



Data Processing Agreement

Executive Summary

This Data Processing Agreement (DPA) is crucial for your business because it:

1. Ensures Legal Compliance

- Meets GDPR requirements for data processing
- Protects your business from potential fines and penalties
- Demonstrates your commitment to data protection to your customers

2. Clarifies Responsibilities

- Clearly defines how we handle your valuable customer data
- Establishes security measures to protect your business information
- Sets out processes for managing data rights and breaches

3. Builds Trust

- Shows your customers that their data is handled professionally
- Provides transparency in data processing activities
- Helps maintain your reputation for data protection

4. Provides Business Continuity

- Ensures data handling continues smoothly if issues arise
- Establishes clear procedures for data management
- Protects your business interests during our partnership

By having this agreement in place, you're not just meeting legal requirements – you're protecting your business assets, customer relationships, and reputation in an increasingly data-driven world.

This Data Processing Agreement ("DPA") is entered into between:

Colloco Marketing Ltd ("Processor")

Company Registration Number: 12305516

Registered Office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

and

[CLIENT NAME] ("Controller")

[CLIENT DETAILS]



1. Definitions

- "GDPR" means the UK General Data Protection Regulation and the Data Protection Act 2018
- "Personal Data" means any information relating to an identified or identifiable natural person
- "Processing" means any operation performed on Personal Data
- "Data Subject" means the individual to whom Personal Data relates
- "Sub-processor" means any processor engaged by Colloco Marketing Ltd

2. Scope and Purpose

2.1 Processing Activities

Colloco Marketing Ltd processes Personal Data for the following purposes:

- Website design and maintenance
- Social media management and content creation
- Customer database management
- Email marketing and mailing list management
- Analytics and reporting
- Client website customer data processing

2.2 Categories of Data

The Personal Data processed may include:

- Names and contact details
- Email addresses
- Social media identifiers
- Customer behaviour data
- Website usage data
- Marketing preferences
- Transaction history
- Any other data provided by the Controller

3. Data Processing Locations and Systems

3.1 Processing Systems

Personal Data is processed using:

- Wix platform (website and CRM)



- Dropbox (primary file storage and backup)
- Microsoft Outlook (email communications)
- iCloud (secondary backup)

3.2 Data Storage Locations

- Primary storage: UK/EEA servers
- Cloud storage: As per service provider policies
- Backup storage: Dropbox and iCloud servers

4. Security Measures

4.1 Technical Measures

We implement appropriate technical measures including:

- Encryption of data in transit and at rest
- Secure password policies (minimum 12 characters, special characters, regular updates)
- Two-factor authentication where available
- Regular security updates and patches
- Automated backup systems
- Access logging and monitoring

4.2 Organizational Measures

We implement appropriate organizational measures including:

- Access control and user authentication
- Confidentiality agreements
- Regular staff training on data protection
- Clear desk and clear screen policies
- Document management and disposal procedures

4.3 Data Access Protocol

- Access granted on a need-to-know basis
- Unique user IDs for all staff members
- Regular access rights review
- Immediate access revocation upon role change/termination
- Prohibition of shared accounts

5. Data Breach Procedures

5.1 Breach Notification

In the event of a Personal Data breach, we will:



1. Notify the Controller without undue delay (within 24 hours of discovery)
2. Provide details of:
 - Nature of the breach
 - Categories of data affected
 - Approximate number of Data Subjects affected
 - Likely consequences
 - Measures taken or proposed
3. Document all breaches and remedial actions
4. Assist Controller with their notification obligations

5.2 Breach Response

Our breach response process includes:

1. Immediate containment measures
2. Impact assessment
3. Evidence preservation
4. Remedial action implementation
5. Process review and improvement

6. Sub-processors

6.1 Authorized Sub-processors

Current authorized sub-processors:

- Wix (website platform and hosting)
- Dropbox (file storage)
- Microsoft (email services)
- Apple (iCloud storage)

6.2 Sub-processor Management

- Controller authorizes the use of above sub-processors
- We will inform Controller of any intended changes
- We ensure sub-processors provide sufficient guarantees
- Sub-processors are bound by similar data protection obligations

7. Data Subject Rights

7.1 Request Handling

We will assist the Controller in responding to Data Subject requests for:

- Access to Personal Data
- Rectification of inaccurate data



- Erasure of Personal Data
- Restriction of processing
- Data portability
- Objection to processing

7.2 Response Procedure

1. Acknowledge receipt within 48 hours
2. Verify identity of requestor
3. Process request within 30 days
4. Document all actions taken
5. Maintain request register

7.3 Data Deletion

Upon request or contract termination:

1. Delete or return all Personal Data as instructed
2. Delete existing copies unless legally required to retain
3. Provide written confirmation of deletion
4. Ensure deletion from all backup systems within 90 days

8. Audit and Compliance

8.1 Audit Rights

- Controller may audit our processing activities
- 30 days' notice required for audits
- We will contribute to audits with necessary information
- Audits conducted during business hours
- Confidentiality agreements required

8.2 Compliance Records

We maintain records of:

- Processing activities
- Security measures
- Data breaches
- Subject access requests
- Staff training
- Sub-processor agreements

9. Term and Termination

- This DPA remains in effect while we process Personal Data



- Obligations continue after termination for retained data
- Data protection provisions survive termination

10. Liability and Indemnity

- We remain liable for compliance with GDPR
- Indemnification as per main service agreement
- Liability caps as per main service agreement

11. Governing Law

This DPA is governed by the laws of England and Wales.

Signatures

For Colloco Marketing Ltd:

Name: Sophia Brading

Title: Director

Date: _____

Signature: _____

For [CLIENT NAME]:

Name: _____

Title: _____

Date: _____

Signature: _____

Document Control

Version: 1.0

Last Updated: 12 December 2024

Review Date: [12 December 2024 + 1 YEAR]

© 2024 Colloco Marketing Ltd. All rights reserved.