# / Data Processing Agreement Template

Data &
Marketing
Association

## What is a data processing agreement?

- A legally binding agreement between a ‘data controller’ and a ‘data processor’ concerning the processing of personal data.
- A data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

  More information to help you determine if you are acting as a data controller, a joint data controller or a data processor can be found here.

## Why do I need a data processing agreement?

- Demonstrates accountability in accordance with Article 5 of UK GDPR.
- Required in accordance with Article 28 of UK GDPR.

## Why is it important?

- Underpins the controller-processor relationship.
- Defines the processing.
- Outlines each party’s responsibilities.
- Protects the personal data being processed and the rights of data subjects concerned.

## When should I use this template?

- Designed to be used by marketing organisations (the controller) that contract third parties to undertake processing of personal data on their behalf (the processor).
- When the processing includes direct marketing or direct marketing purposes.

## How to use this template?

- This is offered to members as a guidance tool. Should you have any questions, you can reach out to the DMA Legal and Compliance team: legaladvice@dma.org.uk .
- This template is drafted on the basis that this Data Processing Agreement is supplemental to a separate outsourcing agreement which deals with the other main commercial terms of the outsourcing arrangement between the Controller and the Processor.
- Sections that are highlighted in grey or written in grey text requires the editor to make amendments according to what has been agreed between the Controller and the Processor.

## Disclaimer

- This template is not to be taken as legal advice from the DMA.
- You have a responsibility to ensure that you undertake your own due diligence on the third parties you plan to work with
- You have a responsibility to ensure that the DPA you use, adequately covers the processing and liabilities
- As such, you should seek your own legal counsel when entering a contract with a third-party processor

## Where can I find further information?

- ICO - Controllers and processors | ICO
- EDPB – Guidelines on the concepts of controller and processor in the GDPR

Please continue on to the next page to view the Data Processing Agreement template.

This Data Processing Agreement is made between:

[COMPANY NAME]

[COMPANY ADDRESS]

("the Controller")

And

[SUPPLIER NAME]

[SUPPLIER ADDRESS]

("the Processor")

Hereinafter collectively referred to as "the Parties"

This Agreement is effective from the following date:

[DAY/MONTH/YEAR]

## 1. Background

Whereas:

**(A)** This Agreement is supplemental to any other separate agreement entered into between the parties and introduces further contractual provisions to ensure the Controller and the Processor comply with their respective obligations under the UK GDPR in respect of the Data Processing.

**(B)** Recital 81 and Article 28 of the UK GDPR place certain obligations upon a Controller to ensure that the Processor engages under the terms of this Agreement provides sufficient guarantees in terms of:

**i)** expert knowledge;
**ii)** reliability and resources;

iii) ability to implement technical and organisational measures which will meet the requirements of the UK GDPR including for the security of processing.

(C) The Controller must also take into account the specific tasks and responsibilities of the Processor under this Agreement in the context of the processing to be carried out and the risks to the rights and freedoms of the data subject.

(D) This Agreement exists to ensure that there are sufficient guarantees in place as required by the UK GDPR and that the processing complies with the obligations imposed on both the Controller and the Processor under the UK GDPR.

## 2. Definitions and interpretations

**"Personal Data"** has the meaning given to it in the UK GDPR and for the purposes of this Agreement, shall mean the categories of data listed in Schedule 1.

**"Data Subject"** shall have the same meaning as set out in Article 4 (1) of the UK GDPR and means an identified or identifiable natural person.

"**Controller"** has the meaning given to it in UK GDPR.

**"Processor"** has the meaning given to is in UK GDPR.

**"Sub-processor"** means any third party appointed to process personal data on behalf of the Processor.

**"GDPR"** means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council. In the UK we have the UK GDPR and Data Protection Act 2018 which govern how personal information can be processed, used, stored, accessed, and managed. After the UK left the EU, the UK GDPR was brought into effect on 1st January 2021.

**"Incident"** has the same meaning as a personal data breach in Article 4 (12) of the UK GDPR and means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data, transmitted, stored or otherwise processed under the terms of this Agreement.

**"Processing"** shall mean any operation or set of operations which is/are performed upon Data, (whether or not by automatic means) including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Such processing may be wholly or partly by automatic means or processing otherwise than by automatic means of

Data which form part of a filing system or one intended to form part of a filing system. A filing system shall mean any structured set of Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis."

## 3. Application

3.1. This Agreement shall apply to all Data processed from the date of this Agreement by the Processor on behalf of the Controller until the date of termination of this Agreement.

