PRIVACY POLICY FOR EAP CLIENTS

CIC appreciates the trust you place in us when sharing your personal data. The security of that data is very important to us. This privacy policy explains how we collect, use and look after your personal data.

We will explain what rights you have with regards to your personal data and how you can exercise those rights.

WHO WE ARE

CNLR is a limited company and trades under the name of CiC. We provide employee assistance programmes to organisations which includes services to be utilised by employees, such as 24/7 Advice Line and counselling support. We offer international services such as global trauma support and peer and professional support programmes and critical incident support. We also offer mediation, training and coaching sessions.

COLLECTION OF PERSONAL DATA

Definitions:

For the purposes of this policy CiC is the Data Controller and:

- A customer is the legal entity (e.g. the company that employs you) we contract with;
- A client includes the employee, partner of an employee or family member of an employee belonging to the customer we contract with;
- An affiliate is a contractor who delivers our counselling and support services on our behalf;
- Third party professional services are a third party that we share your data with in order to deliver critical services to you e.g. GPs and other medical professionals or legal advisors;
- Third party processors are third party service providers who undertake data processing activities on our behalf e.g. IT support services.

LAWFUL BASIS FOR PROCESSING OF PERSONAL DATA

It is necessary to process certain information about you in order to provide you with the best possible support and care. By using our services you have a reasonable expectation that your personal information will be processed.

Table 1 below provides information about what personal data we process about you, the purpose for the processing and the lawful basis for doing so and who the data is shared with. This information is stored in our secure clinical database. We have processes in place to ensure that only those people in our organisation who need to access your data can do so. A number of data sets are collected for multiple purposes, as the table below shows. Some data may be shared with third parties and, where this happens, this is also identified below.

When we process on the lawful basis of legitimate interest, we apply the following test to determine whether it is appropriate:

The purpose test – is there a legitimate interest behind the processing?

Necessity test – is the processing necessary for that purpose?

Balancing test – is the legitimate interest overridden, or not, by the individual's interests, rights or freedoms?

TABLE 1

Data processed	Purpose for processing	Lawful basis	Data is shared with
First Name Last Name Company Work address Home address Email address	Counselling service: to provide and manage the services you, the client, has requested under the contract between CiC-EAP and the organisation you work for.	**Contractual obligation:** To carry out our contractual agreement to provide you (the client) with the services you have self-referred to or been referred to.	Internally but access is restricted to those who require access and only for a specific purpose e.g. Adviceline, Affiliate Counsellors and Clinical Team.

Telephone number Attendance data		**Legitimate interest:** where it is in our legitimate interests to do so, to manage our client relationship and provide a high level of service.	Attendance data may be shared with your organisation if required under contract. We store client data in our secure CiCiS database.
Case notes – counselling sessions and other support	To provide and manage the support service you, the client, has requested under the contract between CiC-EAP and the organisation you work for.	**Legitimate interest:** Where it is in our legitimate interest to provide ongoing support and ensure the client's safety i.e. onward referral - vital interest or medical intervention.	Internally but access is restricted to those who require access and only for a specific purpose e.g. Adviceline, Affiliate Counsellors and Clinical Team.
Case notes which may include special category data (see definition below)	To provide and manage the counselling services you, the client, has requested, we give an assigned affiliate counsellor access to your data through our secure portal.	**Legitimate interest:** to maintain adequate case notes in order to provide the most relevant and appropriate service, care and support.	Internally e.g. Adviceline and shared with the assigned affiliate counsellor and clinical team.
Case notes which may include special category data (see definition below)	To provide and manage the counselling services you, the client, has requested or been	**Legitimate interest:** to maintain adequate case notes in order to provide the most relevant and appropriate service, care and support.	Affiliate counsellor assigned to your case and may be shared with

	referred to, the assigned affiliate counsellor will maintain confidential case notes of your discussions and support. Affiliate Counsellors will upload case notes from counselling sessions to your client record in our CiCiS database through a secure portal and are required under contract to securely destroy any local records they have made.		other appropriate members of the clinical team where there is a need for further support.
First Name Last Name Work address Home Address Date of birth Clinical reason for referral, may include health data.	To refer you, the client, on to professional services e.g. a GP, psychiatrist. Solicitor, (where the details have been provided by you), to make recommendations for further support. To transmit case notes when requested by a solicitor or the physiatrist or Police. In critical situations this could be verbal.	**Consent:** with your consent unless: • there is a risk of harm to you or other people i.e. vital interest or medical intervention • the courts have made a formal order in relation to a court case • there is a legal requirement we must comply with.	Internally e.g. Adviceline and with the GP, psychiatrist or solicitor etc. Will be shared with the assigned affiliate counsellor or other third party professional service if required.
First Name Last Name Work address	To refer on to emergency services e.g. police, hospital emergency	**Consent:** with your consent unless: • there is a risk of harm to you or other people i.e. vital interest or medical intervention	Internally e.g. Adviceline, Clinical Team, and

