

Birkman International, Inc. Global Privacy Notice

Your privacy is important to us. Please read this Privacy Notice (“**Policy**”) and any other privacy notice or fair processing notice Birkman International, Inc. (“**BIRKMAN**”, “**we**” and “**us**”) 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 information.

This Notice has been drafted as 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 Data we can collect or the manner in which we process that Personal Data. In those instances, we may adjust our internal policies and/or practices to adapt to the requirements of local law.

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

This Notice is layered, so you can easily find to the information you want. [Please click on the headings or subheadings to read the full text.](#)

Contents

1.	Notice Scope	2
2.	Privacy Law and Principles	2
3.	Additional and supplementary privacy notices	3
4.	Who we are	3
5.	How to contact us.....	3
6.	What is Personal Data?	3
7.	What types of Personal Data do we collect?.....	4
7.1	Respondents	4
7.2	Customers	4
7.3	Other	4
8.	What is Sensitive or Special Category Data	5
9.	Do you collect sensitive Personal Data?	5
10.	How do we collect your Personal Data?	5
10.1	From you directly	5
10.2	Information Collected through Technical means	6
10.4	Information we receive from public sources	6
11.	How and on what basis do we use your Personal Data?.....	7
12.	Selling Personal Data.....	7
13.	With whom do we share your Personal Data?	7
14.	Do you have a choice about the data we collect and use about you?	8
15.	Children’s Privacy	8

16.	How do we protect your Personal Data?.....	9
17.	Transferring your information overseas	9
18.	Keeping your Personal Data current.....	10
19.	How long do we keep your Personal Data?	10
20.	Data Subject Rights	10
21.	Withdrawing Consent.....	11
22.	Changes to Our Privacy Notice	11
23.	Data Privacy Framework.....	11
24.	Your Rights under the Data Privacy Framework.....	11
25.	Dispute Resolution	12
26.	Do Not Track	12
27.	Contact and Complaints.....	12
28.	Birkman Website Servers.....	13
29.	Additional Information for Residents of the European Economic Area (the “EEA”) Switzerland and the United Kingdom (the “UK”)	13
30.	Additional Information for Residents of California	18
31.	Additional Information about State Privacy Rights	19

1. Notice Scope

This Notice applies to ways in which we interact with individuals, which we referred to herein as “**Data Subjects**”, in connection with our business, including, without limitation:

- visitors to our websites located at <https://birkman.com>, <https://direct.birkman.com>, <https://q.birkman.com>, and <https://app.birkman.com>;(the “**Websites**”);
- Data Subjects we communicate with In email, text, SMS messages, and other electronic messages;
- Data Subjects who access our interfaces or that use any of our Platforms and users of any digital services we provide;
- Data Subjects who interact with social media platforms connected to our Platforms;
- individual representatives of third-party sellers, placement agents, finders, investment bankers, consultants, lawyers, accountants, advisers and other service providers, whether or not engaged by BIRKMAN;
- directors, officers, employees and other representatives of BIRKMAN;

We may provide you, as required, with a supplementary country specific privacy notice when required by local privacy law.

2. Privacy Law and Principles

We always strive to:

- process Personal Data lawfully, fairly and in a transparent way.
- obtain Personal Data only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

- collect Personal Data relevant to the purposes we have told you about and limited only to those purposes.
- take reasonable steps to ensure that Personal Data is accurate and kept up to date.
- subject to applicable legal or other requirements, keep Personal Data only as long as necessary.
- use appropriate technical and/or organizational measures to ensure appropriate security of the Personal Data.

Please see the following sections for more information about specific jurisdictions:

- [Further information for EEA, Swiss and UK residents](#)
- [Further information for California Residents](#)

Please note that Birkman is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

3. Additional and supplementary privacy notices

Employees

We provide our former or existing employees with supplementary privacy notices where we are required to do so and dependent on the employees' geographies and jurisdictions.

General

We may provide additional privacy notices for certain entities within BIRKMAN, and certain geographies and jurisdictions.

4. Who we are

Birkman is an organizational performance company helping organizations better understand interpersonal dynamics and achieve higher performance through positive psychology and is the controller of the Personal Data to which this Privacy Notice relates.

