Biofidelity

Biofidelity Privacy Notice

This document is provided in a **layered format**, using the headings set out below. If you are reading this online, please click on the numbers to be referred to the relevant section.

Contents

1. Introduction

We take your privacy very seriously. Please read this Privacy Notice (sometimes called a “Privacy Policy”) and any other fair processing notice we may provide on specific occasions carefully, as it is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export and delete your personal information.

This Privacy Notice has been drafted to be applied to personal information processing activities globally. The processing activities may be more limited in some jurisdictions due to the restrictions of their laws. For example, the laws of a particular country may limit the types of personal information we can collect or the manner in which we process that personal information. In those instances, we may adjust our internal policies and/or practices to adapt to the requirements of local law.

This Notice supplements our other policies and notices and is not intended to override them.

2. Who we are

We are Biofidelity Ltd a company that transforms human health and the world we live in by developing innovative technologies that unleash the potential of genomics (hereafter referred to as “Biofidelity”, “we”, “us” or “our”).

Biofidelity acts as the data controller for the personal information described in this Privacy Notice. We determine the purposes and means of processing your personal information in compliance with applicable data protection laws, including the GDPR. For any questions or concerns about how we handle your personal information, please contact us at privacy@biofidelity.com.

3. How to contact us

You can contact us at:

Email: privacy@biofidelity.com

Address: Biofidelity Ltd.
330 Cambridge Science Park
Milton Road
Cambridge
England
CB4 0WN

When you contact us via a fill-in form, any information you choose to disclose is sent directly to us to assist us in better answering your request.

4. Data protection officer (DPO)

We have appointed GRCI Law Limited as our DPO, who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, our privacy practices or how we handle your personal data, you can contact our DPO at dpoaas@grcilaw.com.

5. What is meant by personal information or personal data

Personal information (also called personal data) is information which identifies you as an individual.

Some examples are outlined below:

- Personal data is anything which may identify you for example your name, address, bank account details, internet protocol (IP) address, username or another identifier.

Some personal data is unique to you and therefore requires greater protection. This data is referred to as sensitive or special category data which includes information regarding your health, religious or philosophical beliefs, race, or ethnicity to provide a few examples.

6. What personal information we collect

We may collect, use, store and/or transfer different kinds of personal information about you depending on our relationship with you and the jurisdiction in which you live. Personal information we collect includes:

- **Identity Data** includes first name, last name, username or similar identifier, marital status, title, date of birth, gender,
- **Employment Data:** employer, organization and job title, billing address, work email address
- **Contact Data** includes billing address, address, email address and telephone numbers, email address, mailing address and telephone number and any other identifier by which you may be contacted online or offline.
- **Job Application Data** includes C.V application materials and answers to any questionnaires.
- **Transaction Data:** includes details about payments and other details of products and services bought from us.
- **Technical Data:** includes internet protocol (IP) address, 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 used to access our website.
- **Clickstream data:** is a virtual breadcrumb trail that a user leaves behind while browsing. We may record paths you have taken (e.g. sections or stories clicked and the order in which it is done) and use this information to provide customized content.
- **Profile Data:** includes username and password, purchases or orders made, interests, preferences, feedback, Information that you provide by filling in forms on our Site. and survey responses.: This includes information provided at the time of registering to use our Site (when subscribing to a service, posting material. or requesting further service).,

- **Images and personal appearance:** include copies of passports or drivers' licences.
- **Usage Data:** includes information about how individuals use our website, your search queries on the Site and online activity based on their interaction with us, our websites and applications for example searches, site visits, browsing actions and patterns.
- **Communications Data**: includes Records and copies of your correspondence (including email addresses), if you contact us; when you report a problem with our Site and any other types of information you provide when communicating with us.
- **Surveys and Promotions:** Information and responses when you complete a survey or enter a contest or promotion sponsored by us,
- **Marketing Data:** includes preferences in receiving marketing from us and our third parties and communication preferences.
- **Publicly Available Data:** includes identity and contact data from publicly available data sources such as Companies House and LinkedIn.

