Privacy Policy

31 March 2026

We, APower 3 - Coaching, Training & Mind Freedom Ltd, a company incorporated and existing under the laws of England and Wales, with registration number 10567077, with its registered office at 5 Ducketts Wharf, South Street, Bishop's Stortford, United Kingdom, CM23 3AR, represented by Joanna Breen and Sonja Kirschner, directors, trading as Breen & Associates – Results Through People ('Company', 'we', 'our' or 'us') take your privacy very seriously. Please read this Privacy Policy carefully as it contains important information on how and why we collect, store, use and share any personal data relating to you in connection with your use of our services. It also explains your rights in relation to your personal data and how to contact us or a relevant regulator in the event you have a complaint.

We collect, use and are responsible for certain personal data about you. We are the controller of personal data obtained when you register on our website, place an order, subscribe to our newsletter, respond to a survey, or fill out a form, meaning we are the organisation legally responsible for deciding how and for what purposes it is used.

When we do so we are subject to the UK General Data Protection Regulation (UK GDPR). We are also subject to the EU General Data Protection Regulation (EU GDPR) in relation to services we offer in the European Economic Area (EEA).

This Privacy Policy is divided into the following sections:

1. Introduction;
2. Definitions;
3. Scope (What this policy applies to);
4. Data protection principles;
5. Basis for processing personal data;
6. Personal data we collect about you;
7. How your personal data is collected;
8. How and why we use your personal data;
9. How your personal data will be used should you opt for Third-Party Services;
10. Processing of Data for Training, Coaching, Interactive Sessions and Events
11. Marketing;
12. Who we share your personal data with;
13. Where Will We Store the Data;
14. How long your personal data will be kept;
15. Cookies;
16. Documentation and records;
17. Data subject (individual) rights;
18. Data subject (individual) obligations;
19. Information security;
20. Data breaches;
21. International transfers;
22. Training;
23. Consequences of failing to comply;
24. Changes to this Privacy Policy;
25. How to contact us and how to complain;
26. Consent.

1. Introduction

1.1 The Company obtains, keeps and uses personal data (also referred to as personal information) for a number of specific lawful purposes, as set out in this Privacy Policy concerning various data subjects.

1.2 This Privacy Policy sets out how we comply with our data protection obligations and seek to protect personal data relating to our workforce. Its purpose is also to ensure that our staff and our clients understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal data relating to our workforce, and how (and when) we delete that data once it is no longer required.

2. Definitions

Academy Event(s)	means all public webinars, live online training sessions, interactive workshops, and on-demand courses provided by us via our Online Training Academy;
Artificial Intelligence (AI) Tools	means any machine learning models, large language models (LLMs), automated transcription services, or generative AI bots (including but not limited to Zoom AI Companion, ChatGPT, or Otter.ai) capable of processing, summarising, or replicating audio, video, or text data;
criminal records data	means personal data relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
data subject	means the individual to whom the personal data relates;
Delegate(s)	means any individual attending or accessing a Session, whether they purchased access directly, or access was purchased on their behalf by their employer or another Client;
LMS	means Learning Management System, being the third-party software platform or digital infrastructure utilised by Breen & Associates – Results Through People to host, manage, and deliver the Online Training Academy content;
Online Training Academy	means the digital platform, sub-domain, or dedicated online learning environment operated by us (and/or our third-party software providers) through which we market, host, and deliver our live and on-demand Academy Events;
personal data	(sometimes known as personal information) means data relating to an individual who can be identified (directly or indirectly) from that data;
processing data	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying data, or using or doing anything with it;
Session(s)	means any Academy Event, private commissioned training, coaching session, in-person workshop, or any other professional service, consultancy, or interactive

	engagement provided by Breen & Associates – Results Through People, regardless of the delivery format or platform;
special category data	(sometimes known as 'special categories of personal data', 'sensitive personal data' or 'sensitive personal information') means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics data, biometric data (where used to identify an individual) and data concerning an individual's health, sex life or sexual orientation.
Third-Party Services	means any software platforms, applications, employee assistance programmes, or other ancillary services provided by independent Third-Party Providers (including but not limited to HR information systems and mental health platforms) which are resold, administered, or introduced by Breen & Associates – Results Through People to the Client.
Third-Party Provider	means the independent third-party vendor, licensor, or supplier of the Third-Party Services.
Third-Party Terms	means the end-user license agreements (EULAs), terms of use, privacy policies, and other contractual terms established by the Third-Party Providers, which govern the Client's access to and use of such services.