5. How to contact us

If you have any questions, concerns, or complaints about this Privacy Notice, or our privacy practices in general, please contact us as follows:

Name: Birkman International, Inc. Privacy Team

By email: privacy@birkman.com

By mail: Attn: Privacy
575 N. Dairy Ashford Rd, Ste 600
Houston, TX 77079

By telephone: (713) 623-2760

Toll Free Number: 800-215-2760

6. What is Personal Data?

Personal Data. When we use the term “**Personal Data**” we mean information (also known as “personal information” or “personally identifiable information”) that reasonably can be used to identify you as an individual person.

7. What types of Personal Data do we collect?

The personal information that we collect depends on the context of your interactions with us and the websites, the choices you make and your relationship with us and may include the following types of Personal Data:

7.1 Respondents

Data Subjects that are Respondents (anyone who completes The Birkman Method questionnaire) may include:

- **Identification Data:** first and last name, gender, year born, Languages
- **Contact Data:** email address,
- **Behaviour Data:** self-reported behavioral attitudes in the context of the workplace
- **Location Data:** country, zip/postal code,
- **Education:** education information,
- **Employment Data:** employment status and employment details (job title, years worked, organization size, employer name, full- or part-time, seeking, not seeking, not able to work, retired). the purpose for taking the assessment,
- language, ethnicity

7.2 Customers

Our customers can be individuals or companies which may provide Personal Data on its employees. We may collect the following Personal Data from individuals or individual company contacts:

- **Identification Data:** full name, gender, year born, age, Birkman account ID numbers, Languages
- **Contact Data:** email address, mailing addresses (city, state, zip, country), email addresses, phone numbers, work address
- **Location Data:** country, zip/postal code, IP address, telephone codes, address, work address
- **Employment Data:** referral name, company name, employment status, detailed employment information (position title, dates hired, etc.), learning management system (LMS) training history,
- **Education:** education level and areas of study,
- **Transaction data:** referral name, invoicing history, last four digits of credit card.
- **Marketing data** includes preferences in receiving marketing from us and our third parties and communication preferences.

7.3 Other

- **Communication Data:** Any information you voluntarily provide, including online or through communication.
- **Technical data:** includes internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, domain, and operating system and other technology on the devices used to access our websites.

- **Profile Data** includes account registration details on the platform, username and password, interests, preferences, feedback, and survey responses.
- **Publicly available data** includes identity and contact data from publicly available data sources such as LinkedIn.
- **Observations preferences and opinions:** information included in questionnaires and consent.
- **Usage Data:** includes information about how you use our website and services, and online activity based on your interaction with us, our websites and applications for example searches, site visits browsing actions and patterns. Internet or other electronic network activity information, including, but not limited details of your visits to our Platform, including traffic data, location data, logs, and other communication data and the resources that you access and use on the Platform.
- **Other Information** relevant to conducting business with us or becoming our customer or Information classified as personal or protected information by state, federal, or other applicable law.

8. What is Sensitive or Special Category Data

Sensitive or Special Category Data is Personal Data that needs more protection because it is sensitive.

Where you choose to provide us with this information or we have a lawful reason for collecting it, we will only process that sensitive personal information in such jurisdiction if and to the extent permitted or required by applicable law.

9. Do you collect sensitive Personal Data?

We may collect sensitive Personal Data (in some jurisdictions this is called “**Special Category Data**”) depending on your relationship with us e.g. we collect sensitive data from participants including:

- **Demographic Data:** including ethnicity

Where you choose to provide us with this information in your communication with us, we will only process that sensitive personal information in such jurisdiction if and to the extent permitted or required by applicable law.

10. How do we collect your Personal Data?

10.1 From you directly

We collect personal information that you voluntarily provide to us:

- When you express an interest in obtaining information about us.
- When you enter into a contract with us, request an assessment, purchase our products or services.
- When participate in activities with us or on our platform or websites.
- When you correspond with us, contact us or submit an online request.
- When you create an account profile with us.
- When you fill in forms or upload information to the Platform.
- When you complete our research surveys

- When you provide us with customer testimonials and comments.

10.2 Information collected through technical means

As you navigate through and interact with our Platform, we may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns.

