Welcome to Amplify-YP's Privacy Notice

This Privacy Notice is aligned to the General Data Protection Regulation (GDPR) and Data Protection Act 2018. These laws are defined in this notice as the **Data Protection Laws**.

This Privacy Notice applies to personal data collected by Amplify-YP. The Data Protection Laws applies to 'personal data', as defined by the Data Protection Laws, which means any information that relates to an identified or identifiable natural person. It does not include data that has been anonymised so that the individual can no longer be identified (anonymous data).

1. Important Information and who we are

Amplify-YP is a limited company registered in England and Wales (registered number 12207073).

Amplify-YP is a data controller under the GDPR. In delivering a service to you, we may work closely with other healthcare providers and with Investec PLC and Investec Wealth & Investment Limited who may also be independent data controllers of your personal data. We respect your privacy and are committed to operating the highest standards when it comes to protecting your personal data.

We will process your personal data "fairly", "lawfully" and "transparently". This means (i) we will be open and transparent about how personal data is used (ii) we will handle data in line with how we say we are going to handle data and (iii) we will only use or process personal data in accordance with the law. To fulfil these requirements, we set out in this Privacy Notice how Amplify-YP collects, uses, retains and discloses personal data. We also comply with applicable confidentiality guidelines published by regulators and professional bodies (e.g. The Health & Care Professions Council Confidentiality – guidance for registrants).

It is important that you read this Privacy Notice so that you understand how and why we are collecting and/or processing personal data about you. If you have any questions, please contact us at the address provided below.

Data Protection Officer

Amplify-YP has appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO at:

Email address: enquries@amplify-yp.com

Postal address:

10 Wellington Street, Cambridge, CB1 1HW

Telephone number: 0330 027 2180

2. How is Personal Data Collected?

Amplify-YP is contracted by Investec UK to provide an Emotional and Psychological Wellbeing service to Investec UK staff. To provide this service we collect information about you which includes personal information about you and about your health and wellbeing. We collect your personal data in a number of ways. These include:

i. *Direct interactions.*
You may give us your identity and contact data by filling in forms or by corresponding with us by post, phone, email, online or otherwise.

ii. *Investec HR department, Investec manager, Investec colleagues, other health care professionals, health care providers.*
Your manager, HR department or colleague may share correspondence with us (i.e., refer you to our service) on your behalf about your emotional or psychological wellbeing - we may contact you for this reason. If you do not agree to receiving the service when we contact you, we will close the referral and delete your referral.

iii. *Others who are involved in meeting your wellbeing needs*
To effectively support and coordinate your ongoing wellbeing needs, and with your expressed permission (see section 4 below), Amplify-YP will collect information from and/or share information with healthcare professionals, private medical insurance providers and other health care providers about your care and wellbeing needs.

3. The Data we collect about you

We may collect, use, store and transfer different kinds of personal data about you, which we have grouped together as follows:

i. *Identity*
This may include your name and age.

ii. *Contact details*
This may include your address, e-mail address and phone number(s), and place of work.

We also process the following special categories of *sensitive personal data:*

iii. *Information about your physical and mental health and patient records:*
Information about your physical and mental functioning, any ailments, diseases or disabilities and health data.

iv. *Other sensitive data:*
This may include, race or ethnicity, religious or philosophical beliefs, political opinions, sex life, sexual orientation and, sometimes, information about criminal offences (if relevant to your wellbeing).

These special categories of sensitive personal data are subject to a higher level of protection.

If you fail to provide personal data

Where we need to collect personal data to perform the terms of the service we are contracted to provide to you, and you fail to provide that data when requested, we may not be able to provide the service.

4. How we use personal data and our legal basis for processing

We may process your data in the following ways:

