



DATA PROTECTION POLICY

Data Protection Policy

IntoOut Health & Wellbeing Coaching

Effective Date: 1 September 2025

1. Purpose and Scope

This policy outlines how IntoOut Health & Wellbeing Coaching collects, processes, stores, and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and other applicable data protection laws. It applies to all personal data processed in the course of our coaching services.

2. Data Controller

Julie Norton, IntoOut Health & Wellbeing Coaching is the data controller responsible for determining the purposes and means of processing personal data.

Contact Information:

Email: julie@intoout.co.uk

Phone: 07730384005

3. Lawful Basis for Processing

We process personal data based on one or more of the following lawful bases:

- **Consent:** When individuals have given clear consent for processing their personal data for specific purposes.
 - **Contract:** Processing is necessary for the performance of a contract with the individual.
 - **Legal Obligation:** Processing is necessary to comply with legal obligations.
 - **Legitimate Interests:** Processing is necessary for our legitimate interests, provided these are not overridden by the individual's rights and interests.
-

4. Data We Collect

We may collect and process the following categories of personal data:

- **Contact Information:** Name, email address, phone number, postal address.
 - **Health and Wellbeing Information:** Details provided during coaching sessions, assessments, or questionnaires.
 - **Session Notes:** Summaries and observations from coaching sessions.
 - **Payment Information:** Transaction details for services rendered.
 - **Website Usage Data:** Information collected through cookies and analytics tools (if applicable).
-

5. How We Use Personal Data

Personal data is used for the following purposes:

- To provide and manage coaching services.
 - To communicate with clients regarding appointments, resources, and updates.
 - To maintain accurate records for administrative purposes.
 - To comply with legal and regulatory obligations.
 - To send newsletters or promotional materials, with explicit consent.
-

6. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes outlined in this policy or as required by law. Typically, client records are retained for a period of 7 years following the last interaction, after which they are securely deleted or anonymized.

7. Data Sharing

We do not sell or rent personal data to third parties. Data may be shared with:

- **Service Providers:** Such as payment processors, under strict confidentiality agreements.
 - **Legal Authorities:** When required to comply with legal obligations or to protect vital interests.
 - **Professional Advisors:** Such as accountants or insurers, under confidentiality agreements.
-

8. Data Security

We implement appropriate technical and organizational measures to protect personal data, including:

- Secure storage systems with restricted access.
 - Encryption and password protection for digital records.
 - Regular data protection training and awareness.
 - Procedures for responding to data breaches in accordance with ICO guidelines.
-

9. Individual Rights

Individuals have the following rights regarding their personal data:

- Access: The right to request access to their personal data.
- Rectification: The right to request correction of inaccurate or incomplete data.
- Erasure: The right to request deletion of their data, subject to legal obligations.
- Restriction: The right to request restriction of processing under certain conditions.
- Data Portability: The right to receive their data in a structured, commonly used format.
- Objection: The right to object to processing based on legitimate interests.
- Withdraw Consent: The right to withdraw consent at any time, where processing is based on consent.

To exercise these rights, please contact us using the details provided in Section 2.

10. Data Breach Procedure

In the event of a data breach, we will:

- Assess the nature and scope of the breach.
 - Notify the Information Commissioner's Office (ICO) within 72 hours, if required.
 - Inform affected individuals without undue delay, when there is a high risk to their rights and freedoms.
 - Document all breaches and remedial actions taken.
-

11. Policy Review

This policy is reviewed annually or when significant changes occur in our processing activities or applicable laws. The latest version is always available upon request.

Contact Us

For any questions or concerns regarding this policy or your personal data, please contact:

Email: julie@intoout.co.uk

Phone: 07730384005

This policy is adapted from best practices and guidelines provided by reputable sources, including the Information Commissioner's Office (ICO) and industry-specific recommendations for health and wellbeing professionals.