We may log a user's computer IP address, browser type and version, domain, and operating system when a user visits our websites. IP addresses may in some cases be linked to Personal Data. We use the tracked information, including IP addresses, to help diagnose problems with our servers, administer our websites and ensure the security of our network.

We may place a piece of information known as a "cookie" on your computer when you visit our websites. Cookies are commonly used by websites to improve the user's experience. We may use cookies for several purposes – for example, to maintain continuity during an extended user session or to gather data about the usage of our websites for information technology, sales and marketing, and other corporate purposes. Cookies have not been known to transmit computer viruses or otherwise harm computers. Many cookies persist only through a single session or visit, but others may have an expiration date or may remain indefinitely on a computer until deleted.

Our cookies will track only your activity on our websites and will not track your other Internet activity. Our cookies do not gather Personal Data or Financial Information. We may occasionally use third parties to set cookies on our websites and gather cookie information for us or to operate web servers.

10.3 Information we receive from third parties in each case where permissible and in accordance with applicable law

Sometimes we collect your Personal Data from third parties such as organizations, agencies, marketing agencies, market research companies, our suppliers, contractors, customers, partners or consultants only when we have a lawful basis for doing so and have implemented appropriate safeguards to ensure its security and confidentiality.

10.4 Information we receive from public sources

We may collect Information about you from publicly available sources, including any social media platforms such as LinkedIn, public websites and public agencies.

If you are located outside of the United States, please be aware that the Personal Data we collect will be processed and stored in the United States, a jurisdiction in which the data protection and privacy laws may not offer the same level of protection as those in the country where you reside or are a citizen. For more jurisdiction specific information on how we use and process your information see the sections linked below:

- [EEA and UK residents](#)
- [Californian Residents](#)
- [Additional Information about State Privacy Rights](#)

11. How and on what basis do we use your Personal Data?

We may use your Personal Data for a variety of purposes, and (to the extent applicable) on the basis of various legal bases, including, but not limited to, the following:

- Complying with **legal or regulatory obligations**, such as our obligations regarding anti-money laundering due diligence;
- **Performing a contract** with you or to take steps at your request before entering into a contract, including to: (i) provide you with information regarding BIRKMAN or services; (ii) assist you and answer your requests; (iii) evaluate whether we can offer you a BIRKMAN product or service and under what conditions; and (iv) responding to know-your-client and anti-money laundering information requests presented by counterparties with whom we do business on your behalf or for your benefit; and
- Other **legitimate business interests**, such as:
 - Communicating with Data Subjects;
 - Performing activities relating to customer management, financial management and administration;
 - Creating, improving and developing our products and services;
 - Conducting market research, surveys, and similar inquiries to help us understand trends, customer and Website visitor needs;
 - Investigating and resolving disputes and security issues and enforcing our Terms of Service and other agreements;
 - Monitoring and auditing compliance with internal policies and procedures, legal obligations and to meet requirements and orders of regulatory authorities; and

We will not use your Personal Data for any purposes inconsistent with this Notice and the purpose for which it was collected, without your permission or otherwise in accordance with applicable law.

For further information on this for Switzerland, EEA/UK residents see [here](#).

12. Selling Personal Data

We do not barter, trade, or sell access to your Personal Data, other than with your written permission. Financial Information may be shared with third parties for verification, processing, and fraud detection purposes only.

13. With whom do we share your Personal Data?

Within BIRKMAN. We share your Personal Data among BIRKMAN entities and affiliates for the purposes set [forth above](#). In general, BIRKMAN entities and affiliates, in turn, are not permitted to share your information with other non-affiliates entities, except as described herein or otherwise permitted by applicable laws.

To Third Parties. We share your Personal Data with third parties in certain circumstances, including the following:

- **Service Providers** We share Personal Data with service providers that perform services on our behalf (e.g., third-party service providers to operate the Websites)

and with service providers and other counterparties to our customers and investors. These companies may have access to your Personal Data but are permitted to use the information solely to provide the specific service or as otherwise permitted by law. We generally require these providers by contract to keep the information confidential.

