Mastery | Clarity | Wisdom

Helping Education & Non-Profit Organisations Lead with Confidence

Third Party Data Processing Agreement

Prepared for [CLIENT ORGANISATION]

Third-Party Data Processing Agreement

Between:

[Client Name] ("the Client"), a [legal entity type, e.g., academy trust, charity, school] registered in [location] with registered office at [address], and

MCW Mastery | Clarity | Wisdom Ltd ("the Consultant"), a company registered in England and Wales under Company Number 16300406, with its office at 18 Plants Brook Road, Sutton Coldfield, West Midlands, B76 1EX, UK.

Effective Date: [Insert Date]

Recitals: WHEREAS the Data Controller engages the Data Processor to provide consultancy services, including governance coaching, strategic advisory, organisational culture improvement, and leadership mentoring, which involve the processing of personal data on behalf of the Data Controller;

WHEREAS the parties wish to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018;

NOW, THEREFORE, the parties agree as follows:

1. Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person, as defined in UK GDPR, including names, contact details, consultation notes, sensitive data (e.g., health, DBS disclosures), and usage data.
- **Data Subject:** An individual whose personal data is processed (e.g., clients, staff, or prospects of the Data Controller).
- **Processing:** Any operation performed on personal data, including collection, storage, use, disclosure, or deletion.
- **Data Protection Legislation:** The UK GDPR, Data Protection Act 2018, and any other applicable UK data protection laws.
- **Sub-Processor:** A third party engaged by the Data Processor to process personal data on behalf of the Data Controller.

2. Subject Matter and Duration

- **Subject Matter:** The Data Processor shall process personal data as necessary to provide consultancy services to the Data Controller, including managing client relationships, conducting surveys, and delivering events or training.
- **Duration:** This Agreement shall commence on the Effective Date and continue until the termination of the consultancy services or as otherwise agreed, unless terminated earlier in accordance with Clause 10.

3. Nature and Purpose of Processing

- The Data Processor will process personal data to:
    - Deliver governance coaching, strategic advisory, and leadership mentoring.
    - Manage client data via contact forms, emails, and consultations.
    - Organise events and training using third-party tools (e.g., Eventbrite, Zoom).
    - Conduct employee satisfaction surveys or attendance/performance advice, including sensitive data with consent.
    - Support marketing activities based on legitimate interest or consent.

- The types of personal data processed include names, genders, ages, email addresses, phone numbers, job titles, consultation notes, biographical details (e.g., hobbies, pets), dietary requirements, sensitive data (e.g., health, DBS disclosures), payment details, and usage data (e.g., IP addresses, cookie data).

4. Obligations of the Data Processor

The Data Processor shall:

- Process personal data only on documented instructions from the Data Controller, unless required by UK law.
- Ensure personnel authorised to process data are bound by confidentiality obligations.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including encryption, password protection, two-factor authentication (2FA), and secure physical storage (e.g., fireproof safe).
- Assist the Data Controller, at the Controller's cost, in fulfilling data subject rights (e.g., access, erasure) and responding to data breaches.
- Delete or return all personal data to the Data Controller at the end of the service, unless required to retain it by law, and provide evidence of deletion.
- Maintain records of processing activities as required under Article 30 UK GDPR.

5. Sub-Processors

- The Data Processor may engage Sub-Processors to assist in processing, including:
    - GoDaddy (website, CRM, marketing) – https://www.godaddy.com/legal/agreements/privacy-policy.html
    - Microsoft 365 (spreadsheets) – https://www.microsoft.com/licensing/docs/view/Microsoft-Privacy-Statement
    - Eventbrite (events) – https://www.eventbrite.co.uk/support/articles/en_US/Troubleshooting/eventbrite-data-processing-addendum?lg=en_GB
    - Zoom (virtual meetings) – https://zoom.us/docs/en-us/privacy-and-legal.html
    - Monday.com (project management) – https://monday.com/data-processing-agreement
    - Social platforms (Twitter/X, LinkedIn, BlueSky, WhatsApp) for interactions.
- The Data Processor shall inform the Data Controller of any intended changes to Sub-Processors, allowing 30 days for objection. Sub-Processors will be bound by the same data protection obligations via individual log-ins or contractual safeguards.

6. Data Subject Rights

The Data Processor shall, upon the Data Controller's request and at the Controller's cost, assist in responding to data subject requests (e.g., access, rectification) within one month, using data stored in Monday.com, GoDaddy, Microsoft 365, or other systems.

7. Security and Data Breaches

- The Data Processor shall notify the Data Controller without undue delay (within 72 hours) of any personal data breach, providing details and mitigation steps.
- Security measures include restricted access by role, 2FA where available, weekly backups to an external hard drive stored in a fireproof safe, and encryption of digital data.