3. Scope (What this policy applies to)

3.1. This Privacy Policy applies to the personal data of various individuals who interact with our services, including but not limited to Website visitors, Individuals who contact the Company through any communication channels, job applicants, current and former staff of businesses that work with us (such as employees, temporary and agency workers, interns, volunteers, and apprentices), business owners of the businesses that works with us and their teams, HR professionals seeking outsourced HR support from us, and individuals seeking personal performance or business coaching from the Company.

4. Data protection principles

4.1. The Company will comply with the following data protection principles when processing personal data:

4.1.1. we will process personal data lawfully, fairly and in a transparent manner;

4.1.2. we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3. we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;

4.1.4. we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;

4.1.5. we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and

4.1.6. we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5. Basis for processing personal data

5.1. In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1. review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;

(e) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject – see paragraph 5.2 below.

5.1.2. except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose);

5.1.3. document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4. include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5. where 'special category data is processed, also identify a lawful special condition for processing that data (see paragraph 6.3.2 below), and document it; and

5.1.6. where criminal records data is processed, also identify a lawful condition for processing that data, and document it.

5.2. When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1. conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2. if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

5.2.3. keep the LIA under review, and repeat it if circumstances change; and

5.2.4. include information about our legitimate interests in our relevant privacy notice(s).

6. Personal data we collect about you

6.1. The personal data we collect about you depends on the particular activities carried out through our website. We will collect and use the following personal data about you:

- title;
- first name;
- last name;
- e-mail address;
- mailing address;
- information to check and verify your identity, e.g. date of birth;
- your gender, if you choose to give this to us;
- phone number;
- your billing information, transaction and payment card or other payment method information;
- bank account and payment details;
- details of any information, feedback or other matters you give to us by phone, email, post or via social media;
- your use of our services;
- your personal or professional interests;
- your professional online presence, e.g. LinkedIn profile;
- information about the services we provide to you;
- information about how you use our website and technology systems;
- your responses to surveys, competitions and promotions.

6.2. Sometimes you can choose if you want to give us your personal data and let us use it. Where that is the case we will tell you and give you the choice before you give the personal data to us. We will also tell you whether declining to share that personal data will have any effect on use of our services.

6.3. Special category data. Special category data is sometimes referred to as 'sensitive personal data' or 'sensitive personal information'. We may from time to time need to process special category data. We will only process special category data if:

6.3.1. we have a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g. it is necessary for the performance of the contract or to comply with our legal obligations; and

6.3.2. one of the special conditions for processing special category data applies, e.g.:

6.3.3. the data subject has given explicit consent;

6.3.4. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

6.3.5. processing relates to personal data which are manifestly made public by the data subject;

6.3.6. the processing is necessary for the establishment, exercise or defence of legal claims; or

6.3.7. the processing is necessary for reasons of substantial public interest.

6.4. Special category data will not be processed until:

6.4.1. the assessment referred to in paragraph 6.3 has taken place; and

6.4.2. the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

7. How your personal data is collected

7.1. We collect personal data from you:

- directly, when you enter or send us information, such as when you fill in the contact form on our website and/or Pricing Plan Submission Form, communicate with us, contact us (including via email), send us feedback, purchase services via our website, post material to our website and complete customer surveys, and
- indirectly, such as your browsing activity while on our website; we will usually collect information indirectly using the technologies explained in the section 'Cookies' below.