- **Transaction or Other Corporate Event.** Your Personal Data can be disclosed as part of a corporate business transaction, such as a merger, acquisition, joint venture, financing, or sale of company assets, including bankruptcy proceedings, or other investment activity, and could be transferred to a third party as one of the business assets in such a transaction. It also can be disclosed in the event of insolvency, bankruptcy, or receivership. In such an event, we will post prominent notice of the change in ownership.
- **To enforce our rights:** to enforce or apply our Terms of Use and other agreements including for billing and collection purposes and where disclosure is necessary or appropriate to protect the rights, property, or safety of Birkman, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.
- **As Required by Law.** We also disclose your Personal Data if we are required to make disclosures by applicable law or to the government or private parties in connection with a lawsuit, subpoena, investigation, or similar proceeding, or as part of our legislative or regulatory reporting requirements.

14. Do you have a choice about the data we collect and use about you?

Yes, you may always choose what personal information (if any) you wish to provide to us.

In cases where you are requested to affirmatively provide information, such as to complete a form, or an application, or a survey on our website, you may decline to do so. Please understand, however, that in some cases certain information is required to complete an application, form, survey, contract, recruitment activity or assessment and if you decline to provide the information requested you may not be able to participate in the applicable activity or service.

If you would prefer not to receive email marketing messages from us, please use the opt-out instructions included in the email message to opt-out of additional communications.

You may be given additional choices in the context of particular preferences tools or functions that we make available through our Websites and Platform.

15. Children's Privacy

The Websites and Platform is intended for general audiences and not for children. Although the Website is not targeted toward children, we are concerned about the safety and privacy of children who use the Internet. If a child under 16 has provided personal information (as defined by the Children's Online Privacy Protection Act) or Personal Data (under the GDPR) to us through the Websites or Platform, a parent or guardian may inform us using the contact details set out under the "[How to contact us](#)" heading above, and we will use commercially reasonable efforts to delete it from our database, subject to applicable law and this Notice.

16. How do we protect your Personal Data?

We take the obligation to safeguard your Personal Data seriously. Your Personal Data held by us will be kept confidential in accordance with applicable BIRKMAN policies and procedures.

We will use all reasonable efforts to ensure that all Personal Data is kept secure and safe from any loss or unauthorized disclosure or use. All reasonable efforts are made to ensure that any Personal Data held by us are stored in a secure and safe place and accessed only by our authorized employees and transferees.

Birkman takes commercially reasonable procedural, physical, and electronic measures to keep your Personal Data secure. We protect your information during electronic transmission by using the Transport Layer Security (TLS) protocol, which encrypts the information that you transmit to us and the information that we transmit to you.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Platform, you are responsible for keeping this password confidential. We ask you not to share your password with anyone. We urge you to be careful about giving out information in public areas of the Platform like message boards. The information you share in public areas may be viewed by any user of the Platform.

Unfortunately, the transmission of information via the Internet is not completely secure. Although we will do our best to protect your personal information, we do not have any control over what happens between your device and the boundary of our information infrastructure. You should be aware of the many information security risks that exist and take appropriate steps to safeguard your own information.

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

17. Transferring your information overseas

We do business globally and may centralize certain aspects of our information processing activities and data storage in different countries. We may therefore have to share and transfer your Personal Data from one country to another, or even across multiple jurisdictions, including, but not limited to transfers between the EEA Switzerland, UK and the US. Your Personal Data may therefore be subject to privacy laws that are different from those in the country where the personal information is collected or those in your country of residences. We will ensure your personal information has an appropriate level of protection and will undertake appropriate due diligence and risk assessments prior to transferring the information.

We will ensure the transfer of your personal information in line with applicable Privacy Law. Often, this protection is set out under a contract with the organization that receives your Personal Data. You can find more details of the protection given to your information when it is transferred overseas by contacting us.

Birkman International, Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) For more information see our section on the Data Privacy Framework [here](#).

Where a privacy regulatory authority requires a corresponding privacy regulatory approval before we transfer your Personal Data outside your jurisdiction, we will obtain the approval before transferring your Personal Data.

18. Keeping your Personal Data current

In general, we seek to ensure that we keep your Personal Data accurate and up to date. However, you are responsible for, and we kindly request that you inform us of, any changes to your Personal Data (such as a change in your contact details).