7. Sensitive and special category data

In connection with our operations, including recruitment, we may collect and process sensitive or special category personal data, as defined under applicable data protection laws, including the UK GDPR, EU GDPR, and relevant U.S. privacy laws. This data may include:

- Information about your race, ethnicity, or nationality, religious beliefs, and/or sexual orientation.
- Information about your health, including medical conditions, disabilities, and health or sickness records.
- Information about criminal convictions and offenses where required by law, such as for certain roles where background checks are appropriate and legally permitted.

We will only process such data where:

- It is necessary to fulfill our legal obligations (e.g., compliance with employment or health and safety laws).
- You have provided your explicit consent (e.g., for voluntary diversity monitoring or trial participation).

For recruitment purposes, information about criminal convictions will only be collected where appropriate for the nature of the role and where we are legally permitted to do so. This may include information provided by you or obtained through lawful background checks. Such processing is conducted in connection with our obligations under employment laws or other legal requirements.

We have implemented appropriate policies and safeguards, as required by law, to ensure the secure and lawful processing of sensitive and special category data. For more information on these safeguards, or to request further details about how we handle this type of data, please contact us using the details provided in this Privacy Notice.

8. How we collect your personal data

In order for us to operate effectively, we may request and collect information about you, the data we collect depends on the context of your interactions with us and the choices that you make, including your privacy settings and the features that you use.

We collect personal data from you:

8.1. Directly:

Most of the personal data that we collect about you will be information that you provide to us directly:

- when you fill in forms or correspond with us by post, phone, email or otherwise.
- when you subscribe to our publications
- when you take part in discussion boards or other forms of social media
- when you are a user of our products and associated product software

8.2. Indirectly:

We collect information through your behaviour and interactions with us:

- when you interact with our website, we may 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
- information we learn about you through our relationship and the way you interact with us

In some circumstances we may also receive information from:

- regulatory bodies

- other companies supplying services to us
- data analytics to improve our website, products/services, marketing, customer relationships and experiences
- publicly accessible social media networks such as Facebook, Instagram, LinkedIn, Google, and Twitter
- providers of technical, payment and delivery services
- publicly available sources such as Companies House and LinkedIn

Click here for more information about our use of cookies and how to disable them.

9. Children

Our Site is not directed to children under the age of 16, and we do not knowingly collect or process personal data from children. If we become aware that we have inadvertently collected personal information from a child without appropriate parental or guardian consent, we will take steps to delete the information as soon as possible. If you believe we may have inadvertently collected data from a child, please contact us at privacy@biofidelty.com.

10. Data accuracy

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

11. Why we use your personal data

We need your personal information to conduct our business and provide you with our Site and Products. Most commonly we will use your personal information in the following circumstances:

- It's necessary to provide our services, fulfil a transaction or otherwise perform a contract with you or at your request prior to entering into a contract.
- It's necessary to contact individuals regarding updates, and support.
- It is in our legitimate interest to use personal information in such a way to ensure that we provide our services in the best way that we can, protect the security of our systems, website users and detect or prevent fraud, wherever we process your personal data for these purposes, we ensure that your interests, rights and freedoms are carefully considered
- It is our legal obligation to use your personal information to comply with any legal obligations imposed upon us

Please contact us if you have any questions about how we use your personal data.

- **EEA and UK residents:** For more information about our basis for processing your personal data see: "*Additional Information for EU and UK Residents"*

12. Your rights

We will only collect, process and/or use personal information where we are satisfied that we have an appropriate legal basis to do so. Depending on your location and applicable data protection laws, you may have certain rights regarding your personal data. These rights may include the right to access, correct, update, or delete your data; the right to restrict or object to certain types of processing; the right to data portability; and the right to withdraw your consent where processing is based on consent. You may also have the right to lodge a complaint with a supervisory authority.

To exercise your rights or for more information, please contact us at privacy@biofidelity.com. We will review and respond to your request in accordance with applicable data protection laws.

Please note that we may need to verify your identity before processing certain requests.