7.2. We also may collect personal data about you from other sources as follows:

- from publicly available sources (such as search engine results) or through professional networking sites and subscription-based platforms (including but not limited to LinkedIn and LinkedIn Sales Navigator); and
- by purchasing contact data or marketing lists from third-party data providers, provided that such providers have confirmed their compliance with Data Protection Legislation (as defined in our Terms of Business). While we conduct reasonable due diligence to ensure that we engage with reputable third-party providers who demonstrate compliance with Data Protection Legislation, we rely on the representations, warranties, and assurances provided by such third parties regarding the lawful collection of your data. We do not control their data collection methods or internal processing protocols. Consequently, to the fullest extent permitted by applicable law, we accept no liability for any non-compliance by such third parties regarding the original collection of data, provided that we have acted in good faith and relied on their confirmation of compliance.

8. How and why we use your personal data

8.1. Under data protection law, we can only use your personal data if we have a proper reason, e.g.:

- where you have given consent;
- to comply with our legal and regulatory obligations;
- for the performance of a contract with you or to take steps at your request before entering into a contract; or
- for our legitimate interests or those of a third party.

8.2. A legitimate interest is when we have a business or commercial reason to use your personal data, so long as this is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interests, to balance our interests against your own. You can obtain details of this assessment by contacting us (see section 'How to contact us' below).

8.3. The table below explains what we use your personal data for and why.

What we use your personal data for	Our reasons
Creating and managing your account with us.	For our legitimate interests, i.e., to be as efficient as we can so we can deliver the best service to you at the best price.
Providing services to you.	To perform our contract with you or to take steps at your request before entering into a contract.
Conducting checks to identify you and verify your identity or to help prevent and detect fraud against you or us.	To comply with our legal and regulatory obligations.
Enforcing legal rights or defend or undertake legal proceedings.	Depending on the circumstances: – to comply with our legal and regulatory obligations; – in other cases, for our legitimate interests, i.e., to protect our business, interests and rights.
Customising our website and its content to your particular preferences based on a record of your selected preferences or on your use of our website.	Depending on the circumstances: – your consent as gathered by the separate cookies tool on our website – see section 'Cookies' below – where we are not required to obtain your consent and do not do so, for our legitimate interests, i.e., to be as efficient as we can so we can deliver the best service to you at the best price If you have provided such a consent you may withdraw it at any time by e.g. by changing the setting on the cookies tool (this will not affect the lawfulness of our use of your personal data in reliance on that consent before it was withdrawn).
Retaining and evaluating information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive or to check our website is working as intended.	Depending on the circumstances: – your consent as gathered by the separate cookies tool on our website – see section 'Cookies' below; – where we are not required to obtain your consent and do not do so, for our legitimate interests, i.e., to be as efficient as we can so we can deliver the best service to you at the best price. If you have provided such a consent you may withdraw it at any time by e.g. by changing the setting on the cookies tool (this will not affect the lawfulness of our use of your personal data in reliance on that consent before it was withdrawn).
Communications with you not related to marketing, including about changes to our terms or policies or	Depending on the circumstances:

changes to the products and/or services or other important notices.	– to comply with our legal and regulatory obligations; – in other cases, for our legitimate interests, i.e., to be as efficient as we can so we can deliver the best service to you at the best price.
Protecting the security of systems and data used to provide the services.	To comply with our legal and regulatory obligations. We may also use your personal data to ensure the security of systems and data to a standard that goes beyond our legal obligations, and in those cases our reasons are for our legitimate interests, i.e., to protect systems and data and to prevent and detect criminal activity that could be damaging for you and/or us.
Statistical analysis to help us understand our customer base.	For our legitimate interests, i.e., to be as efficient as we can so we can deliver the best service to you at the best price.
Updating and enhancing customer records.	Depending on the circumstances: – to perform our contract with you or to take steps at your request before entering into a contract; – to comply with our legal and regulatory obligations; – where neither of the above apply, for our legitimate interests, e.g. making sure that we can keep in touch with our customers about existing orders and new products.
Disclosures and other activities necessary to comply with legal and regulatory obligations that apply to our business, e.g. to record and demonstrate evidence of your consents where relevant.	To comply with our legal and regulatory obligations.
Marketing our services to existing and former customers.	For our legitimate interests, i.e., to promote our business to existing and former customers. See section 'Marketing' below for further information.
To share your personal data with trusted third parties who assist us in operating our website, conducting our business, or providing services to you. These parties are required to keep your information confidential. In such cases information will be anonymised where possible and only shared where necessary.	For our legitimate interests, i.e., to be as efficient as we can so we can deliver the best service to you at the best price.
To share your personal data with members of our group and third parties that will or may take control or ownership of some or all of our business (and professional advisors acting on our or their behalf) in connection with a significant corporate transaction or	Depending on the circumstances: – to comply with our legal and regulatory obligations;