To update or edit your Personal Data that we have on file, including your communication preferences, please contact us using the contact details set out under the "[How to contact us](#)".

19. How long do we keep your Personal Data?

In general, we will process and store your Personal Data for as long as it is necessary in order to fulfil our contractual, regulatory and statutory obligations, which may differ depending on the relevant BIRKMAN entity or jurisdiction. Subject to those qualifications, our goal is to keep such data for no longer than necessary in relation to the purposes for which we collect and use the Personal Data (we refer to the purposes as set forth above). If you have any specific questions in this respect, please feel free to [contact us](#).

20. Data Subject Rights

BIRKMAN uses your Personal Data in compliance with applicable Privacy laws, most notably, the General Data Protection Regulation (GDPR) and US data protection legislation. These privacy laws and some laws in other regions such as Canada have rights that allow you greater control of and access to your Personal Data.

These rights may include the right:

- To request and obtain a copy of your personal information
- To request rectification and/or erasure
- To restrict processing of your personal information
- Data portability (if applicable)

BIRKMAN does not use automated decision making that has a legal consequence for or otherwise materially and negatively impacts a data subject.

The application of these and any other privacy rights you may have depends on applicable data protection law and if you would like more information about your specific rights under data protection law in your jurisdiction and how to exercise those rights, please [contact us](#).

We may request specific information from you to help us confirm your identity, verify your rights, and respond to your request, including to provide you with the Personal Data that we hold about you, if applicable.

Applicable law may allow or require us to deny your request, or we may have destroyed, erased, or made your Personal Data anonymous in accordance with our record retention obligations and practices.

We will consider and act upon any requests in accordance with applicable privacy laws.

21. Withdrawing Consent

If we rely on your consent to process your personal information, which may be express or implied consent according to the applicable law, you have the right to withdraw consent at any time. You can withdraw your consent by [contacting](#) us.

Please note that this will not affect the lawfulness of the processing before the withdrawal, nor when applicable law allows, will it affect the processing of your personal information on the basis of any other lawful ground other than consent.

22. Changes to Our Privacy Notice

We may update this Notice from time to time. If we make any material changes to this Notice, we will change the "last updated" date so that you can quickly determine whether there were material changes since the last time you reviewed the Notice. You are advised to review this Notice periodically for any changes. Changes to this Notice are effective when they are posted on this page.

23. Data Privacy Framework

Birkman International, Inc complies with the EU-US Data Privacy Framework (EU-US DPF), and the UK Extension to the EU-US DPF, and the Swiss-US Data Privacy Framework (Swiss-US DPF) as set forth by the US Department of Commerce. Birkman International, Inc has self-certified to the US Department of Commerce that it adheres to the EU-US Data Privacy Framework Principles (EU-US DPF Principles) with regard to the processing of Personal Data received from the European Economic Area (EEA) in reliance on the EU-US DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-US DPF.

Birkman International, Inc has certified to the US Department of Commerce that it adheres to the Swiss-US Data Privacy Framework Principles (Swiss-US DPF Principles) with regard to the processing of Personal Data received from Switzerland in reliance on the Swiss-US DPF.

If there is any conflict between the terms in this privacy notice and the EU-US DPF Principles and/or the Swiss-US 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/>

24. Your Rights under the Data Privacy Framework

Under the DPF, you have rights in relation to your Personal Data. These include:

- Information on the types of Personal Data collected.
- Information on the purposes of collection and use.
- Information on the type or identity of third parties to which your Personal Data is disclosed.
- Choices for limiting use and disclosure of your Personal Data.
- Access to your Personal Data.
- Notification of the organization's liability if it transfers your Personal Data.

- Notification of the requirement to disclose your Personal Data in response to lawful requests by public authorities.
- Reasonable and appropriate security for your Personal Data.
- A response to your complaint within 45 days.
- Cost-free independent dispute resolution to address your data protection concerns.
- The ability to invoke binding arbitration to address any complaint that the organization has violated its obligations under the DPF Principles to you and that has not been resolved by other means. under the Data Privacy Framework “Recourse, Enforcement and Liability” [Principle and Annex I of the Data Privacy Framework](#).
- You can also verify our self-certification to the DPF and check the information we have provided by viewing our details on the DPF list

When we engage third parties to process personal information on our behalf under the Data Privacy Framework, these third parties must also comply with the obligations of the Framework. We accept liability for any non-compliance by these third parties, unless we can demonstrate that we are not responsible for the event leading to any incurred damages.

