



DR ANDREAS VASSILIOU

Counselling Psychologist | Existential Psychotherapist

PRIVACY NOTICE

For website visitors, enquiry contacts, therapy clients and clinical supervisees

Version 2.0 | Last updated: 15 August 2026

This notice explains how I collect, use, disclose, retain and protect personal data in connection with my website, enquiries, psychotherapy services and clinical supervision. It also explains the rights available to you under data protection law.

This notice is provided for transparency; it is not a consent form. Where I rely on consent for a specific, optional use of information, I will ask for that consent separately.

Who I am and how to contact me

I, Dr Andreas Vassiliou, am the data controller for the personal data described in this notice. This means that I determine why and how that personal data is processed. I practise in Larnaca and Nicosia, Cyprus, and provide some services online.

Email: vassiliou@cyprus-psychotherapy.com

Telephone: Cyprus +357 96433000 | United Kingdom +44 7832 650404

Website: www.cyprus-psychotherapy.com

My processing is principally governed by the EU General Data Protection Regulation (EU GDPR) and the Cyprus Law Providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of Such Data, Law 125(I)/2018. Where applicable, the UK GDPR and the UK Data Protection Act 2018 may also apply. I am registered with the UK Information Commissioner's Office (ICO), registration number ZA524887.

Who this notice covers

This notice covers personal data relating to:

- people who visit the website or submit the contact form;
- people who contact me to enquire about therapy or supervision;
- individual psychotherapy clients, including adolescents where applicable;
- both participants in couples therapy; and
- clinical supervisees and people enquiring about supervision.

It does not describe how an insurer, Employee Assistance Programme (EAP), referring organisation or another independent professional processes information for its own purposes. Those organisations should provide their own privacy information.

How this notice is provided

The current version is available through the Privacy Notice link on my website. When I collect personal data directly from you, I will draw your attention to this notice at or before the point of collection – for example, through the contact form, my first substantive response to an enquiry, or the information provided when therapy or supervision begins.

If I receive your personal data from another source, such as an insurer, EAP, parent or guardian, I will provide or draw your attention to the relevant privacy information within the period required by law – normally by the first communication with you and no later than one month – unless a lawful exception applies. A paper copy or an alternative accessible format is available on request.

Personal data I may process

I collect only information that is relevant to the purpose for which it is needed. Depending on the nature of our contact, this may include:

- identity and contact details, including name, postal address, telephone number, email address and communication preferences;
- information included in an enquiry, intake form, referral or initial discussion;
- appointment, attendance, cancellation, fee, invoice, payment and accounting information;
- emergency-contact and GP or family-doctor details, where provided;
- insurer or EAP referral, policy, authorisation and funding information;
- clinical information supplied by you or created in the course of therapy, including clinical notes, assessments, correspondence, reports and outcome measures where these are used;
- information concerning physical or mental health, relationships, family circumstances, personal history, medication, risk, and other matters discussed because they are relevant to the work;
- other special-category information that may arise in therapy, such as information revealing racial or ethnic origin, religious or philosophical beliefs, sex life or sexual orientation;
- for couples therapy, information concerning either participant, the relationship and other people mentioned in the work;
- for work with adolescents, information relating to the young person and, where relevant, parents, guardians, schools, referrers or other professionals;
- for clinical supervision, professional and registration details, supervision agreements, attendance and fee records, supervision notes and clinical material brought for discussion;
- online-session information, such as meeting links, account identifiers and basic connection metadata; and
- website and contact-form data, which may include IP address, browser or device information, security logs, cookie identifiers and the content of messages submitted through the website, depending on the website settings and services in use.

Clinical notes are kept to support safe, ethical and coherent practice. Where practicable, I separate identifying details from clinical notes and use a client code. Coded or pseudonymised information remains personal data if it can be linked back to a person.

I do not routinely make audio or video recordings of therapy or supervision sessions. Any recording would require a separate, explicit prior agreement, a defined purpose and a specified retention period.