## 4. Duration of processing

4.1. The Processor shall process the Data for as long as the separate outsourcing agreement for the provision of the Services dated [EDITOR'S NOTE date/month/ year of outsourcing agreement] remains in full force and effect.

## 5. Processing

5.1. For the purposes of UK Data Protection Legislation, the Company is the Controller and hereby appoints the Supplier as its Processor, on the basis that the only Processing that the Processor is authorised to do is the Processing described in Schedule 1.

5.2. The Processor shall process the Personal Data it processes on behalf of the Controller, solely for the provision the "Services" as outlined in Schedule 2 of this Agreement. [EDITOR'S NOTE describe specifically what the processing is designed to achieve] in accordance with the written instructions of the Controller (including when making a transfer of personal data to countries outside the UK) unless required to do by law. The Processor must inform the Controller of what processing the Processor is required to do so by law unless the Processor is prohibited under the relevant law from notifying the Controller of such processing. The Processor shall not process the Data for any other purpose except with the express written consent of the Controller.

5.3. The Processor shall provide reasonable assistance to the Controller in the preparation of a Data Protection Impact Assessment (where applicable) prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

5.3.1. a systematic description of the envisaged Processing operations and the purpose of the Processing
5.3.2. an assessment of the necessity and proportionality of the Processing operations
5.3.3. an assessment of the risks that the Processing shall pose to the rights and freedoms of Data Subjects; and
5.3.4. the measures proposed or envisaged to address such risks, including

appropriate technical and organisational measures to ensure the protection of the Personal Data

5.4. The Controller confirms and warrants that the Processing of the Personal Data, including the transfer of the Personal Data to the Processor, has been and will continue to be carried out in accordance with the relevant provisions of the UK GDPR.

## 6. Processor's responsibilities

6.1. The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6.2. The Processor is aware that it may be subject to enforcement action by any relevant data protection supervisory authority to which the Controller is subject under Article 58 (Powers of the supervisory authority) of the UK GDPR.

6.3. The Processor is aware that if it fails to meet its obligations as set out in this Agreement and under Article 83 (General conditions for imposing administrative fines) of the UK GDPR, it may be subject to an administrative fine.

6.4. The Processor is aware that if it fails to meet its obligations under UK GDPR, it may be subject to a penalty under Article 84 (Penalties) of the UK GDPR.

6.5. The Processor is aware that if it fails to meet its obligations under UK GDPR, it may have to pay compensation to individual Data Subjects under Article 82 (right to compensation and liability) of the UK GDPR.

6.6. The Processor will appoint a data protection officer, if required in accordance with Article 37 (designation of the data protection officer) of the UK GDPR.

6.7. The Processor will appoint (in writing) a representative within the European Union if required because it is not established in the European Union and the provisions of Article 3 (2) apply in accordance with Article 27 (representatives of controllers or processors not established in the Union) of the UK GDPR.

## 7. Security and Confidentiality

7.1. The Processor and the Controller shall implement appropriate technical and organisational measures to ensure a level appropriate to the risks that are presented by the data processing in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal transmitted, stored or otherwise processed.

7.2. Both the Controller and Processor shall take into account the following when determining the measures:

7.2.1. the state of the art, and
7.2.2. the cost of implementation of the measures, and
7.2.3. the nature, scope context and purposes of processing, and
7.2.4. the risk of varying likelihood and severity for the rights and freedoms of individual Data Subjects

7.3. The Controller and Processor agree that the security measures taken in accordance with Clause 7.1.of this Agreement after assessment with the requirements of the UK GDPR are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of Personal Data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected having regard to the state of the art and the cost of their implementation; shall ensure a level of security appropriate to the risk.

7.4. The measures taken shall include amongst others the following items, where appropriate, from the non- exhaustive list below:

7.4.1. The pseudonymisation and encryption of Personal Data (where appropriate)
7.4.2. the ability to ensure the ongoing confidentiality, integrity and availability and resilience of processing systems and services
7.4.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical Incident
7.4.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

7.5. The Controller and the Processor may use adherence to an approved code of conduct as referred to by Article 40 of the UK GDPR or an approved certification mechanism as referred to in Article 42 as an element by which to demonstrate compliance with the requirements set out above in clauses 7.2, 7.3 and 7.4. of this Agreement.

7.6. The Processor shall ensure that each of its employees, agents or subcontractors are made aware of its obligations with regard to the security and protection of the Personal Data and shall require that they enter into binding obligations with the Processor in order to maintain the levels of security, protection and confidentiality provided for in this Agreement.

