



NeuroTribe UK

Registered Office Address: 61 Bridge Street, Kington, HR5 3DJ

Data Protection and Information Sharing Policy

1. Introduction

NeuroTribe UK CIC (hereinafter referred to as "the Company") is committed to protecting the privacy and confidentiality of your personal data and sensitive information in accordance with the General Data Protection Regulation (GDPR) and UK data protection legislation. This policy outlines your rights under data protection law (section 1.1) and the guidelines and procedures to ensure compliance with these regulations and safeguard the rights of data subjects (sections 2 through 9).

1.1 Your rights regarding your personal data

You have rights under data protection law. The rights available to you depend on our reason for processing your information and may only apply in certain circumstances. You can check the [Information Commissioners website](#) for more detail or contact NeuroTribe UK's DPO (Data Protection Officer) Kyra Hall-Gelly MBACP at info@neurotribe.uk or by calling 07712 205 300.

- **Your right to be informed**
– this notice informs you what data we collect and how we use it.
- **Your right of access –**
You have the right to ask us for a copy of your personal information and an explanation of why we are using it. You can find guidance and a template to make a subject access request on the ICO website here:
<https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data/preparing-and-submitting-your-subject-access-request/>
- **Your right to rectification -**
You have the right to ask us to correct information about you which you think is inaccurate or incomplete.
- **Your right to erasure -**
This is known as the 'right to be forgotten' and you have the right to ask us to erase your personal information in certain circumstances.

- **Your right to restriction of processing -**
You have the right to ask us to limit the processing of your information.
- **Your right to object to processing -**
You have the right to request we stop processing some or all of your data.
- **Your right to data portability -**
You have the right to get your personal data from us in a way that is accessible.
- **Rights around automated decision making and profiling –**
We do not use automated decision-making or profiling (a process whereby decisions are made about you without people being involved).

If you make a data rights request you are not required to pay a charge for doing so and we are committed to responding to your request within one month.

Please contact us at info@neurotribe.uk if you wish to make a request with regard to any of your rights.

2. Data Protection Compliance

2.1 The Company is registered with the Information Commissioner's Office (ICO) as a data controller and complies with all applicable data protection laws and regulations.

2.2 All sensitive data and information collected, processed, stored, maintained, and destroyed by the Company shall be handled in accordance with the provisions of the GDPR and UK data protection legislation.

2.3 All files and documents containing sensitive data and information held on personal computers by the Company and its associate therapists shall be encrypted and password protected.

3. Data Retention

3.1 Data retention refers to the period for which personal data is stored by the Company. In line with best practices and legal requirements, the Company shall retain personal data for a period of three years from the date of the last interaction with the data subject, unless there is a legal or regulatory obligation to retain it for a longer period.

3.2 After the expiration of the three-year retention period, the Company shall take appropriate measures to securely and permanently delete or anonymize the personal data in accordance with applicable data protection laws and regulations.

3.3 In cases where there is a legal or regulatory requirement to retain personal data beyond the three-year period, the Company will ensure compliance with such requirements and implement appropriate safeguards to protect the data.

3.4 Clients shall be informed about the data retention period during the Initial Consultation, and their explicit consent shall be obtained regarding the retention and processing of their personal data for the specified period.

3.5 The Company shall regularly review its data retention practices to ensure compliance with legal requirements and align with its data protection obligations.

4. Information Sharing

4.1 Information sharing with third parties shall only be conducted with the prior written consent of the data subject, unless otherwise required by law or authorized by a court order.

4.1.1 Client information is never sold to Third Party organizations for any purpose.

4.2 No notes pertaining to therapy or any other personal information shall be released to any agency, including the police, without the explicit written consent of the data subject, except in medical, mental health, or safeguarding emergencies. In such emergencies, only the necessary information to ensure the safety of the client shall be shared on a need-to-know basis with the relevant agencies. This data sharing will be communicated to the client at the earliest opportunity.

5. Communication of Sensitive Client Information

5.1 All sensitive client information shall be communicated with appropriate agencies and/or professionals on a need-to-know basis and only with the prior written consent of the data subject, except in the case of medical, mental health, or safeguarding emergencies.

5.1.1 Where it has been necessary to communicate with appropriate agencies and/or professionals whether verbally or in writing, communication will be logged and stored in line with section 12.2.

5.2 In cases of medical, mental health, or safeguarding emergencies, where there is an immediate risk to the well-being of the data subject or others, the necessary agencies shall be provided with only the necessary information to keep the client safe, and on a need-to-know basis. This data sharing will be communicated to the client at the earliest opportunity.

6. Informed Consent and Limits of Confidentiality

6.1 The Boundaries and Limits of Confidentiality:

6.1.1 All content discussed in therapy, supervision, or reflective practice remains confidential between the therapist and the client, unless something that is said indicates

possible serious harm to the client or another individual. In such cases, where it is necessary to break confidentiality, the client will be informed at the earliest opportunity and to the extent possible.

6.1.2 Furthermore, in the event that a historic case of abuse is disclosed by the client-survivor, and there is no immediate threat of harm to another individual, the principle of client autonomy shall be upheld. The client and the counselor will collaborate in making decisions regarding appropriate actions to be taken.

6.2 Clients shall be informed of this policy, including the exceptions outlined in **sections 5.1 and 5.2**, during the Initial Consultation with their therapist. The Limits of Confidentiality shall be fully explained to them, and their Informed Consent to the policy shall be obtained.

6.3 From time to time an agreement may be made between the Company and an organizational client to use a different confidentiality policy. Where this is the case, such a policy will be agreed in writing and clearly communicated to all appropriate service users so that Informed Consent can be obtained from service users.

7. Paramourncy Principle and Child Safety

7.1 This policy adheres at all times to the Paramourncy Principle of The Children Act 1989, which states that the safety of the child is paramount.

8. Responsibilities of Associate Therapists

8.1 All associate therapists working with the Company are required to abide by this Data Protection and Information Sharing Policy in its entirety.

8.2 Associate therapists are provided with access to and are required to use the fully encrypted and GDPR-compliant Kiku system (<https://www.wearekiku.com>) to store all notes pertaining to their work with the Company.

8.2 All members of the Company are required to use Egress, a fully encrypted, cloud email security system, to communicate any and all sensitive information and documentation where Kiku cannot be used for any reason.

9. Policy Review

9.1 This policy shall be regularly reviewed and updated as necessary to ensure compliance with current data protection laws and regulations.

9.2 Any changes to this policy shall be communicated to all relevant personnel and associates within a reasonable timeframe.

By adhering to this Data Protection and Information Sharing Policy, the Company aims to maintain the highest standards of data protection, confidentiality, and privacy for all data

subjects, ensure compliance with applicable laws and regulations, and prioritize the safety of clients, particularly in medical, mental health, or safeguarding emergencies.