- ***EEA and UK residents***: For more information about your rights see: "*Additional Information for EU and UK Residents"*
- ***US State residents***: For more information about your rights see: "*Supplemental Information for U.S. Residents"*

13. Unsubscribe and opting out

You have the right to opt out of receiving future communications from us at any time. To unsubscribe from email communications, l or update your subscription preferences please contact us at privacy@biofidelity.com. Please note that it may take up to 7 days for your request to be fully processed.

If you wish to opt out of other forms of communication or have any issues with unsubscribing, you can contact us directly using the email address, as above, or phone number provided on our website. We will process your request promptly in accordance with applicable data protection laws, including the UK GDPR, the EU GDPR, and relevant U.S. privacy laws such as the CAN-SPAM Act and CCPA, where applicable.

Please note that opting out of marketing communications does not affect transactional or service-related communications necessary for the performance of a contract or other legitimate purposes.

14. How long we hold your personal data

We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected, as outlined in this Privacy Notice, or to comply with applicable legal, regulatory, or contractual obligations. Retention periods vary depending on the nature of the data, the context of the processing, and jurisdictional requirements. For example, personal data may be retained longer where required by laws in the United States (e.g., tax or employment laws) or the United Kingdom (e.g., data protection and employment regulations). Once retention periods have elapsed, we securely delete, anonymise, or archive personal data in accordance with applicable data protection laws, including GDPR and UK GDPR, as well as U.S. state-specific privacy laws such as the California Consumer Privacy Act (CCPA). If you require further details on specific retention periods, please contact us using the information provided below.

15. Who do we share your personal data with?

We may occasionally share your personal data with the following types of organisations, ensuring that they maintain confidentiality, safety, and security in accordance with applicable data protection laws:

1. **Potential Employers** as part of a job application or recruitment process.
2. **Service Providers**, including those offering IT, system administration, and software services.
3. **Payment Service Providers**, for processing transactions.
4. **Third Parties Involved in Our Services**, such as webinar hosts
5. **Marketing Use**: If you provide a testimonial or commentary about our company, services, or partners, we may use these in our marketing materials both on and off our site.
6. **Analytics Providers**, such as Google Analytics, to assist us with insight analytics.
7. **Suppliers and Administrative Support**: Third parties, employees, agents, subcontractors, and professionals who provide products, services, and administrative support to us.
8. **Regulatory and Legal Authorities**, such as law enforcement agencies, judicial bodies, tax authorities, or other government and regulatory entities, where required by law.
9. **Business Transactions**: As part of a proposed sale, reorganisation, transfer, financial arrangement, asset disposal, or similar transaction related to our business or assets.
10. **Other Parties with Your Permission**: We may share data with other third parties explicitly authorised by you.

This list is non-exhaustive, and there may be other situations where we need to share your personal data to effectively provide our services.

We only share your personal data with organisations that implement appropriate measures to protect your information. Contractual obligations are imposed on these organisations to ensure they use your data solely for the services they provide to us or to you.

We will not share your personal data with any other third party without your explicit consent, unless required or permitted by law. The specific information shared will depend on your interactions with us and will always be limited to what is necessary for the intended purpose.

Third-Party Providers

Please note, this Privacy Notice does not apply to personal data collected directly by third-party providers who may share information with us. We strongly encourage you to review the privacy policies of any third-party providers before submitting your personal data to them.

16. Do we transfer personal data overseas?

We operate globally, and certain aspects of our information processing and data storage may be centralised in countries outside your own. As a result, we may need to share and transfer your personal information across multiple jurisdictions, including the UK, USA, and countries within the European Economic Area (EEA). These jurisdictions may have data protection laws that differ from those in the country where your personal information was collected or your country of residence.

To safeguard your personal information, we ensure that all international transfers comply with applicable data protection laws, including the UK GDPR, EU GDPR, and relevant U.S. privacy regulations. We undertake thorough due diligence and risk assessments before any data transfer, ensuring your information has an appropriate level of protection. Where required, we implement legal safeguards such as Standard Contractual Clauses (SCCs) or other approved mechanisms to ensure your data is handled securely and lawfully.