restructuring, including a merger, acquisition, asset sale, initial public offering or in the event of our insolvency. In such cases information will be anonymised where possible and only shared where necessary.	– in other cases, for our legitimate interests, i.e., to protect, realise or grow the value in our business and assets.

9. How your personal data will be used should you opt for Third-Party Services?

9.1. Should you decide to opt for any Third-Party Services (including but not limited to cloud-based HR software, payroll systems, and mental health or Employee Assistance Programmes), please be aware that for the purposes of Data Protection Legislation, the respective Third-Party Providers act as independent data controllers (or data processors on behalf of your employer, as applicable) in relation to any of your personal data processed during the provision of their services. Your use of these platforms is strictly governed by the applicable Third-Party Terms.

9.2. We will only provide Third-Party Providers with your personal data when we are entitled to do so, subject always to our Terms of Business and this Privacy Policy. We will not provide Third-Party Providers with any instructions in relation to you which are inconsistent with our Terms of Business, this Privacy Policy, or other lawful instructions provided by you or your employer.

9.3. You acknowledge that certain Third-Party Services (in particular, mental health, wellbeing, coaching, or therapy platforms) may involve the processing of special category personal data. We strictly do not have access to, nor do we process, the content of confidential therapy sessions, specific health data, or private consultations of authorised users. The Third-Party Provider is solely responsible for securing such sensitive data in accordance with the Data Protection Legislation.

9.4. Third-Party Services may utilise Artificial Intelligence (AI) features. While a Third-Party Provider's policies may indicate how personal data is processed regarding machine learning, it is your sole responsibility to review and verify their specific AI data usage policies directly with them. We do not own or control these AI algorithms, data training models, or data processing protocols, and we make no representations regarding their use of your personal data for machine learning purposes.

9.5. Please note that Third-Party Services are provided by independent entities. We are not responsible or liable for any data breach, unauthorised access, data loss, or cyber security incident that occurs within the systems, servers, or platforms of these Third-Party Providers. Any such incidents must be addressed directly with the respective provider.

9.6. Personal data stored within third-party platforms is strictly subject to the retention policies of those respective providers. Upon termination of your service with them, data will be deleted or archived in accordance with the respective Third-Party Terms. Please note that where we act as a reseller or administrator for Third-Party Services, requests regarding data subject rights (such as rights of access, rectification, or erasure of data held within those platforms) should be directed to the respective service provider or your employer (the Data Controller).

9.7. When setting up or administering accounts for Third-Party Services on your behalf, we strictly adhere to the principle of data minimisation. We will only transfer the minimum amount of personal data strictly necessary (e.g. full name and corporate email address) to provision the account and facilitate your access to the requested platform.

9.8. Where we receive usage reports, analytics, or service feedback from Third-Party Providers (particularly concerning EAP, mental health, or wellbeing services), we ensure that such data is provided to us in a strictly aggregated and anonymised format. We do not receive, request, or process any metrics that could identify an individual user's interaction with sensitive support services.

9.9. You acknowledge that Third-Party Providers may host, store, or process your personal data on servers located outside of the United Kingdom (UK) or the European Economic Area (EEA). Such international data transfers are governed entirely by the applicable Third-Party Terms and the safeguarding mechanisms they have implemented (such as Standard Contractual Clauses or adequacy decisions).