25. Dispute Resolution

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Birkman commits to refer unresolved complaints concerning our handling of Personal Data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to the International Centre for Dispute Resolution - American Arbitration Association (ICDR-AAA), an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://go.adr.org/dpf_irm.html for more information or to file a complaint. The services of ICDR-AAA are provided at no cost to you.

26. Do Not Track

BIRKMAN does not track Data Subjects over time and across third-party websites to provide targeted advertising and therefore does not respond to Do Not Track (“DNT”) signals. However, some third-party sites do keep track of your browsing activities when they serve you content, which enables them to tailor what they present to you. If you are visiting such sites, your browser allows you to set the DNT signal so that third parties (particularly advertisers) know you do not want to be tracked. You should consult the help pages of your browser to learn how to set your preferences so that websites do not track you.

27. Contact and Complaints

BIRKMAN takes very seriously any complaints we receive about our use of your Personal Data. Questions, comments, requests or complaints regarding the Website, this Notice, the Terms of Service and/or our use of your Personal Data should be addressed to us at our [contact details](#).

Any Personal Data we receive from you when making a complaint will be treated in accordance with this Notice and only to process the complaint and check on the level of service we provide. Similarly, where inquiries are submitted to us, we will only use the information supplied to us to deal with the inquiry and any subsequent issues and to check on the level of service we provide.

For further information on contacts and complaints, Swiss, EEA/UK residents can click [here](#).

28. Birkman Website Servers

Please be aware that a website may contain links to other websites hosted by third parties. BIRKMAN does not control and is not responsible for the content or privacy practices and policies of such third-party websites. We encourage you to be aware when you leave the Website and to read the privacy policies of each third-party website, especially if such website collects Personal Data from you.

29. Additional Information for Residents of the European Economic Area (the “EEA”) and the United Kingdom (the “UK”)

For purposes of the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 and the UK GDPR (as defined in the UK Data Protection Act 2018 (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2018 (SI 2019/419)) (both referred to herein as the “**GDPR**”), in addition to the information above, the below applies to any Data Subject whose Personal Data we collect while they are resident in the EEA or the UK and Switzerland when so specified.

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, please contact our DPO at dpoaas@grcilaw.com.

Further details about our processing of your personal information for UK and EEA residents

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.

Table 1: GDPR Lawful Basis of processing

Lawful Basis	Purpose	Types of Personal Data
Contract	Business Contracts Ensuring compliance with Vendor, Supplier, Consultancy and other third-party Contracts	We may use the following Personal Data: <ul style="list-style-type: none">• Commercial data• Communication data• Education and Training data• Contact data• Identification data• Location data• Payment data

<p>Legitimate interest</p> <p>Note 1: When we rely on this, we will carry out a Legitimate Interests Assessment to ensure we consider and balance any potential impact on you (both positive and negative), and your rights under Data Protection Law.</p> <p>Our legitimate business interests do not automatically override your interests – we will not use your Personal Data for activities where our interests are overridden by the impact on you unless we have your consent or are otherwise required or permitted to by law.</p>	<p>Managing our business</p> <p>We process Personal Data for our own legitimate business interest. This relates to us managing our business to enable us to maintain and monitor the performance of our website and services and to constantly look to improve the website and the services it offers to our users, including when we respond to your queries, communications and complaints.</p>	<p>We may use the following Personal Data:</p> <ul style="list-style-type: none"> • Communication data • Contact data • Location data • Marketing data • Technical data • Profile data • Usage data • Other Information
<p>Legitimate interest (see Note 1)</p>	<p>Provide and maintain our websites</p> <p>To provide and maintain our website, including to monitor the usage of these, troubleshooting, data analysis, network security and system testing necessary for our legitimate interests in maintaining the usability, security and integrity of our website.</p>	<p>We may use the following Personal Data:</p> <ul style="list-style-type: none"> • Communication data • Contact data • Location data • Marketing data • Technical data • Profile data • Usage data
<p>Legitimate interest (see Note 1)</p>	<p>Recommendations and marketing</p> <p>To make recommendations to you about services that may interest you.</p>	<p>We may use the following Personal Data:</p> <ul style="list-style-type: none"> • Identity data • Contact data • Technical data • Marketing and communications data • Usage data

