Privacy Notice

This privacy notice discloses the privacy practices for Executive IP, LLC ("EIP"). This privacy notice applies to all information collected by Executive IP in connection with EIP's training programs. It will notify you of the following:

1. The personally identifiable information collected from you, how it is used, and with whom it may be shared.
2. The choices are available to you regarding the use of your data.
3. The security procedures in place to protect the misuse of your information.
4. How you can correct any inaccuracies in the information.

Information Collection, Use, and Sharing

EIP will only collect, store, and use information you provide us with voluntarily. EIP will only use your information in connection with our video-based training programs. EIP will not sell or rent your information to anyone. EIP will not share your information with any third party outside of our organization, other than as necessary to deliver you EIP's training programs and to store information related to your training activity. EIP may contact you via email in the future to deliver additional information to you about our training programs or about changes to EIP's privacy policy.

Your Access to and Control Over Information

You may opt out of any future contacts from EIP at any time. And, you can do the following at any time by contacting EIP via the email address or phone number given on our website:

- See what data (if any) EIP has about you.
- Correct any data EIP has about you (if it is incorrect).
- Request that EIP delete any data EIP has about you.
- Express any concern you have about EIP's use of your data.

Security

We use commercially reasonable precautions to protect your personally identifiable information both online and offline. When it's online, it's encrypted. When it's offline, we only provide access to your personally identifiable information to employees and contractors who need the information to perform a specific job and are bound by confidentiality. The computers/servers in which EIP stores personally identifiable information are kept in a secure environment. When personal data is deleted EIP does this safely such that the data is irrecoverable. Appropriate back-up and disaster recovery solutions are in place.

General Data Protection Regulation Compliance

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure

that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Lawful purposes

a. All data processed by the EIP must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The EIP shall note the appropriate lawful basis in its Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the EIP's systems.

Data minimisation

EIP shall ensure that personal data are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (providing you with EIP training programs and tracking your activity in connection with EIP training programs).

Accuracy

EIP shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / removal

To ensure that personal data is kept for no longer than necessary, EIP shall put in place an archiving policy for each area in which personal data is processed and review this process annually. The archiving policy shall consider what data should/must be retained, for how long, and why.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, EIP shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.