Where personal data comes from

Most personal data is obtained directly from you, including through:

- the website contact form, email or telephone;
- intake documents, questionnaires or other forms;
- therapy or supervision sessions; and
- correspondence and administrative communications.

I may also receive personal data from:

- an insurer, EAP, employer, training organisation or other funding or referring body;
- a parent or guardian, where work with a young person is being considered or provided;
- the other participant in couples therapy;
- a GP, health professional or other professional, where there is an appropriate basis for communication; and
- website, email, video-conferencing and IT service providers that generate technical or security information.

Clinical material brought to supervision should be anonymised or pseudonymised as far as practicable. Supervisees should avoid sharing directly identifying information unless it is necessary, proportionate and lawfully authorised.

Why I use personal data and the lawful bases

Data protection law requires a lawful basis under Article 6 of the GDPR. Where the information includes health data or another special category of personal data, an additional condition under Article 9 is also required. The basis used depends on the particular purpose and circumstances.

Purpose	Lawful basis and explanation
Enquiries and arranging services	To respond to an enquiry, consider whether I can offer an appropriate service, arrange an initial discussion and take steps at your request before a contract. Article 6(1)(b) (steps before entering into a contract) and, for basic practice administration and security, Article 6(1)(f) (legitimate interests). If an enquiry contains health information, Article 9(2)(h) may apply in connection with assessing or providing treatment under professional confidentiality.
Providing therapy or clinical supervision	To provide the agreed service, manage appointments and fees, communicate with you, maintain appropriate records and support safe and ethical practice. Article 6(1)(b) (performance of a contract) and, where necessary, Article 6(1)(f) (legitimate interests). For health and clinical data, Article 9(2)(h) (health care or treatment, including relevant professional supervision, under responsibility and confidentiality of a health professional).

Purpose	Lawful basis and explanation
Clinical records, risk and coordination	To maintain clinical continuity, consider risk, respond appropriately to urgent circumstances and, where appropriate, coordinate with another professional. Article 6(1)(b), 6(1)(c) where a specific legal obligation applies, 6(1)(d) in a qualifying vital-interests emergency, or 6(1)(f). Relevant Article 9 conditions may include 9(2)(h), 9(2)(c) where a person is incapable of giving consent in a life-threatening situation, or 9(2)(f) for legal claims.
Fees, invoices and accounts	To administer payments, keep accounts and comply with tax and financial obligations. Article 6(1)(b) (contract) and Article 6(1)(c) (legal obligation). Any clinical information included in financial records is kept to the minimum necessary.
Insurer or EAP arrangements	To confirm eligibility or authorisation, administer funded sessions and provide the minimum information required under the relevant arrangement. Article 6(1)(b) and/or Article 6(1)(f), with Article 9(2)(h) for relevant health information. I use consent where a disclosure is genuinely optional and consent is the appropriate basis.
Optional disclosures requested by you	For example, sending information to a GP, solicitor or another professional at your request. Article 6(1)(a) (consent) and, where special-category information is involved, Article 9(2)(a) (explicit consent), unless another lawful basis is more appropriate. Consent may be withdrawn at any time for future processing based on it.
Complaints, regulation and legal claims	To respond to a complaint, cooperate with a regulator or professional body, obtain legal advice, or establish, exercise or defend legal claims. Article 6(1)(c) where a legal obligation applies and/or Article 6(1)(f) (legitimate interests); Article 9(2)(f) for special-category data necessary for legal claims.
Website operation and security	To operate and protect the website, prevent misuse and respond to contact-form enquiries. Article 6(1)(f) (legitimate interests). Where consent is legally required for non-essential cookies or analytics, Article 6(1)(a) applies and the relevant choice should be provided through the website.

Where I rely on legitimate interests, those interests include operating a safe and secure professional practice, maintaining appropriate records, communicating effectively, meeting professional standards, preventing misuse and establishing or defending legal claims. I consider whether the processing is necessary and proportionate and whether your rights override those interests.