Legitimate interest (see Note 1)	<p>To measure and analyze the effectiveness of the advertising we serve you.</p>	<p>We may use the following Personal Data:</p> <ul style="list-style-type: none"> • Identity data • Contact data • Location data • Technical data • Marketing and communications data • Usage data
Legitimate interest (see Note 1)	<p>To comply with applicable laws and regulations and regulatory obligations To comply with our legal and regulatory obligations; for our legitimate interests, i.e., to protect our business, interests and rights in the Clinical trial.</p>	<p>We may use all categories of Personal Data depending on the legal requirement, law and circumstances.</p>
Legitimate interest (see Note 1)	<p>Rights and claims To enforce or apply our website terms of use, our notice terms and conditions, or other contracts. To exercise our rights, to defend ourselves from claims and to keep to laws and regulations that apply to us and the third parties we work with.</p>	<p>We may use all categories of Personal Data depending on the legal requirement, law and circumstances.</p>
Legitimate interest (see Note 1)	<p>Data subject rights Verifying your identity when you exercise your data subject rights. Fulfilling data subject rights requests.</p>	<p>We may use you're your categories of Personal Data we hold on you depending on the details and nature of your data subject request.</p>
Legitimate interest (see Note 1)	<p>Fraud and business reorganization or group restructuring 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 reorganization or group restructuring exercise.</p>	<p>We may use all categories of Personal Data depending on the legal requirement, law and circumstances.</p>

Legitimate interest (see Note 1)	<p>To make Marketing suggestions and recommendations to you about services that may be of interest to you and necessary for our legitimate interests (to develop our products/services and grow our business). We may use the following Personal Data:</p>	<p>We may use the following Personal Data:</p> <ul style="list-style-type: none"> • Communication data • Contact data • Education and Training data • Identification data • Location data • Marketing data • Profile data • Publicly available data • Usage data
Legal obligations Note 2: We may use your Personal Data to comply with laws (for example, if we are required to cooperate with a police investigation after a court order orders us to).	<p>Legal requirement - All categories of Personal Data The processing is necessary for compliance with legal obligations, such as but not limited security requirements.</p>	<p>We may use all categories of Personal Data depending on the legal requirement, law and circumstances.</p>
Legal obligations (see note 2)	<p>To comply with applicable law, for example in response to a request from a court or regulatory body, where such request is made in accordance with the law.</p>	<p>We may use all categories of Personal Data depending on the legal requirement, law and circumstances.</p>
Legal obligations (see note 2)	<p>Criminal activity To detect fraudulent or criminal activity, we may share information with forces such as the police.</p>	<p>We may use all categories of Personal Data depending on the law and circumstances.</p>
Consent Note 3: We may have to get your consent to use your Personal Data, such about you or when we want to send you marketing. Wherever consent is the only reason for using your Personal Data, you have the right to change your	<p>Marketing To measure and analyze the effectiveness of the advertising we serve you.</p> <p>We may collect IP addresses and store Cookies on visitors' devices.</p>	<p>We may use the following Personal Data, depending on what you consent to:</p> <ul style="list-style-type: none"> • Communication data • Contact data • Education and Training data • Identification data • Location data • Marketing data

<p>mind and/or withdraw your consent at any time by clicking the Unsubscribe button at the bottom of an applicable email or by contacting us.</p>		<ul style="list-style-type: none"> • Profile data • Publicly available data • Observations preferences and opinions • Usage data
<p>Consent (see Note 3)</p>	<p>Data analytics We use data analytics to improve our website, products/services, marketing, customer relationships and experiences.</p>	<p>We may use the following Personal Data, depending on what you consent to:</p> <ul style="list-style-type: none"> • Identity data • Transaction data • Technical data • Profile data • Usage data

