Alpamayo Coaching Ltd

Privacy Notice

Alpamayo Coaching Ltd (AC) is registered with the Information Commissioners Office (ICO), Registration reference number ZA703965.

Alpamayo Coaching Ltd (AC) is committed to respecting the privacy rights of all customers of its services and visitors to its website (www.alpamayocoaching.com). AC complies with data protection laws at all times and have set out this Privacy Notice to explain what personal data we collect, why we collect it, how we protect it, and to explain your rights.

Note that AC using the services of WIX for website provision and Lumina Learning for various coaching related services. Both are referenced within this notice in relation to their processing of data on behalf of AC.

1. Personal data AC collects

AC collects the following data on coaching clients:

- your name, e-mail address, and other appropriate contact contact details;
- information about your requirements for coaching/ training/ facilitation services provided by AC which are used to prepare specifics in support of the service being requested;
- in relation to coaching only, and with your express permission, written notes and recordings of coaching sessions;
- data collected through AC's website provider, WIX, in the form of persistent cookies that can identify the user and their surfing behaviour on their site (see https://support.wix.com/en/article/cookies-and-your-wix-site).
- data collected by Lumina Learning (www.luminalearning.com) in generation and delivery of their personality profile (Spark and Emotion). AC is data controller over information gathered by Lumina Learning, and the portraits it produces, in relation to AC clients only.

AC's website and services is not intended for use by children and as such we do not knowingly collect data relating to children.

2. How AC protects your data

AC is committed to keeping your data secure. All personal data is stored in encrypted files in a single location with access only provided to the coach responsible for a given client.

The way that WIX handles and secures data as described in its own privacy notice located at https://www.wix.com/about/privacy.

Lumina Learning has its own privacy notice at https://www.luminalearning.com/generalprivacynotice/index/en-us including information about how it protects your data. In general the data provided to Lumina Learning is secured in an account for which you provide username and password.

3. How AC uses your data

AC uses your data for three reasons only:

- to provide information, support and services to you;
- to enrich and inform the coaching/ training/ facilitation service being provided to you'
- to manage customer service interactions with you;

4. When and how AC might share your data

- AC will never sell your personal data neither will it share your data with any other party in the sense of transferring it from AC to that third party.
- How information is shared by WIX and Lumina Learning is described in their privacy notices accessed through the links in Section 2.
- High quality coaching is supported by coaching supervision. AC coaches will undertake professional coach supervision. This process may involve the discussion of an AC client's coaching session on the clear understanding that (a) the client's identity is not revealed and (b) the supervision itself is strictly confidential. The purpose of this is for coach development and protection.
- As part of the accreditation process that quality assures the coaching practice of AC staff there is a requirement to keep a log of names and email addresses of clients. These may be shared with the accrediting body (International Coach Federation) during reaccreditation. The purpose of this sharing is to allow the ICF to contact the client to confirm that the claimed coaching hours have been completed. There is no expectation to discuss the content or outcomes.

5. How long we keep your data

AC only keep your data for as long as it needs to. More specifically:

Coaching information – typically for a period of 5 years after completion of the coaching programme;

Lumina Learning profiles - typically for a period of 5 years after the issue of the Lumina portrait.

6. Transferring data outside of the European Economic Area (EEA)

AC is required to tell you if it transfers data outside of the EEA. The data AC collects and processes is not transferred outside of the EEA.

7. Legal basis for using your data

AC generally relies on your consent to use your personal data in relation to monitoring website usage and sending you direct e-mails through our mailing list, or providing customer care, information or support should you choose to contact us directly through our website.

AC also processes your data because it is in our legitimate interests that it does so, namely:

- promoting, marketing and advertising our products and/or services;
- sending information to you by e-mail or text message about our products and/or services;
- protecting the Organisation, our staff, volunteers, funders, partners and clients/customers/service users by taking appropriate legal action against third parties who have committed criminal acts;
- fulfilling our duties to our customers/clients/service users.

8. Cookies

AC uses WIX to provide website services. WIX uses some persistent cookies. More information can be found at https://support.wix.com/en/article/cookies-and-your-wix-site.

9. Your legal rights

You have the following rights:

- the right to ask what personal data AC holds about you;
- the right to ask AC to update and correct or delete any out-of-date or incorrect personal data that AC holds about you;
- the right to opt out of any marketing communications that AC may send you;
- To exercise any of the above rights please contact jeremy.d.hinks@gmail.com. You also have the right to lodge a complaint with the Information Commissioner's Office (the supervising authority for data protection in the UK). To do that please visit their website at https://ico.org.uk/concerns/.

10. Reviewing and changing how we use data

This Privacy Notice was last updated in February 2024. It is reviewed and updated annually. Given the pace of change in information technology it is possible that AC will need to change the way it manages data, and the third parties it engages to provide the necessary services to its clients. Should any change in data type or use be required we will be in touch with all our clients to ensure that we have their express permission to use their data under any new regime.

AC will always seek to minimise the amount of data we collect and use, and to only keep it for as long as we need to.

Whenever any change is made to how AC collects or uses personal data AC will update this Privacy Notice and any other relevant policies.

11. How to find out more or to make a complaint

We've endeavoured to make this Privacy Notice clear, informative and understandable, but if it is not then please contact us and we shall provide further information as required. We will also look to improve the wording of this Privacy Notice, based on feedback.

To provide feedback, ask for more details or to make a complaint about our collection or use of your personal data then please contact jeremy.d.hinks@gmail.com.

You can also complain to the Information Commissioner's Office in the UK - please visit their website to see how you can do that.

Data Controller

Dr Jeremy Hinks

1st February 2024

Appendix

The information in these appendices is intended to provide clarity around the key elements of the GDPR regulations. It does not constitute legal advice. Instead it is a synthesis of information used to guide the preparation of this policy.