9.10. Where you choose to integrate Third-Party Services with your existing internal systems (e.g. via APIs or automated data syncing tools), you acknowledge that we do not provide technical setup, configuration, or integration support. You and the respective Third-Party Provider are solely responsible for ensuring that the transmission and syncing of personal data are secure. Once the personal data is transmitted to or from the Third-Party Provider's environment, its security, storage, and processing fall entirely under their jurisdiction and your responsibility.

9.11. We do not maintain redundant backups or shadow copies of the personal data you store natively within Third-Party Services. In the event of subscription termination, it is entirely the responsibility of the user or the employer to export, migrate, and secure their personal data before the Third-Party Provider permanently purges it in line with their respective data retention schedules.

9.12. You acknowledge that upon provisioning your account, Third-Party Providers may send you direct communications, such as system notifications, onboarding guides, or promotional materials, in accordance with their own policies. We do not manage or control these communications, and any requests to opt-out, unsubscribe, or modify your communication preferences regarding such direct emails must be executed directly through the Third-Party Provider’s platform or unsubscribe mechanisms.

9.13. In the event you request technical support, administration, or troubleshooting assistance regarding a Third-Party Service, we may need to share specific details of your query, including relevant personal data, error logs, or system screenshots, with the Third-Party Provider’s technical support team. Such targeted data sharing is conducted strictly for the purpose of resolving your operational issue and remains subject to the applicable Third-Party Terms.

9.14. Certain Third-Party Services may employ automated decision-making or profiling techniques, for instance, to recommend specific wellbeing resources, match users with coaches, or generate automated HR analytics. We do not participate in, control, or define the logic underlying these automated processing activities. Any inquiries, rights requests, or objections related to such automated decision-making must be directed to the respective Third-Party Provider.

10. Processing of Data for Training, Coaching, Interactive Sessions and Events

10.1. When you register for, purchase access to, or attend a Session (or when a Client provides your details to us for these purposes), we will collect personal data including your name, email address, job title, company name, billing information, and IP address. During live virtual or recorded in-person sessions, if you choose to actively participate, we may also collect your voice, image, video feed, and any text inputted into the public chat function.

10.2. For quality assurance, and to facilitate the creation of on-demand content and training resources, virtual live Sessions are routinely recorded:

- For public sessions where tickets are purchased online, attendees will be notified of the recording via an automated audio notification and/or a persistent visual indicator (e.g. a red recording icon or banner generated by the hosting platform such as Zoom, Google Meet, MS Teams or any other platform of choice) or the visible presence of an AI note-taking bot in the participant list. This ensures that all attendees, including those who join the session late and may have missed the initial audio prompt, are fully informed. By joining or remaining in the session after such notification is provided, Delegates provide clear consent to the recording in accordance with Article 7 of the UK GDPR.

- Where training is privately commissioned by a Client for their team, Delegates will be informed verbally, via an on-screen notice, or via the platform's persistent visual recording indicator, or via the visible presence of an AI note-taking bot prior to or during the commencement of the recording in accordance with our transparency obligations under Article 13 of the UK GDPR.

- Any Delegate who does not wish to have their personal data recorded during a Session must ensure their microphone and camera remain disabled throughout the session and abstain from using the public chat function.

10.3. We may utilise integrated, platform-native AI tools (such as automated closed-captioning, transcription, or summarisation features) during Sessions to take notes, enhance accessibility and create learning resources. These authorised tools operate under our direct control and are bound by strict confidentiality standards. By participating in the Session, you acknowledge that your voice and text inputs may be processed by these AI sub-processors. However, to strictly protect the Intellectual Property of our materials and the privacy of all attendees, we expressly prohibit Delegates from introducing their own personal or unauthorised AI bots into any Session to record or transcribe.

10.4. We strictly prohibit the use of unauthorised third-party AI bots (e.g. Otter.ai, Fireflies) by Delegates to record or transcribe sessions.

10.5. We process your data in relation to Sessions on the following lawful bases: (a) to process your registration, grant you access, and deliver the educational services; (b) to record sessions for quality assurance, training purposes, and the commercial development of our on-demand Online Training Academy library; (c) where strictly required by applicable data protection laws, for the capturing of your audio and visual data.