What we do	Lawful basis
Use the data provided in referrals, webforms and face-to-face requests provided by the Investec employee or from an Investec representative (e.g. their manager or HR) on their behalf	GDPR Article 6(1)(b) {performance of a contract} - when the Investec employee or representative provides us with their personal data or that of a relative, for instance to obtain advice and signposting, this is a necessary step to take at the request of the data subject entering into a contract.
Provide our core services of the Emotional and Psychological Wellbeing services: - Advice & Signposting - Case management - Claims and referral advocacy - Brief emotional containment work	GDPR Article 6(1)(b) {performance of a contract} - In providing the core services we are performing the contract with you, our data subject. GDPR Article 6(1)(a) {Consent} – we need consent from the Investec employee to advocate on their behalf with their employer, medical insurance claims and referrals to care and wellbeing services (e.g., to the NHS) GDPR Article 9 (2)(h) – {medical diagnosis, the provision of health or social care treatment or management of health or social care systems or a contract with a health professional} in order to provide emotional containment, preventative advice and support access to appropriate healthcare
Contact Investec employee regarding the services we provide	GDPR Article 6(1)(f) {legitimate interests} - we may contact the Investec employee for our legitimate interests so that we can gather more information for the provision of our services, or to deliver those services most effectively; for example, to request the employee completes a customer service satisfaction survey.
Responding to complaints	GDPR Article 6(1)(b) {performance of a contract} - In responding to complaints we are performing the contract with you, our data subject.
Retain personal data under our data retention policy after the work with the Investec employee has ended	GDPR Article 6(1)(f) {legitimate interests} - we need to retain the Investec employee's personal data for only as long as necessary under the law to protect our legitimate interests. This includes providing Investec anonymised aggregate data on activity and performance and using such aggregate data to provide analytical insights.
Report a crime, a significant risk to self or risk to others or comply with a legal investigation. .	GDPR Article 6(1)(c) {compliance with legal obligations} - we must comply with our legal obligations GDPR Article 6(1)(d) {Protect the vital interests of the data subject or of another living person} - we may need to share information to protect your life or the life of someone else if the person does not have capacity to make that decision; for example, the person

	is mentally incapacitated and we cannot rely on another lawful basis for sharing.

We may also process your data for the establishment, exercise or defence of legal claims; and in some cases, with your consent.

Please contact the Amplify-YP Data Protection Manager if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table above.

5. Do I have to consent to the processing of my data?

Health data is data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's health status.

The conditions under which we seek consent are listed under section 4.

Amplify-YP will also comply with clinical confidentiality guidelines (such as the Health & Care Professions Council) in relation to the sharing of any health records.

6. Confidentiality and patient's records

In addition to the protections under the Data Protection Laws, your health data are also subject to the Common Law Duty of Confidentiality.

In receiving the referral we assume consent under common law – whether expressed or implied (implied consent means that the subject knows or would reasonably expect the proposed use or disclosure and has not objected)

We may be authorised or required by law, for example under statute, common law (including duty of care) or legal proceedings to share information with statutory authorities. There may also be an overriding public interest, for example where a person is contagious, or the public is at risk, such that there is a public interest in disclosure that overrides the public interest in maintaining confidentiality.

7. Change of Purpose

We will only use your personal data for the purposes described in this Privacy Notice. If we need to use your personal data for an unrelated purpose, we will update this Privacy Notice and notify you in accordance with the Data Protection Laws.

8. Cookies

Cookies are small text files that are placed on your computer, smartphone or other device when you visit our website. We may use cookies in order to improve our services and optimise our website.

For more information about cookies, including how to view the cookie that have been set and how to manage or delete them, please visit www.allaboutcookies.org.

9. Data Anonymisation and Aggregation

As outlined in section 4 above, your personal data may be converted into statistical or aggregated data which cannot be used to identify you, and then used to produce statistical research and reports. This aggregated data may be shared and used in all the ways described above.

10. Children

We understand the importance of taking extra precautions to protect the privacy and safety of children. In some situations we may collect information provided to us about family members of referred employees if it is relevant to the wellbeing referral.

If you are a parent or guardian and would like to access, correct, delete or exercise any of your child's data protection rights, please contact us using the contact details provided in section 1 above. We may need to ask you additional information to confirm that you are the child's parent or guardian.

11. Disclosure of Personal Data

Third party recipients

We may have to share your personal data for the purposes set out in in section 4 above with:

i. those involved in your care, such as: your private health insurance provider, healthcare professionals; NHS providers; private therapists

ii. suppliers acting as data processors who provide IT and systems administration services; we use the following data processors:
   a. Google -(G Suite) for email, calendar, contacts, word processing, online feedback forms and statistical analytics.
   b. Pipedrive - The cloud CRM system is used to store our appointment, contact and activity data
   c. Tutanota - an end-to-end encrypted email solution for communicating sensitive data with others such as Investec employees; e.g., their health data
   d. Wix - for online appointment scheduling and website hosting
   e. Toll Free Forwarding - a virtual call forwarding system to route inbound phone call enquiries through a single phone number to our staff
   f. tawk.to - provider of live web chat support & messaging application
   g. Whereby - secure video calling platform
   h. Signal Private Messenger - end-to-end encryption messaging and video calling app

iii. statutory authorities where it is required by law or by others under or as permitted by law and

iv. with our legal and other professional advisors including our solicitors.

