Appropriate Policy Document

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require us to have an APD in place.

This document demonstrates that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. It outlines in our retention policies with respect to this data.

Our general record of processing activities under GDPR Article 30 include:

(a) the condition which is relied upon; Is the contractual obligation to be able to deliver the paid services.
(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
(c) The personal data is retained and erased in accordance, with the retention policies outlined in this APD.

The APD therefore complements our general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. As per Schedule 1, Part 4 paragraph 41.

We will keep the APD under review and will need to retain it until six months after the date we stop the relevant processing. If the Commissioner asks to see it, we will provide it free of charge. As per Schedule 1 Part 4 paragraph 40.

Description of data processed

I. We collect the following data,
ii. Client Name
iii. Contact Number
iv. Email Address
v. What type of therapy (CBT, EMDR, Counselling)

vi. What delivery method (face to face, virtual, telephone)
vii. How many sessions needed.
viii. 3rd party therapist

Schedule 1 condition for processing

Please see the link below to our privacy policy

https://pinnaclewellbeing.co.uk/gdpr-privacy-policy/

Procedures for ensuring compliance with the principles

Accountability principle
i. We maintain appropriate documentation of our processing activities. ii. We have appropriate data protection policies. iii. We carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?
Principle (a): lawfulness, fairness and transparency
i. We identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data. ii. We make appropriate privacy information available with respect to the SC/CO data. iii. We are open and honest when we collect the SC/CO data, and we ensure that we do not deceive or mislead people about its use.
Principle (b): purpose limitation
i. We clearly identified our purpose(s) for processing the SC/CO data. ii. We included appropriate details of these purposes in our privacy information for individuals. iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we check that this is compatible with our original purpose or get specific consent for the new purpose.

Principle (c): data minimisation
i. We satisfied that we only collect SC/CO personal data we need for our specified purposes. ii. We satisfied that we have sufficient SC/CO data to properly fulfil those purposes. iii. We periodically review this SC/CO data and delete anything we don't need.
Principle (d): accuracy
i. We have appropriate processes in place to check the accuracy of the SC/CO data we collect, and we record the source of that data. ii. We have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and we update it as necessary. iii. We have a policy and set of procedures which outline how we keep records of mistakes and opinions; we deal with challenges to the accuracy of data, and we ensure compliance with the individual's right to rectification.
Principle (e): storage limitation
i. We carefully review how long we keep the SC/CO data, and we justify this amount of time by fulfilling statuary obligations, consent accuracy. ii. We regularly review our information and erase or anonymise this SC/CO data when we no longer need it. iii. We clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.
Principle (f): integrity and confidentiality (security)
i. We analyse the risks presented by our processing and use this to assess the appropriate level of security we need for this data. ii. We have an information security policy (or equivalent) regarding this SC/CO data, and we take steps to make sure the policy is implemented, and it is regularly reviewed. iii. We have put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing.

Retention and erasure policies

Please see the link below for our retention period.

APD review date

Written on 1st March 2024 and review date is 1st September 2024