10.6. Sessions are hosted using third-party teleconferencing software and LMS. These platforms may process or store your personal data on servers located outside the UK or the European Economic Area (EEA) (e.g. in the United States). Where such international transfers occur, we ensure they are safeguarded by appropriate mechanisms approved under the UK GDPR, such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses (SCCs).

10.7. Video and audio recordings of Sessions may be retained and hosted on our platforms as on-demand content indefinitely, or until the educational content is deemed commercially obsolete. You retain the right to request the erasure of your personal data from such recordings, subject to technical feasibility (e.g. blurring your image) and our overriding legitimate commercial interests.

10.8. When you access on-demand courses via our Online Training Academy, we collect technical and behavioural data regarding your engagement (module completion rates, assessment scores, watch times). This data is processed on the basis of our legitimate interest to improve our educational offerings and, where applicable, to report compliance and attendance metrics back to the Client (your employer) who commissioned the training.

10.9. If you notify us of specific accessibility requirements prior to an event, this may inadvertently disclose health-related information (Special Category Data). We will process this information based on your explicit consent, solely for the purpose of making reasonable adjustments, and will securely delete this specific data once the relevant Session has concluded.

10.10. Where a Client commissions private virtual, hybrid, or in-person training where multiple Delegates share a single physical room and conferencing camera, or during in-person workshops, the recording may capture wide-angle footage of the room. The Client (the commissioning lead) is solely responsible for managing local consent and ensuring that any Delegate who has opted out of being recorded is seated outside the camera's field of view.

11. Marketing

11.1. We will use your personal data to send you updates (by email, text message, telephone or post) about our services, including exclusive offers, promotions or information on new products and/or services.

11.2. We have a legitimate interest in using your personal data for marketing purposes (see section 'How and why we use your personal data' above). This means we do not need your consent to send you marketing information. If we change our marketing approach in the future so that consent is needed, we will ask for this separately and clearly.

11.3. You have the right to opt out of receiving marketing communications at any time by:

11.3.1. contacting us at team@breenassociates.co.uk;

11.3.2. using the 'unsubscribe' link in emails; or

11.3.3. updating your marketing preferences on our website.

11.4. We will always treat your personal data with the utmost respect and never sell or share it with other organisations for marketing purposes.

11.5. For more information on your right to object at any time to your personal data being used for marketing purposes, see section 'Data subject (individual) rights' below.

12. Who we share your personal data with

12.1. We routinely share or are planning to share personal data with:

- third parties we use to help deliver our products and/or services to you, e.g. payment service providers;
- other third parties we use to help us run our business, e.g. marketing agencies or website hosts and website analytics providers;

12.2. online services, online media and social media platforms and similar organisations where we might run our marketing campaigns. We only allow those organisations to handle your personal data if we are satisfied they take appropriate measures to protect your personal data.

12.3. We or the third parties mentioned above occasionally also share personal data with:

- our and their external auditors, e.g. in relation to the audit of our or their accounts, in which case the recipient of the information will be bound by confidentiality obligations;
- our and their professional advisors (such as lawyers and other advisors), in which case the recipient of the information will be bound by confidentiality obligations;
- law enforcement agencies, courts, tribunals and regulatory bodies to comply with our legal and regulatory obligations.

13. Where Will We Store the Data?

13.1. Personal data (and special category data) will be kept securely in accordance with this Privacy Policy.

13.2. Personal data (and special category data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

13.3. We store all our customer and lead data using the following trusted services:

- Wix: For managing and storing website-related data.
- QuickBooks: For financial and accounting data.
- GoCardless: For processing and storing payment information.

13.4. Additionally, some data, such as first name, last name, and email address, is stored on our People Keys account. This service is used for psychometric testing and managing personality profiles of clients.

13.5. These storage providers are selected for their commitment to data security and compliance with data protection regulations. While we rely on these reputable services to handle your data, we do not directly control their security measures.

14. How long your personal data will be kept

14.1. Personal data (and special category data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained.

14.2. Different retention periods apply for different types of personal data. All data retention practices will comply with GDPR and UK GDPR requirements.