For further details about the measures we use to protect your personal information when it is transferred internationally, please contact us at privacy@biofidelity.com.

17. Third-party links

Our website may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

18. How to withdraw consent

You can 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 supply certain products or services to you. We will tell you if this is the case at the time you withdraw your consent. If you wish to withdraw your consent, please contact us at privacy@biofidelity.com.

For more information on Consent in US states see: "*Consent Requirements Regarding Targeted Advertising, Sale of Personal Information, and Sensitive Data Processing*"

19. Do we use automated decision-making or profiling?

We do not use automated decision-making or profiling.

20. How we keep your personal data secure

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.

21. How to make a complaint

If you have any concerns about our handling of your personal information or believe your privacy rights have been infringed, you have the right to make a complaint. We are committed to resolving privacy-related complaints promptly and effectively.

We encourage you to contact us directly at privacy@biofidelity.com so that we can address any issues promptly. However, if you are not satisfied with our response, you

may also have the right to file a complaint directly with your local privacy regulator. We have provided some contact details for your reference below:

- **United Kingdom**: You can file a complaint with the Information Commissioner's Office (ICO) via www.ico.org.uk.
- **European Economic Area (EEA)**: If you are located in the EEA, you can reach out to your local data protection authority. A list of EEA data protection authorities can be found here.
- **United States**: You may also reach out to the consumer protection agency in your state or contact the Federal Trade Commission (FTC) for general privacy concerns via www.ftc.gov.
- **California Consumer Privacy Act (CCPA)**:
  Complaints can be directed to the **California Attorney General's Office** or, under the new California Privacy Rights Act (CPRA), to the **California Privacy Protection Agency (CPPA)**. **Website**: https://oag.ca.gov/privacy/ccpa
- **Colorado, Connecticut, Virginia, and Other States**:
  States with privacy laws (e.g., Colorado Privacy Act, Virginia Consumer Data Protection Act) direct complaints to their respective Attorneys General.
  Check the specific Attorney General's website for complaint procedures. You can find the contact information for each Attorney General's office through the National Association of Attorneys General (NAAG) directory: Find my AG - National Association of Attorneys General
- **Canada**: If you have concerns regarding our data practices in Canada, you may file a complaint with the Office of the Privacy Commissioner of Canada (OPC) via www.priv.gc.ca.
- **Australia**: For data privacy inquiries in Australia, you may reach out to the Office of the Australian Information Commissioner (OAIC) via www.oaic.gov.au.
- **New Zealand**: Contact the Office of the Privacy Commissioner New Zealand via www.privacy.org.nz.
- **Hong Kong**: If you are in Hong Kong, you may contact the Office of the Privacy Commissioner for Personal Data (PCPD) via www.pcpd.org.hk.

22. Non-Discrimination

We will not discriminate against individuals for exercising any of their privacy rights. We provide the same level of service and pricing to all users, regardless of privacy preferences, except where allowed by law.

23. Policy changes and updates

We may update this Policy and Terms of Use periodically to reflect changes in our practices or law. Your continued use of this Site after we make changes is deemed to be

acceptance of those changes, so please review this Policy regularly. Your continued use of the Site will indicate your acceptance of the revised terms.

24. Supplemental information for U.S. residents

This section applies to individuals residing in the United States, with specific provisions for residents of states with enacted privacy laws. This notice outlines how we process personal information, including our practices related to consent, and the rights granted to residents under various state laws, including California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New York, Nevada, Oregon, Rhode Island, Tennessee, Texas, Utah, Vermont, and Virginia.

24.1 US residents rights

Us Residents in certain states have specific rights regarding their personal information. These rights vary depending on the state, as indicated below.