Table 2: Sensitive Personal data

The lawful basis of processing for sensitive Personal Data is set out below:

Purpose	Lawful Basis
<p>Research purposes - Aggregation</p>	<p>Processing of Personal Data for scientific research purposes, we may aggregate the Data Subject's responses with the responses of other individuals to develop group norms, conduct validation studies, perform statistical analysis, develop new products and services, and otherwise improve our assessments.</p>
<p>Research purposes - Ethnicity</p>	<p>Consent - Research and products</p>

GDPR Data Subject Rights

Under the GDPR, in certain circumstances, a UK, Swiss or EEA-resident Data Subject has certain individual rights with respect to the Personal Data that we hold about them. In particular, you may have the right to:

- Request access to any data held about you;
- Ask to have inaccurate data amended;
- Request data held about you to be deleted, provided the data is not required by BIRKMAN to perform a contract, defend a legal claim or to comply with applicable laws or regulations;
- Prevent or restrict processing of data which is no longer required; and

- Request transfer of appropriate data to a third party where this is technically feasible.

Additionally, in the circumstances where you may have provided your consent to the collection, processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

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 for access is clearly unfounded or excessive.

To exercise any of these rights, please contact us using the contact details set out under the [“Contact and Complaints”](#) heading above. We may need to request further information from you to help us confirm your identity to help facilitate your request. This is a security measure to ensure that Personal Data is not mistakenly disclosed.

Complaints to Local Authorities

As a resident of the EEA, Switzerland or UK, you are also entitled to direct any complaints in relation to our processing of your Personal Data to your national or local data protection supervisory authority.

UK residents can contact the ICO [here](#).

EU residents can find their applicable local data protection supervisory authority [here](#).

30. Additional Information for Residents of California

The information below may apply to Data Subjects who are residents of California.

California Data Subject Rights

California’s “Shine the Light” law permits California residents to annually request and obtain information free of charge about what personal information is disclosed to third parties for direct marketing purposes in the preceding calendar year. For more information on these disclosures, please contact us using the contact details set out under the [“Contact and Complaints”](#) heading above.

In addition, Data Subjects in California may have a right under the California Consumer Privacy Act (“**CCPA**”) to request erasure of their Personal Data or access to Personal Data that we have collected in the last twelve (12) months.

You may submit requests for access or erasure of your personal information by contacting us at privacy@birkman.com

Individuals who submit requests for access or erasure of personal information will be required to verify their identity by answering certain questions. We will not disclose or delete any information until identity is verified.

If you are making a request for access, we may not be able to provide specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of your personal information, your account with us, or our systems or networks.

If you are making a request for erasure, we will ask that you confirm that you would like us to delete your personal information again before your request is addressed.

You may designate an authorized agent to submit a request on your behalf by providing that agent with your written permission. If an agent makes a request on your behalf, we may still ask that you verify your identity directly with us before we can honor the request.

Agents who make requests on behalf of individuals, will be required to verify the request by submitting written authorization from the individual. We will not honor any requests from agents until authorization is verified.

Under the CCPA, you cannot be discriminated against for exercising your rights to access or request erasure of their Personal Data.

31. Additional Information about State Privacy Rights

State consumer privacy laws may provide their residents with additional rights regarding our use of their personal information.

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia provide (now or in the future) their state residents with rights to:

- Confirm whether we process their personal information.
- Access and delete certain personal information.
- Correct inaccuracies in their personal information, taking into account the information's nature processing purpose (excluding Iowa and Utah).
- Data portability.
- Opt-out of Personal Data processing for:
 - targeted advertising (excluding Iowa);
 - sales; or
 - profiling in furtherance of decisions that produce legal or similarly significant effects (excluding Iowa and Utah).
- Either limit (opt-out of) or require consent to process sensitive Personal Data.

The exact scope of these rights may vary by state. To exercise any of these rights or to appeal a decision regarding a consumer rights request please [contact](#) us here.

Nevada provides its residents with a limited right to opt-out of certain personal information sales. Residents who wish to exercise this sale opt-out rights may submit a request to us [here](#). However, please know we do not currently sell data triggering that statute's opt-out requirements.

Last Updated: July 9, 2025