What happens if you do not provide information

You are not required to provide more information than is reasonably necessary. However, I need sufficient identity, contact, administrative and relevant clinical information to respond to an enquiry, assess whether I can offer a service and provide that service safely. If necessary information is not provided, I may be unable to arrange or continue therapy or supervision. Emergency-contact and GP details are normally voluntary unless there is a particular clinical, contractual or legal reason for requesting them. Non-essential website cookies or analytics, where used, are optional.

Who I may share personal data with

I do not sell personal data and do not share it for direct marketing. I disclose only what is necessary for the relevant purpose. Depending on the circumstances, recipients may include:

- an insurer or EAP funding sessions, where it requires limited attendance, authorisation, billing or other agreed information;
- a GP, psychiatrist or other health professional, at your request or where there is an appropriate clinical and lawful basis;
- professional supervisors or consultants, using anonymised or pseudonymised information wherever practicable and subject to confidentiality;
- providers supporting the website, email, online sessions, data storage, backup and IT security. These may include Wix for the website and contact form, Google email services and Zoom for online sessions;
- banks, payment providers, accountants, bookkeepers and tax authorities, to the limited extent necessary for payments and financial compliance;
- a professional indemnity insurer, legal adviser, regulator or professional body where necessary in connection with a complaint, regulatory matter or legal claim; and
- emergency services, safeguarding bodies, courts or public authorities where disclosure is required or permitted by law, or is necessary and proportionate to protect life or respond to a serious risk.

Service providers may act as data processors on my instructions or as separate controllers for particular activities. Where required, I use contractual and confidentiality arrangements appropriate to their role. My professional duty of confidentiality remains relevant in addition to data protection law.

Particular contexts

Confidentiality

Confidentiality is central to therapy and supervision, but it is not absolute. The therapeutic or supervision agreement explains the relevant limits and how concerns about serious risk, safeguarding, legal requirements or professional complaints may be handled. Any disclosure is considered carefully and limited to what is necessary.

Young people

When I work with a person under 18, I explain in language appropriate to their age and understanding what information I keep, why I keep it, who may receive it and what their rights are. The involvement of a parent or guardian depends on the young person's age, understanding, the applicable law and the therapeutic framework agreed at the outset. I do not routinely disclose the content of sessions to a parent or guardian, although I may need to act where there is a serious concern about safety or a legal obligation. Wherever possible, this is discussed with the young person.

Couples therapy

A couples-therapy record may contain personal data about both participants and other people mentioned in the work. Each participant has rights in relation to their own personal data, but not an automatic right to receive the other person's personal data. Information may therefore be withheld or redacted where necessary to protect another person's rights and confidentiality. The handling of individual emails or communications is considered within the therapeutic framework agreed for the couple.

Clinical supervision

I keep proportionate records of the supervision provided, including administrative details and brief supervision notes. Clinical material should be anonymised or pseudonymised as far as possible. If identifiable clinical information is received, it is treated as confidential special-category data and protected accordingly. Supervisees remain responsible for their own data-protection and confidentiality obligations in relation to material they bring to supervision.

International data transfers

Some technology providers may store, access or process personal data outside Cyprus, the European Economic Area (EEA) or the United Kingdom. This may occur, for example, in connection with website hosting, email, online sessions, cloud storage, security or technical support.

Where data protection law treats this as an international transfer, I take steps to ensure that an appropriate transfer mechanism and safeguards are in place. Depending on the destination and provider, these may include an adequacy decision, the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or UK Addendum, together with additional measures where appropriate. Information about the applicable safeguard, and a copy where legally available, may be requested using the contact details above.

How I protect personal data

I use technical and organisational measures appropriate to the sensitivity of the information and the risks involved. These include, as applicable:

- password-protected devices and accounts, device-locking and access controls;
- software and security updates and protection against malicious software;
- secure physical storage for paper records;
- separating identifying information from clinical notes where practicable;
- data minimisation and restricted access;
- careful selection of service providers and appropriate contractual safeguards; and
- secure deletion or destruction when the relevant retention period ends.