Home Address Date of birth Reason for requesting emergency support which may include health data.	where there is a risk of harm to you, the client, or others. To transmit data when requested by the emergency services. In critical situations this could be verbal.	• the courts have made a formal order in relation to a court case • there is a legal requirement we must comply with.	externally with the emergency services. May be shared with your affiliate counsellor or other third party professional service if required e.g. GP.
First Name Last Name Company/Employer Address Content of call	To collect details of a call to the adviceline. The call data is collected in adviceline counsellor notebooks. Notes are shredded immediately they are finished with.	**Legitimate interest:** to maintain adequate case notes in order to provide the most relevant and appropriate service, care and support.	Adviceline
First Name Last Name Company/Employer Address Content of call	To collect details of a call to the adviceline. Notes from the call to Adviceline are entered into our secure CiCiS database.	**Legitimate interest:** to maintain adequate case notes in order to provide the most relevant and appropriate service, care and support.. **Vital interest** – to assess if onward referral is required to a third party e.g. medical intervention.	Internally and may be shared with the assigned affiliate counsellor or other third party professional service if required.
Equality and Diversity Data Gender, age, Disability, marriage and civil partnership,	Adviceline collects equality and diversity data to enable the monitoring and evaluation of the	**Consent:** your consent to collect this data is requested at the beginning of the call to the Adviceline.	Internally with assigned affiliate counsellor and clinical team.

pregnancy and maternity, race, religion, sexual orientation and gender reassignment	uptake of services by customers based on their protected characteristics under the Equality Act 2010. The data is anonymised, and analytics provided to the customer organisation (if required by contract) and CiC to inform decision making to improve inclusivity. This data may also be used to identify if the customer would benefit from an affiliate counsellor with specific training and experience in a protected characteristic.	**Contractual obligations:** To carry out our contractual obligations to provide anonymised inclusivity data where the client contract requires it.	Anonymised analysis data is shared with the customer organisation.
First Name Last Name Company/Employer Address Telephone number Reason for call	Connect Assist: To provide an out of hours call answering service. Data is entered directly into the secure CiCiS database.	**Contractual obligation:** to carry out our contractual obligation to provide a 24 hour service. **Legitimate interest:** to maintain adequate case notes in order to provide the most relevant and appropriate service, care and support.	Third party service provider – Connect Assist and with affiliate counsellor who provides support.

		Vital interest – to assess if onward referral is required to a third party e.g. medical intervention.	

SPECIAL CATEGORY DATA

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection

Special category data is defined under GDPR 2016 Article 9 as personal data revealing ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Health data is collected as part of case notes and is necessary in order to provide the most appropriate care and support service to you. Therefore, as a client you have a reasonable expectation that special category data must be processed in order to receive the care and support service. The lawfulness of processing health data for this purpose is based on GDPR Article 6 (b) and Article 9 (b) and DPA 2018 Schedule 1 (1).

We only collect special category data that falls within the equality and diversity data listed in Table 1 for the purposes recorded. We only collect equality and diversity data with your consent.

THIRD PARTIES SERVICE PROVIDERS WHO WE MAY SHARE YOUR DATA WITH OR WHO COULD POTENTIALLY HAVE ACCESS (AS DEFINED IN TABLE 1)

- **Government and law enforcement agencies:** We may be required by law to share your data with other organisations, such as government or law enforcement agencies:
    - to satisfy any applicable law, regulation, legal process, or governmental request;
    - to detect, prevent, or otherwise address fraud, security, or technical issues;
    - protect our rights, property or safety, our users and the public.

    This may include exchanging information with other companies and organisations for fraud protection and spam/malware prevention if required by law.

- Professional advisors including lawyers, bankers, auditors and insurers.

  Third parties to whom we sell, transfer, or merge parts of our business or our assets.

If we do share data with third parties, we always do so securely, and we won't share more than we need to.

- Service providers who provide IT and system hosting services that could be defined as 'data processors' under Data Protection Legislation. Generally, these service providers do not have access to data but as they host or manage the servers on which the data resides there is potential, in exceptional circumstances, that the data could be accessed e.g. during disaster recovery. All such service providers are thoroughly vetted and have stringent access controls in place.

Our service providers: we have listed in Table 2 service providers who are providing services that makes them 'processors' as defined by GDPR 2016. We will always ensure they follow similarly high standards to CiC and are bound by contractual confidentiality, data protection and information security requirements.

TABLE 2

Service provider	Purpose of processing	Link to Privacy Policy
Mailchimp	Provides marketing mail portal	https://mailchimp.com/legal/privacy/?_ga=2.2884912.1025376997.1527161488-2091482877.1526982076
Connect Assist	Out of hours call centre	https://www.connectassist.co.uk/privacy-policy/
Workbooks CRM	Cloud based CRM	https://www.workbooks.com/sites/default/files/_assets/pdf/legal/privacy-notice.pdf
ACM Solutions	Manages the hosted virtual server for CiCiS. Developers for CiCis clinical database.	https://www.acm-solutions.co.uk/privacy.html

Our IT Department	Provides IT services. Manages IT infrastructure	https://www.ouritdept.co.uk/wp-content/uploads/2018/05/OurITDept-Privacy-Policy.pdf
Law Express	Provides legal advice	https://lawexpress.co.uk/privacy-policy
KTEG (Everyday Matters)	Personal Concierge Service	
True Bearing/ Bread & Butter Advice	Financial Guidance	https://www.truebearing.co.uk/data-security-policy/
PayPlan	Provides debt advice and solutions	https://www.payplan.com/legal/privacy-policy/

YOUR RIGHTS

The GDPR aims to give you more control of your data. It provides new and strengthened rights.