1.1 What is personal data?

Personal data is any information relating to a person. When you handle personal data you are processing it. This includes almost any operation performed on it: collection, recording, organization, alteration, transmission and destruction.

1.2 The six key principles relating to data processing

Six key Data Protection Principles are at the heart of all data processing and interlink with each other:

1. *Lawfulness*, *Fairness and Transparency*: You must make sure any personal data is processed lawfully, fairly and transparently. This includes:

- telling individuals about how you intend to use their data, which you must inform them about when you collect their data
- handling individuals' data only in ways they would reasonably expect;
- making sure you do not do anything unlawful with individuals' data;
- having legitimate grounds for collecting and using personal data.

The most common way of doing this is to obtain an individual's consent. Consent means an individual's freely given, specific, informed and unambiguous indication of their wishes by which that person, by a statement or some form of clear affirmative action, agrees to the processing of their personal data (so pre-ticked boxes, opt-outs or consent by default are not permitted). If you ask individuals to agree to the use of their data by third parties you must also say who those parties are. And, you must keep a record of consents, noting who consented, when, how and a copy of the exact consent request. Individuals must be told that they can withdraw their consent at any time, and it must be as easy for them to withdraw consent as it is for them to give it.

2. *Purpose limitation*: You can only collect personal data for specified, explicit and legitimate purposes. You must not process data in a way that is incompatible with those purposes. You need to be clear with individuals about the purpose(s) for which you hold their personal data so that you can then ensure that you process the data in a way that is compatible with your original purpose(s).

3. *Data minimisation*: You must make sure your use of personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) for which you process data. In practice you should identify the minimum amount of personal data you need to properly fulfil your purpose. You should not hold more personal data than you need. Nor should the data you hold include irrelevant details.

4. *Accuracy*: Make sure that your data is accurate and, where necessary, kept up to date. In practice this means: taking reasonable steps to ensure the accuracy of any personal data you obtain; ensuring that the source of any personal data is clear; carefully considering any challenges made by an individual to the accuracy of information; and, considering whether it is necessary to update the information.

5. *Storage limitation*: You mustn't keep data for longer than necessary. In practice this means: reviewing the length of time you keep personal data; considering the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it; securely deleting information that is no longer needed for this purpose or these purposes; and updating, archiving or securely deleting information if it goes out of date (for UK regulatory guidance about deleting personal data please see here). Generally-speaking it is for you to decide how long you will keep data, but please be aware that most countries have separate rules about certain personal data that must be kept for certain periods of time, e.g. with regard to tax records.

6. *Integrity and Confidentiality*: You must make sure personal data is processed securely including protection against unauthorised or unlawful data processing and against accidental loss, destruction or damage. In short, make sure that you use appropriate technical or organisational measures. In practice, this means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. You need to design and organise your security to fit the nature of the data you hold and the harm that may result from a security breach. You also need to make sure you have the right physical and technical security, backed up by robust policies and procedures and be ready to respond to any breach of security swiftly and effectively. There is no "one size fits all" solution to information security. The security measures that are appropriate for you will depend on your circumstances, so you should adopt a risk-based approach to deciding what level of security you need.

1.3 Managing breaches of data processing regulations

Generally speaking a data breach is any data security issue which exposes (or could expose) personal data. If there is a data breach (or a suspected one) it must be reported to a data protection regulator within 72 hours of becoming aware of the breach. In the event of a breach it is recommended that the data controller:

- prevents the further spread/loss of data; recover the data that has been lost;
- identifies risks arising from the breach;
- contacts appropriate parties – in addition to notifying a regulator the data controller may also need to inform the individuals who have been affected of the breach;
- prevents future breaches.

1.4 What rights do subjects have in relation to their data?

The data controller must tell people about the rights they may exercise with regard to their data. These are

a. *Subject Rights Access* – this means that an individual can seek to obtain confirmation as to whether or not personal data concerning them is being processed by a given data controller, where and for what purpose, and to be provided with a copy of that personal data free of charge;

b. *The Right to be Forgotten* (data erasure) – this means that an individual can seek to have personal data held by a given data controller erased, subject to certain conditions such as the data no longer being relevant to original purposes for processing, or where an individual has withdrawn their consent to processing that data;

c. *The Right to Rectification* – this means that an individual can seek to have personal data that a given data controller holds on them corrected without undue delay where the data concerning them is inaccurate;

d. *The Right to Restriction* – this means that an individual can seek to restrict a given data controller processing the personal data held on them, subject to certain conditions such as where the individual contests the accuracy of the data held on them for a period enabling the data contoller to verify the accuracy of the data in question;

e. *The Right to Object to Processing* – An individual can object to processing personal data that a given data controller holds on them where certain conditions apply which are so-called "legitimate interests" (i.e. not consent), including profiling. Where the data controller processes personal data for direct marketing purposes, the individual also has the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing. Note that under separate EU rules that sit alongside GDPR, individuals can object to direct marketing by a particular channel e.g. email or telephone; also note that ensuring that consent has been properly obtained for direct marketing is very important. Finally, an individual can also seek to "not be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

f. *The Right to Portability* – this means that an individual can receive the personal data concerning them which they have previously provided to a given data controller in a "structured, commonly used and machine-readable format" and have that data transmitted to someone else, subject to certain conditions such as where the individual consented to a given data controller processing their data.

g. *The Right to Lodge a Complaint with a Data Protection Regulator* – this means that an individual can make a complaint before a regulator about data protection issues concerning them. If this happened it would quite likely because an individual is not satisfied with the way a given data controller has dealt with their rights request.