15. Cookies

15.1. A cookie is a small text file which is placed onto your device (e.g. computer, smartphone or other electronic device) when you use our website. We use cookies on our website.

15.2. We use cookies to help us remember and process the items in your shopping cart, understand and save your preferences for future visits and compile aggregate data about site traffic and site interaction so that we can offer better site experiences and tools in the future. We may contract with third-party service providers to assist us in better understanding our site visitors. These service providers are not permitted to use the information collected on our behalf except to help us conduct and improve our business.

16. Documentation and records

16.1. We will keep written records of processing activities which are high risk, i.e., which may result in a risk to individuals' rights and freedoms or involve special category data or criminal records data, including:

16.1.1. the purposes of the processing;

16.1.2. a description of the categories of individuals and categories of personal data;

16.1.3. categories of recipients of personal data;

16.1.4. where possible, retention schedules; and

16.1.5. where possible, a description of technical and organisational security measures.

16.2. As part of our record of processing activities we document, or link to documentation, on:

16.2.1. information required for privacy notices;

16.2.2. records of consent;

16.2.3. controller-processor contracts;

16.2.4. the location of personal data;

16.2.5. DPIAs; and

16.2.6. records of data breaches.

16.3. If we process special category data or criminal records data, we will keep written records of:

16.3.1. the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

16.3.2. the lawful basis for our processing; and

16.3.3. whether we retain and erase the personal data in accordance with our policy document and, if not, the reasons for not following our policy.

16.4. We will conduct regular reviews of the personal data we process and update our documentation accordingly.

17. Data subject (individual) rights

17.1. You (in common with other data subjects) have the following rights in relation to your personal data:

17.1.1. to be informed about how, why and on what basis that data is processed;

17.1.2. to obtain confirmation that your data is being processed and to obtain access to it and certain other information, by making a data subject access request;

17.1.3. to have data corrected if it is inaccurate or incomplete;

17.1.4. to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

17.1.5. to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal data but you require the data to establish, exercise or defend a legal claim; and

17.1.6. to restrict the processing of personal data temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

17.2. If you wish to exercise any of the rights in paragraphs 8.1.3 to 8.1.6. please contact Joanna Louise Breen, Data Officer, at team@breenassociates.co.uk.

18. Data subject (individual) obligations

18.1. Individuals are responsible for helping the Company keep their personal data up to date. You should let us know if the data you have provided to the Company changes.

18.2. You may have access to the personal data of other members of staff and suppliers of the Company in the course of your engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 15.1. above.

18.3. If you have access to personal data, you must:

18.3.1. only access the personal data that you have authority to access, and only for authorised purposes;

18.3.2. only allow other Company staff to access personal data if they have appropriate authorisation;

18.3.3. only allow individuals who are not Company staff to access personal data if you have specific authority to do so from Joanna Louise Breen, Data Officer;

18.3.4. keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction;

18.3.5. not remove personal data, or devices containing personal data (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the data and the device; and

18.3.6. not store personal data on local drives or on personal devices that are used for work purposes.

18.4. You should contact Joanna Louise Breen, Data Officer, if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

18.4.1. processing of personal data without a lawful basis for its processing or, in the case of special category data, without one of the conditions in paragraph 6.3.2. being met;

18.4.2. any data breach as set out in this Privacy Policy and applicable laws;

18.4.3. access to personal data without the proper authorisation;

18.4.4. personal data not kept or deleted securely;

18.4.5. removal of personal data, or devices containing personal data (or which can be used to access it), from the Company's premises without appropriate security measures being in place;

18.4.6. any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

19. Information security

19.1. The Company will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

19.1.1. making sure that, where possible, personal data is pseudonymised or encrypted;

19.1.2. ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

19.1.3. ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and

19.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

19.1.5. pseudonymisation and encryption of personal data;

19.1.6. ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

19.1.7. ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

19.1.8. ensuring protection of personal data during transmission;

19.1.9. ensuring protection of personal data during storage;

19.1.10. ensuring physical security of locations at which personal data are processed;