8. Data Transfers

- Data is not routinely transferred internationally. Occasional remote access by our personnel working remotely (under flexible working arrangements) from European countries (typically France, Germany, Spain, Italy, Malta, Gibraltar, Denmark, or Iceland) will be safeguarded by our company procedures and use of a secure Virtual Private Network. At the data of writing, we use NordVPN for this purpose. https://www.vpn.com/provider/nordvpn/privacy-and-data-protection/ [1]
- The Data Controller consents to such access arrangements, subject to the Data Processor's compliance with UK GDPR.

9. Audits and Inspections

- The Data Controller or its authorised representative may audit the Data Processor's compliance with this Agreement, with reasonable notice (at least 14 days) and at the Controller's expense.
- The Data Processor shall provide necessary information and access to records.

10. Termination

- This Agreement terminates upon completion of services or by either party with 30 days' written notice.
- Upon termination, the Data Processor shall delete or return all personal data, unless required to retain it by law, and provide certification of compliance.

11. Liability

- The Data Processor shall be liable for damages caused by processing that infringes UK GDPR, except where caused by the Data Controller's instructions.
- Liability is limited to direct damages up to the value of fees paid under the consultancy agreement.

12. Governing Law and Jurisdiction

- This Agreement is governed by the laws of England and Wales. Disputes shall be subject to the exclusive jurisdiction of the courts of England and Wales.

13. Signatures

For the Data Controller:
Name: [Client Representative Name]
Title: [Title]
Signature: _____
Date: [Insert Date]

For the Data Processor:
Name: Matthew Clements-Wheeler
Title: Founder and CEO
Signature: _____
Date: [Insert Date]

[1] Confirmation of advice we have received is summarised at the end of this document.

Analysis of Employee Data Access Under UKGDPR

This section provides a comprehensive examination of whether an employee accessing sensitive personal data via a secure VPN while temporarily in Europe or further afield constitutes a transfer outside the UK under the UK General Data Protection Regulation (UKGDPR). The analysis draws on official guidance, legal interpretations, and practical considerations, ensuring a thorough understanding for organisations and individuals navigating data protection laws.

Background on UKGDPR and Data Transfers

UKGDPR, enacted post-Brexit, mirrors the EU's General Data Protection Regulation (GDPR) but is tailored to the UK's legal framework. It governs how personal data, including sensitive personal data (e.g., health, race, or religious information), is processed and transferred. A "restricted transfer" under UKGDPR occurs when personal data is sent from the UK to a country outside the UK that lacks an adequacy decision, requiring additional safeguards like standard contractual clauses or binding corporate rules. However, the definition of a transfer is critical, and not all data movements qualify.

Employee Access: Not a Restricted Transfer

The scenario involves an employee, temporarily located in Europe or further afield, accessing data via a secure VPN. The key legal insight is that such access does not constitute a restricted transfer under UKGDPR, based on guidance from the Information Commissioner's Office (ICO) and the European Data Protection Board (EDPB). The EDPB, while primarily for the EU, provides influential guidance, and the ICO aligns closely, especially for international data flows.

According to the ICO's guide on international transfers (ICO Guide on International Transfers), a transfer requires the data to be sent to a "separate controller or processor, legally distinct from the sender." An employee, acting on behalf of the company, is not a separate entity but part of the same legal organization. This is further supported by the EDPB's guidelines, which clarify that an employee temporarily in a third country accessing the company's database does not constitute an international transfer (EDPB Guidelines on International Transfers).

For example, a UK company with an employee on a business trip in France accessing HR data via a VPN is not transferring data to France; the data remains under the company's control, and the employee is merely performing their role. This interpretation is echoed in legal analyses, such as from wrighthassall.co.uk, which states that such activities do not trigger transfer obligations under UK data protection law (Does accessing personal data on your work device while abroad constitute an international transfer of personal data?).

Sensitive Personal Data: Additional Considerations

Your query asked about "sensitive personal data," which under UKGDPR includes special categories like health data, requiring heightened protection. However, the classification as a transfer does not change based on data sensitivity; it hinges on whether the data is sent to a separate organization. The focus for sensitive data is ensuring security measures, such as encryption via the VPN, are robust. The ICO emphasizes that while access from abroad doesn't constitute a transfer, organizations must still protect data security, especially for sensitive information (ICO Guide on International Transfers).

Technical Aspects: VPN and Data Transmission

A secure VPN connects the employee's device to the company's network, typically in the UK, allowing access to data stored on UK servers. Technically, data is transmitted from the UK to the employee's device abroad, but legally, this is not classified as a transfer if the employee is part of the same entity. This is akin to remote working within the UK; the location of the employee does not transform the access into a transfer. Guidance from pinsentmasons.com confirms that strict transfer rules do not apply when employees access data remotely while on business trips (Data transfers guide addresses business trips).