- **Right to Know**: The right to request information on the categories and specific pieces of personal information we have collected, used, disclosed, or shared, as well as the sources, purposes, and third parties involved.
  (California, Colorado, Connecticut, Iowa, Utah, Virginia)
- **Right to Access**: The right to access copies of personal information held by us.
  (California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New York, Nevada, Oregon, Rhode Island, Tennessee, Texas, Utah, Vermont, Virginia)
- **Right to Correct**: The right to request corrections to inaccurate personal information.
  (California, Colorado, Connecticut, Iowa, Utah, Virginia)
- **Right to Delete**: The right to request deletion of personal information, subject to legal limitations and exceptions.
  (California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New York, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia)
- **Right to Opt-Out of Sale or Sharing**: The right to opt-out of the sale or sharing of personal information for purposes such as targeted advertising or profiling.
  (California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, Vermont, Virginia)
- **Right to Limit Use of Sensitive Personal Information**: California residents have the additional right to limit the use and disclosure of their sensitive personal information to purposes specified under the CPRA.
  (California)

- **Universal Opt-Out Mechanism**: The right to use a universal opt-out mechanism to signal privacy preferences across platforms (where applicable). *(California, Colorado, Connecticut, Iowa)*

24.2 Consent requirements regarding targeted advertising, sale of personal information, and sensitive data processing

In accordance with various state privacy laws, we provide consumers with the right to opt out of the use of their personal information for targeted advertising or its sale to third parties. While these laws do not always require upfront consent, they ensure that consumers have control over how their data is used for these purposes. Additionally, certain states require explicit consent to process "sensitive" personal information, which may include data such as race, ethnicity, health information, biometric data, and, in some cases, precise geolocation. We are committed to respecting these rights, providing options to manage the use of your personal information, and ensuring that your sensitive data is only processed in compliance with applicable legal requirements.

24.3 Shine the light law and similar requirements

Under California's *Shine the Light* law (California Civil Code Section § 1798.83), California residents are entitled to request and receive information regarding certain types of personal information that we share with third parties for their direct marketing purposes.

In addition to California, the following states have similar, though narrower, laws concerning data transparency or opt-out rights:

- **Nevada**: Nevada law allows residents to opt-out of the sale of their personal information to third parties. While this law does not require detailed disclosures about data sharing for direct marketing, Nevada residents may request that we refrain from selling their personal data. For opt-out requests, please contact us at [Privacy Contact Email].
- **Vermont**: Vermont's law requires data brokers to disclose certain data-sharing practices and allows residents to opt-out of the sale of personal information if their data is collected by a data broker. Vermont residents may contact us for more details on our data-sharing practices.

To make a *Shine the Light* request or exercise similar rights under Nevada or Vermont law, please:

- Contact us at privacy@biofidelity.com including "Shine the Light Request" or "Data Sharing Request" in your subject line, or

Please specify the nature of your request (e.g., *Shine the Light*, Nevada Opt-Out, or Vermont Disclosure Request) and include sufficient details in your request to help us identify your records. We will process and respond to your request within the required timeframes.

Please note that we may require additional information to verify your identity before processing certain requests. Once verified, we will respond within the timeframe specified by the relevant state law.

25. Supplemental information for Canadian residents

This section applies to residents of Canada and addresses federal and provincial privacy requirements, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws. This is part of our commitment to protect personal information and ensure transparency about how we process it.

25.1. Scope of this privacy section

This section applies to personal information collected, used, and disclosed by us in the course of commercial activities and to fulfil obligations under applicable Canadian privacy laws, including:

- **PIPEDA** (Federal) – Applies across Canada, except where provincial privacy laws supersede it.
- **Provincial Privacy Laws** – Include British Columbia's Personal Information Protection Act (BC PIPA), Alberta's Personal Information Protection Act (AB PIPA), and Quebec's Act Respecting the Protection of Personal Information in the Private Sector (ARPPIPS, also known as Quebec's Law 25).
- **Provincial Health Privacy Laws** – In some provinces, specific laws govern health information.

25.2. Consent and lawful basis for processing

We rely on consent and other lawful bases for processing personal information, as required by Canadian privacy laws.

- **Express or Implied Consent**: Where required, we obtain your express or implied consent to collect, use, or disclose your personal information. Consent may be implied for purposes that are obvious or necessary to fulfil your request.
- **Exceptions to Consent**: In certain cases, we may collect, use, or disclose personal information without consent if required or authorized by law (e.g., for fraud prevention, security, or legal compliance).