No method of electronic communication or online storage can be guaranteed to be completely risk-free. Please avoid including extensive or unnecessary clinical detail in the website contact form or routine email. If a more secure method is appropriate for particular information, this can be discussed.

How long I keep personal data

I retain personal data only for as long as it is reasonably needed for the relevant purpose and to meet applicable legal, tax, insurance and professional requirements. My standard retention periods are:

Record type	Standard retention period
Enquiries that do not lead to a service	12 months after the last substantive contact.
Adult individual and couples-therapy records	7 years after the final session or clinical contact.
Records relating to a client under 18	Until age 25, or 7 years after the final session or clinical contact, whichever is later.
Clinical-supervision records	7 years after the final supervision session or contact.
Appointment diary and routine non-financial administration	Normally 2 years after the last contact, unless the information forms part of a clinical, supervision, accounting or legal record retained for longer.
Routine emails and messages	Deleted when no longer needed and normally within 12 months. Clinically or professionally significant correspondence may be incorporated into the relevant record and retained for the period applying to that record.
Invoices and accounting or tax records	7 years after the end of the relevant tax year, or for any longer period required by applicable law.
Website and technical security data	For the shortest period necessary for website operation, security and troubleshooting, after which the data is deleted or anonymised in accordance with the relevant provider settings and retention controls.

A record may be retained for longer where there is an active complaint, safeguarding concern, regulatory process, legal claim, court order or another documented lawful reason. It may be deleted earlier where the purpose has ended and no legal or professional reason requires continued retention. Backup copies may remain for a limited period before being securely overwritten.

Your data-protection rights

Depending on the circumstances and the lawful basis used, your rights may include:

- the right to be informed about how your personal data is used;
- the right to request access to your personal data;
- the right to ask for inaccurate or incomplete information to be corrected;
- the right to ask for erasure in circumstances where the law provides that right;
- the right to ask for processing to be restricted in certain circumstances;
- the right to data portability for certain data processed by automated means on the basis of consent or contract;
- the right to object to processing based on legitimate interests, taking account of your particular situation;
- the right to withdraw consent at any time where consent is the basis for a specific activity, without affecting earlier lawful processing; and
- the right to lodge a complaint with a data-protection supervisory authority.

I do not use personal data to make solely automated decisions, including profiling, that produce legal or similarly significant effects.

These rights are not absolute. For example, information may need to be retained to comply with an obligation or defend a legal claim, and access may be limited where disclosure would adversely affect another person's rights and confidentiality or where another legal exemption applies.

To exercise a right, contact me using the email address above. I may ask for information needed to verify identity. I will respond without undue delay and normally within one month. Where permitted by law, that period may be extended by up to two further months because of complexity or the number of requests; if so, I will explain this within the initial month. There is normally no fee, although a reasonable fee may be charged, or a request refused, where it is manifestly unfounded or excessive or where additional copies are requested.

Questions and complaints

You are welcome to contact me with any question or concern about personal data. You are not required to contact me before approaching a supervisory authority.

Cyprus

The competent authority in Cyprus is the Office of the Commissioner for Personal Data Protection:

Address: 15 Kypranoros Street, 1061 Nicosia, Cyprus; P.O. Box 23378, 1682 Nicosia

Telephone: +357 22818456

Email: commissioner@dataprotection.gov.cy

Website: www.dataprotection.gov.cy

United Kingdom

Where UK data-protection law applies, you may also contact the Information Commissioner's Office (ICO): www.ico.org.uk

Under the EU GDPR, you may also have the right to complain to a supervisory authority in the EU or EEA country of your habitual residence, place of work or the place of the alleged infringement.

Changes to this notice

I review this notice periodically and update it when my practices, service providers or legal obligations change. The current version and revision date will be available through the Privacy Notice link on my website. If a material change affects how I use the personal data of current clients or supervisees, I will bring it to their attention before beginning the new use where required.

Alternative formats

If you would find this notice easier to use in another format or language, please contact me. A paper copy can also be provided.