In most cases, we will seek your consent to make a referral to another organisation or advocate on your behalf. An exception, for example, will be with the NHS if an emergency referral is required and you do not have mental capacity to make a decision about your own care and treatment needs.

We will not by default share your personal health information with your employer without your consent, and assuming your employer does not already have this information. If we are seriously concerned about your welfare and feel your employer needs to know we will encourage you to share this information with your employee in the first instance. If the concern is related to an imminent and severe risk to self or others, we will make a clinical judgement as to whom to disclose the information under GDPR Article 6(1)(c) or GDPR Article 6(1)(d).

We require all third parties who process data on our behalf to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may share your personal data with more parties than the ones listed above. Should this be the case, we will inform you of the change in accordance with applicable laws and regulations

Transfers of personal data outside the European Economic Area (EEA)

Your personal data may be transferred outside the UK and the European Economic Area for the purposes set out above. While some countries have adequate protections for personal data under applicable laws, in other countries steps will be necessary to ensure appropriate safeguards apply to it. These include imposing contractual obligations or other safeguards to provide adequate levels of protection.

12. Data Security

At Amplify-YP we take our duty to protect personal data and our confidentiality obligations seriously. We are committed to taking all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper.

Amplify-YP has also appointed a **Data Protection Manager** (DPM) who has professional experience and knowledge of data protection law, specifically in relation to the type of processing that Amplify-YP carries out.

Everyone who works for us is required to undertake annual information governance and cybersecurity training and is provided with information governance and acceptable usage (of IT equipment) policies that they are required to read, understand and agree to follow. Amplify-YP's policies ensure the healthcare professionals who provide our services are aware of their information governance responsibilities and follow best practice guidelines ensuring the necessary safeguards and appropriate use of person-identifiable and confidential information.

Additionally, everyone working for Amplify-YP is subject to the common law duty of confidentiality. Information provided in confidence will only be used for the purposes advised and consented to by the service user, unless it is required or permitted by the law.

We have put in place appropriate security measures, including encryption and using anonymisation or pseudonymisation processes where necessary, to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your

personal data to those Amplify-YP employees, agents, contractors and other third parties on a "need to know" basis. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach in accordance with applicable laws and regulations.

Data Protection Impact Assessment (DPIA)

We carry out DPIAs on processing that is likely to result in high risk to individuals to help identify and minimise data protection risks.

If you would like a copy of a DPIA that we have carried out, please contact our DPM.

13. Data Retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting/analytics requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Details of retention periods for different aspects of your personal data are available in our retention policy which you can request by contacting our DPM.

14. Your Legal Rights

You have the following rights under Data Protection Laws in relation to your personal data.

Request access to your personal data. The Data Protection Laws gives you certain rights to see the information that Amplify-YP holds about you and why.

We will confirm whether we are processing your personal data and we will provide you with additional information including what type of data we have, where we collected it from, whether we send it to others, including any transfers outside the EEA, subject to the limitations set out in applicable laws and regulations. We will provide you free of charge with a copy of your personal data, but we may charge you a fee to cover our administrative costs if you request additional copies of the same information.

Request correction of your personal data. You can ask us to correct any incomplete or inaccurate data we hold about you, although we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. You can ask us to delete or remove personal data where there is no good reason for us continuing to process it. However, that we may not always be able to comply with your request of erasure for legal reasons, and we will let you know if this is the case, at the time of your request.

Object to processing of your personal data. You can object to the processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on

your fundamental rights and freedoms. However, that we may not always be able to comply with your request for legal reasons, and we will let you know if this is the case, at the time of your request.

Request restriction of processing your personal data. You can ask us to restrict the processing of your personal data in certain cases.

Request transfer of your personal data. You can ask us to transfer your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Please note this right only applies in certain cases.

Right to withdraw consent. You can withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to or for you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact the DPO. Contact details are above. We may ask you to provide additional information e.g. your full name, address, date of birth, etc. so that your identity can be verified.

No fee usually required

You will not have to pay a fee to exercise any of your above rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

In so far as it is practicable, we will notify the third parties we shared your personal data with of any correction, deletion, and/or limitation on processing of your personal data.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you of the reasons for the delay and keep you updated.

15. Questions?

If you have any questions about our Privacy Notice, information we hold about you or complaints about how we process your personal information please contact the DPM (contact details above). Complaints can also be made to the Information Commissioner's Office, the UK supervisory authority for data protection issues (www.ico.org.uk).

16. Changes to our Privacy Notice

We keep our fair processing notice under regular review and we will place our updated Privacy Notice in a visible place. This notice was last updated on 28 January 2020.