19.1.11. ensuring access controls, including role-based access and least privilege principles;

19.1.12. ensuring secure disposal of personal data and equipment used to process personal data;

19.1.13. conducting personnel training and awareness programs on data protection and security;

19.1.14. ensuring third-party compliance with data protection standards when personal data is shared or processed by subcontractors;

19.1.15. encryption of backups and their secure storage;

19.1.16. monitoring and responding to unauthorised access attempts and anomalies in data processing;

19.1.17. implementing data minimization principles, ensuring only necessary data is collected and processed;

19.1.19. maintaining up-to-date software and applying security patches promptly;

19.1.19. securing endpoints, including laptops, mobile devices, and other portable media;

19.1.20. ensuring network security, including firewalls, intrusion detection/prevention systems, and secure network architecture;

19.1.21. segregation of duties to prevent conflicts of interest and reduce the risk of unauthorised access;

19.1.22. ensuring secure configuration and management of cloud services used to process personal data;

19.2. Where the Company uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. In particular, contracts with external organisations must provide that:

19.2.1. the organisation may act only on the written instructions of the Company;

19.2.2. those processing the data are subject to a duty of confidence;

19.2.3. appropriate measures are taken to ensure the security of processing;

19.2.4. sub-contractors are only engaged with the prior consent of the Company and under a written contract;

19.2.5. the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;

19.2.6. the organisation will assist the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

19.2.7. the organisation will delete or return all personal data to the Company as requested at the end of the contract; and

19.2.8. the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something infringing data protection law.

20. Data breaches

20.1. A data breach may take many different forms, for example:

20.1.1. loss or theft of data or equipment on which personal data is stored;

20.1.2. unauthorised access to or use of personal data either by a member of staff or third party;

20.1.3. loss of data resulting from an equipment or systems (including hardware and software) failure;

20.1.4. human error, such as accidental deletion or alteration of data;

20.1.5. unforeseen circumstances, such as a fire or flood;

20.1.6. deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

20.1.7. 'blagging' offences, where data is obtained by deceiving the organisation which holds it.

20.2. The Company will:

20.2.1. make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

20.2.2. notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

21. International transfers

21.1. The Company may transfer personal data outside the UK on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the data has provided adequate safeguards by way of binding corporate rules, standard data protection clauses, or of compliance with an approved code of conduct.

22. Training

22.1. The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

23. Consequences of failing to comply

23.1. The Company takes compliance with this policy very seriously. Failure to comply with the policy:

23.1.1. puts at risk the individuals whose personal data is being processed; and

23.1.2. carries the risk of significant civil and criminal sanctions for the individual and the Company; and

23.1.3. may, in some circumstances, amount to a criminal offence by the individual.

23.2. Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

23.3. If you have any questions or concerns about anything in this policy, do not hesitate to contact Joanna Louise Breen, Data Officer.

24. Changes to this Privacy Policy

24.1. We may change this Privacy Policy from time to time at our sole and absolute discretion. The up-to-date version will be available on our website, and the date of the version will be included in the notice at the beginning of the Privacy Policy published on the website.

25. How to contact us and how to complain

25.1. Joanna Louise Breen, Data Officer, is responsible for data protection compliance within the Company. If you have any questions or comments about the content of this policy or if you need further information, you should contact us via team@breenassociates.co.uk.

25.2. You also have the right to lodge a complaint with the Information Commissioner in the UK and/or a relevant data protection supervisory authority in the EEA state of your habitual residence, place of work or of an alleged infringement of data protection laws in the EEA.

25.3. The UK's Information Commissioner may be contacted using the details at www.ico.org.uk/make-a-complaint or by telephone: 0303 123 1113.

25.4. For a list of EEA data protection supervisory authorities and their contact details see here.

26. Consent

26.1 By accessing or using our website(s), you agree to the terms outlined in this Privacy Policy. Your use of our website(s) signifies your acceptance of the policies and practices described herein. If you do not agree with any part of this Privacy Policy, please discontinue use of the website(s). Your continued use of the website constitutes your acceptance of any changes or updates to the Privacy Policy.