Important note for Quebec residents: Under Quebec's ARPPIPS, as amended by Law 25, explicit consent is required for processing "sensitive" information, including health data. In some cases, written consent may be required.

25.3. Rights of Canadian residents

Canadian residents have specific privacy rights under federal and provincial laws, which may vary slightly by province.

1. **Right to Access**
   You have the right to request access to your personal information, including details on how it has been used or disclosed.
2. **Right to Correct**
   You may request corrections to your personal information if it is inaccurate or incomplete.
3. **Right to Withdraw Consent**
   You may withdraw consent for the collection, use, or disclosure of your personal information, subject to legal or contractual restrictions.
4. **Right to Complain**
   If you believe your privacy rights have been violated, you may file a complaint with the relevant privacy commissioner's office:

   - Office of the Privacy Commissioner of Canada (PIPEDA): For individuals - Office of the Privacy Commissioner of Canada
   - British Columbia Privacy Commissioner (BC PIPA): How do I make a complaint? - Office of the Information and Privacy Commissioner for BC
   - Alberta Privacy Commissioner (AB PIPA): https://oipc.ab.ca/
   - Quebec Commission d'accès à l'information (CAI): Commission d'accès à l'information du Québec

5. **Right to Data Portability (Quebec)**
   Quebec residents have the right to request that their personal information be transferred to another organization in a structured, commonly used, and machine-readable format, subject to certain conditions under Law 25.

We will respond to your request within the timeframe required by the applicable federal or provincial privacy law.

26. Additional information for EU and UK residents

We are subject to the UK General Data Protection Regulation (UK GDPR) and the EU General Data Protection Regulation (EU GDPR) in relation to goods and services we offer to individuals and our wider operations in the UK and European Economic Area (EEA).

26.1 Further details about our processing

The table below describes the ways we plan to use your Personal Data, and which Lawful Basis we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Purpose	Type of Information Collected	Lawful Basis	Explanation of Legitimate Interests
To provide our services: Manage accounts, fulfil transactions, or perform a contract with you or at your request	Identity Data, Contact Data, Transaction Data, Profile Data, Technical Data	Performance of a contract	N/A
Service updates and support: Contact individuals regarding services, updates, and customer support	Contact Data, Communications Data, Profile Data	Legitimate interests (communication and support)	Necessary to maintain communication and provide assistance to users and clients, ensuring efficient and responsive service to fulfil expectations.
Recruitment and job applications: Process applications, schedule interviews, and assess suitability for roles	Identity Data, Contact Data, Employment History, Qualifications, References	Legitimate interests (recruitment)	Necessary to assess and manage job applications and recruit suitable candidates for organisational needs.
Recruitment and job applications: Collect and process sensitive data related to diversity, health, or criminal background checks	Race, Ethnicity, Religion, Sexual Orientation, Health Data, Criminal Convictions	Compliance with a legal obligation	Necessary to comply with applicable laws for certain roles or voluntary diversity monitoring. Safeguards are in place to ensure secure and lawful processing.
Recruitment and job applications: Collect and process sensitive data for voluntary diversity monitoring	Race, Ethnicity, Religion, Sexual Orientation	Consent	Explicit consent is obtained for voluntary participation in diversity monitoring initiatives.
Manage health and safety: Ensure the wellbeing of employees, visitors, and trial participants	Identity Data, Health Data, Emergency Contact Details	Legitimate interests (safety management)	Necessary to maintain a safe environment and respond effectively to emergencies.
Cookies: Collect and analyse information about website usage to improve user experience and functionality	Technical Data, Usage Data	Consent	Consent is obtained where required by law for non-essential cookies.
Cookies: Collect and analyse information about website usage to improve user experience and functionality	Technical Data, Usage Data	Legitimate interests (website analytics)	Necessary to analyse website performance, improve user experience, and maintain functionality.