Right to access – you can ask us whether we're processing your personal data, including where and for what purpose. You can also request an electronic copy of your personal data free of charge. If you require further copies of the data there may be a charge where permitted by the legislation.

Right to restrict processing – in certain circumstances, you can ask us to restrict our use of your personal data.

Right to rectification – you can ask us to correct inaccurate personal data we hold about you.

Right to erasure (right to be forgotten) – in certain circumstances, you can ask us to erase your personal data.

Right to data portability – you can ask us to provide you with a copy of your personal data in a commonly used electronic format so that you can transfer it to other businesses.

Right to object to automated decision-making – in certain circumstances, you can ask us not to make automated decisions about you based on your personal data that produce significant legal effects.

Right to lodge a complaint – you can lodge a complaint with the supervisory authority ICO but we ask that you allow us to see if we can resolve the problem first (See complaints and queries section).

This means you can at any time:

- inform us of a correction to your personal data;
- withdraw any permission you have previously given to allow us to use your information;
- object to any automated decision-making;
- ask us to stop or start sending you marketing messages;
- ask us to send you (or someone you nominate) a copy of the information we hold about you;
- ask us to stop processing your information in certain circumstances.

DATA SUBJECT ACCESS REQUEST (DSAR)

You have the right to request a copy of the personal data we hold about you and to have any inaccuracies corrected. We will require you to prove your identity with 2 pieces of approved identification. We will use reasonable efforts consistent with our legal duty to supply, correct or delete personal information about you on our files.

We will need two copies of forms of identification, which can be: passport, driving licence, birth certificate, utility bill (from last 3 months), current vehicle registration document or a bank statement (from last 3 months). If you can advise of the specific information that you require, we can process your request more quickly. We will respond to your request within one month of you providing information that confirms your identity.

We will then give you a description of your data, why we have it, who it could be disclosed to and it will be in a format that you can access easily.

If you wish to make a DSAR request please contact us using the contact details at the end of this notice and we will provide you with the necessary request documents.

RETENTION OF YOUR DATA

We will only retain your personal data for a period of time that is calculated depending on the type of personal data and the purposes for which we hold that data. We will keep your data in line with our retention of records schedule. We are required to retain case records for seven years after our relationship with you has ended, unless there is a legal reason for keeping them longer (e.g. an ongoing legal claim).

We retain information that enables us to:

- maintain business records to comply with our contractual obligations
- comply with record retention requirements under the law and our professional code of conduct.
- defend or bring any existing or potential legal claims
- maintain records of anyone who does not want to receive marketing from us
- deal with any future complaints regarding services we have delivered
- if required to by law enforcement agencies

The Retention of Records Schedule is communicated to all relevant staff to ensure data is not retained for longer than necessary.

HOW WE PROTECT YOUR PERSONAL DATA

We are committed to protecting your information. CiC are certified to the ISO 27001 Information Security Standard. We take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of your personal data and against accidental loss or destruction of, or damage to, your personal data.

The measures we use are designed to provide a level of security appropriate to the risk of processing your personal information. However, please bear in mind that IT infrastructure and the internet cannot be guaranteed to be 100% secure. We have security measures in place and restrict access to databases only to those who need access appropriate to their job role.

All personal information and details provided as part of an enquiry, support or service request, or financial details are stored on a secure server. We do not store credit card numbers or related identifying information on any of our servers.

Digital data and hard copy data are securely disposed of when no longer required. This is conducted in line with our information security 'Disposal of Data Policy' and procedure.

CHANGES TO THIS PRIVACY POLICY

We keep our privacy policy under regular review. This privacy policy was last updated on 25th May 2018.

QUERIES OR COMPLAINTS

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. Please get in touch if you think we are using or collecting your data in an inappropriate way.

You can call us on 020 7938 0992 and ask to be referred to the DPO or Client Services Manager;
or you can email dpo@cic-eap.co.uk or you can write to us at the address listed at the beginning of this document.

You can also contact or make a complaint directly to the supervisory body for the UK. This is the Information Commissioners Office (ICO)
You can visit their website at: https://ico.org.uk/
Or contact them on: 0303 123 1113

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Guy Outram	25/05/2018
2	Added clarification on the types of special category data that may be collected. Separated definitions of third parties into professional services and service providers and updated the data shared with column.	Guy Outram	26/06/2018
3	Added references to emergency services	Guy Outram	28/06/2018
4	Added additional service providers to Table 2	Guy Outram	24/08/2018
5	Amended terminology to Customers i.e organisation and Client i.e. staff member/employee receiving the service.	Guy Outram	22/02/2019
6	Updated wording in sections Special Category Data and Retention of Records to make the statement clearer. Removed references to categories now defined in Pol-022	Guy Outram	06/06/2019