement with us for the purposes of supplying services to us.	Performance of a contract

Recruitment and Employment

For more information about our processing personal data with respect to recruitment, please refer to

our Candidate Privacy Notice on this website. If you are employed by Caristo please refer to our Internal Privacy Notice, which you can find on SciLife or from HR.

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We do not currently actively market to you, however we do have a Contact Us form on our website. In completing this form, or contacting us via our *info@caristo.com* email address or telephone number, you consent to our contacting you in order to provide you with more information on our company, as requested in your message. In order to contact you, we will process and store your email address, phone number and the content of your message in line with this policy.

As regards marketing, we may in future contact you from time to time with information about our products and services. Most messages we send will be by email. The Contact Us form on our website includes an opt-in box for you to choose whether to receive our marketing messages. You can change your preferences at a later date by clicking on the "unsubscribe" or "manage preferences" link at the bottom of our marketing messages. You can also let us know that you do not wish to receive further marketing communications at any time by sending an email to info@caristo.com.

Cookies and online tracking

Our website uses cookies to enable, optimise and analyse website operations. Please see our separate cookies policy for more information.

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 require an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at *privacy@caristo.com.*

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.

9. Disclosures of your personal data

We may share your personal data with any member of the Caristo group of companies from time to time for the purposes stated in this Policy.

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, including:

- **Service providers**: We rely on trusted third parties who assist us in managing our business and providing the website, such as providers of website analytics, de-identification services, network services, hosting and cloud computing services, marketing and other administrative services.
- **Advisors**: We work with various professional advisors, including tax consultants and legal advisors, with whom we may share your personal data.
- **Legal**: We may also disclose your personal data to law enforcement agencies, regulatory bodies, public authorities or pursuant to the exercise of legal proceedings if we are legally required to do so, or if we believe, in good faith, that such disclosure is necessary to comply with the law, enforce our polices, the Website Terms and Conditions, protect our or others' rights, property or safety or for the purposes of preventing or detecting and investigating an unlawful act.
- **Business transaction**: if we are involved in a merger, acquisition or asset sale, financing, reorganisation, bankruptcy, receivership, sale of company assets, or transition of service to another provider, your personal data may be sold, transferred or otherwise shared, including as part of any due diligence process.

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.

10. Where your personal data is held

Personal data may be held at our offices and those of our third party agencies, service providers, representatives and agents as described above (see above: '*Disclosures of your personal data*'). Some of these third parties may be based outside the UK/EEA. For more information, including on how we safeguard your personal data when this happens, see below '*Transferring your personal data out of the UK and EEA*'.

Transferring your personal data out of the UK and EEA

To deliver services to you, it is sometimes necessary for us to share your personal data outside the UK/EEA, e.g.:

- with your and our service providers located outside the UK/EEA; or
- if you are based outside the UK/EEA.

Under data protection law, we can only transfer your personal data to a country or international organisation outside the UK/EEA where:

- the UK government or, where the EU GDPR applies, the European Commission has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'adequacy decision' or an 'adequacy regulation');
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or
- a specific exception applies under data protection law. These are explained below.

Adequacy decision

We may transfer your personal data to certain countries, on the basis of an adequacy decision. These include:

- all European Union countries, plus Iceland, Liechtenstein and Norway (collectively known as the 'EEA');
- where the EU GDPR applies, all countries considered adequate by the European Commission, available at: Adequacy decisions (europa.eu);
- where the UK GDPR applies, all countries considered adequate by the UK Government, available at: International data transfers: building trust, delivering growth and firing up innovation - GOV.UK (www.gov.uk).

The list of countries that benefit from adequacy decisions and regulations will change from time to time. We will always seek to rely on an adequacy decision, where one exists.

Transfers with appropriate safeguards

Where there is no adequacy decision, we may transfer your personal data to another country or international organisation if we are satisfied the transfer complies with data protection law, appropriate safeguards are in place, and enforceable rights and effective legal remedies are available for data subjects.

The safeguards will usually include using legally-approved standard data protection contract clauses.

To obtain a copy of the standard data protection contract clauses and further information about relevant safeguards please contact us at *privacy@caristo.com*.

Transfers under an exception

In the absence of an adequacy decision or appropriate safeguards, we may transfer personal data to a third country or international organisation where an exception applies under relevant data protection law, e.g.:

- you have explicitly consented to the proposed transfer after having been informed of the possible risks;
- the transfer is necessary for the performance of a contract between us or to take pre-contract measures at your request;
- the transfer is necessary for a contract in your interests, between us and another person; or
- the transfer is necessary to establish, exercise or defend legal claims.

We may also transfer information for the purpose of our compelling legitimate interests, so long as those interests are not overridden by your interests, rights and freedoms. Specific conditions apply to such transfers and we will provide relevant information if and when we seek to transfer your personal data on this ground.

If you would like further information about data transferred outside the UK/EEA, please contact us at *privacy@caristo.com*.

11. Data Security

Caristo is ISO/IEC 27001:2013 certified; which is indicative of our commitment to implement reasonable and appropriate technical and organisational measures to securely protect the personal information we process against accidental or unlawful destruction, loss, unauthorised access, change, damage or disclosure.

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 it. They will only process your personal data on our instructions and if they are subject to a duty of 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.

12. Data Retention

How long will you use my personal data for?

We will only retain your personal data for (a) 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 or (b) as long as we have contractually agreed to hold it. 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.

13. Your legal rights

You have the right to:

a) **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.

b) **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.

c) **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 at the time of your request.

d) **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.

e) **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 because 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.

f) **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.

g) **Withdraw consent** at any time where we are relying on consent to process your personal data. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact us at *privacy@caristo.com*. 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.

14. 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.

15. 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.