Purpose	Type of Information Collected	Lawful Basis	Explanation of Legitimate Interests
Data Transfers: Transfer personal data across jurisdictions to support global operations and services	Identity Data, Contact Data, Technical Data	Legitimate interests (global operations)	Necessary to facilitate global operations and comply with applicable international transfer mechanisms, including Standard Contractual Clauses or other approved safeguards.
Data Transfers: Transfer personal data across jurisdictions to support global operations and services	Identity Data, Contact Data, Technical Data,	Compliance with a legal obligation	Ensures compliance with applicable legal frameworks governing international transfers.
Complaints and queries: Respond to and manage complaints, queries, or feedback	Identity Data, Contact Data, Communications Data, Profile Data	Legitimate interests (customer service)	Provides effective and timely resolution of complaints and queries to improve customer experience, ensure service satisfaction, and maintain customer trust.
Communications through website: Facilitate communication via website contact forms, live chat, or other channels	Identity Data, Contact Data, Communications Data	Legitimate interests (communication)	Necessary to enable users to reach out for support, inquiries, or feedback and to ensure efficient communication and problem resolution.
Marketing: Provide promotional information about services and updates (general marketing)	Contact Data, Marketing Preferences	Consent	Necessary to promote services to clients or users who have provided explicit consent, ensuring compliance with GDPR, UK GDPR, and U.S. privacy laws.
Marketing: Promote services and updates to existing customers or users in a similar context	Contact Data, Marketing Preferences	Legitimate interests (marketing)	Necessary to promote services to existing customers or users who have a reasonable expectation of receiving such communications (e.g., soft opt-in).
Marketing effectiveness: Measure and analyse advertising impact and effectiveness	Marketing Data, Technical Data, Clickstream Data, Usage Data, Publicly Available Data	Legitimate interests (advertising optimisation)	Enables analysis of marketing and advertising efforts to improve effectiveness and tailor offerings for optimal customer engagement, based on relevant user interactions.

26.2 Your rights

Please see more details about your rights in the table below. In most circumstances, you do not need to pay any charge for exercising your rights. We have one month to respond to you.

Access –the right to request a copy of the personal data we hold on you. In most cases, this will be free of charge, however in some limited circumstances, for example, repeated requests for further copies, we may apply an administration fee.

Rectification of personal data – this right 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.

Erasure of personal data – You can ask us to delete or remove your personal information in some circumstances such as where there is no good reason for us continuing to process it. We may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, job applicants who submit their personal info through the job application portal may also need to contact the potential Employer to have this data deleted or requested.

Restriction of processing personal data – this enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) 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; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Objection to processing of personal data – you can ask us to stop processing your personal information, and we will do so, if we are relying on legitimate interests to process your personal information, except if we can show compelling legal grounds for the processing; or if we are processing your personal information for direct marketing purposes.

Automated decision making – you have the right to ask for a decision to be made manually, where a decision is made using automated means and this harmfully affects you.

Portability – you have the right to have personal data we hold about you transferred securely to another service provider in electronic form.

In most circumstances you do not need to pay any charge for exercising your rights. We have 1 month to respond to you.

26.3 Our EU representative

We have appointed GRCI Law to act as our EU Representative. If you wish to exercise your rights under the EU General Data Protection Regulation (GDPR) or have any queries in relation to your rights or privacy matters generally please email eurep@grcilaw.com or post your request or query to Head of Data Privacy Manager Service, GRCI Law Limited, IT Governance Europe, Third Floor, The Boyne Tower, Bull Ring, Lagavooren, Drogheda, Co. Louth, A92 F682.

When contacting our Representative please ensure you include our company name in any correspondence.

26.4 Our UK representative

We have appointed GRCI Law Limited to act as our UK Representative. If you wish to exercise your rights under the UK General Data Protection Regulation (GDPR), or have any queries in relation to your rights or privacy matters generally please email our Representative at ukrep@grcilaw.com or post your request or query to UK Representative, Unit 3, Clive Court, Bartholomew's Walk, Cambridgeshire Business Park, Ely, Cambridgeshire, CB7 4EA, UK

When contacting our Representative please ensure you include our company name in any correspondence.