7.7. The Processor shall not divulge the Personal Data whether directly or indirectly to any person, firm or company without the express consent of the Controller except to those of its employees, agents and subcontractors who are engaged in the processing of the Personal Data and are subject to the binding obligations referred to in clause 7.6 of this Agreement above.

## 8. Data Subject's Rights

8.1. The Processor shall have appropriate technical and organisational means taking account of the nature of the Processing in so far as this is possible for the fulfilment of the Controller's obligation to respond to requests for exercising the following Data Subject's rights:

8.1.1. information rights under Articles 13 and 14 of the UK GDPR
8.1.2. right of access by the Data Subject under Article 15 of the UK GDPR
8.1.3. right to rectification under Article 16 of the UK GDPR
8.1.4. right to erasure under Article 17 of the UK GDPR
8.1.5. right to restriction of processing under Article 18 of the UK GDPR
8.1.6. notification regarding the right of rectification and/or erasure of personal data and/or restriction of processing under Article 19 of the UK GDPR
8.1.7. right to data portability under Article 20 of the UK GDPR

## 9. Data Incidents

9.1. The Processor must have effective processes for the identification, management and reporting of Incidents. Any Incident, suspected or actual, involving the Controller's Personal Data must be reported immediately to the Controller. An Incident may include but not be limited to:

9.1.1. Security breach or fraud
9.1.2. Misuse of relevant system storing Controller's Personal Data
9.1.3. Misuse, loss or corruption of the Controller's Personal Data
9.1.4. Unauthorised access to, use of, alteration, amendment or deletion of Controller's Personal Data
9.1.5. Physical security incident
9.1.6. Any unapproved requirement to disclose Controller's Personal Data to a third party.

9.2. The Processor will be expected to promptly investigate any such Incident, provide status updates throughout the Incident, where appropriate cooperate with reasonable Controller requests during the management of the Incident or permit the Controller to support the management of the

Incident, and send a written report to the Controller, describing the nature of the Incident, stating any control weaknesses discovered, and any actions taken/planned. A plan to agree any reasonable additional controls, either identified by the Processor or the Controller, to prevent or reduce the likelihood of a similar Incident must be agreed and monitored.

9.3. The Processor will assist the Controller in informing Data Subjects if there has been an Incident involving the Processor.

9.4. The Processor will assist the Controller in informing any relevant supervisory authority of an Incident.

## 10. Sub-processing

10.1. The Processor will not engage a sub-processor to process the Controller's Personal Data, without the prior specific or general or written authorisation of the Controller.

10.2. If the Processor employs a sub-processor under the Controller's prior general written authorisation the Processor will inform the Controller in writing of any intended additions to or replacement of sub-processor(s) the Processor uses to carry out processing of the Controller's personal data at least [EDITOR'S NOTE number of days to be inserted] days before the date of any intended additions or changes to the sub processors.

10.3. If the Controller objects to any such additions to or replacement the Controller shall inform the Processor within [EDITOR'S NOTE number of days to be inserted] days of receiving the notice in Clause 10.2. of this Agreement. Upon receipt of such a notice of objection the Processor shall not make the intended addition or replacement of [a] sub–processor(s).

10.4. The Processor, upon receipt of a notice under Clause 10.3. of this Agreement above may choose another sub–processor(s) it wishes to add to or act as a replacement to the existing sub-processor(s) it uses to carry out the processing. The Processor will then inform the Controller in accordance with clause 10.2. of this Agreement and the Controller will have the right to object in accordance with clause 10.3. of this Agreement.

10.5. The Processor shall ensure by written contract that any agent or sub-processor employed by the Processor to process Personal Data to which this Agreement relates:

10.5.1. imposes the same contract terms as listed in Clause 7 – Security and Confidentiality of Data and Clause 9 Data Incidents of this Agreement on any agent or sub- processor.
10.5.2. makes it clear that the Processor and not any agent or sub-processor will be liable to the Controller for the compliance of the agent or sub- processor with data protection law.

10.6. The Processor will immediately inform the Controller of any Incident involving any of its permitted sub-contractors or sub-processors in accordance with Clause 9 Data Incidents of this Agreement.

10.7. The Processor will assist the Controller in informing Data Subjects if there has been an Incident involving any of its permitted sub-contractors or sub-processors in accordance with Clause 9 Data Incidents of this Agreement.

10.8. The Processor will assist the Controller in informing any relevant supervisory authority of an Incident.

## 11. Audit, inspections and legal processing

11.1. The Processor must provide the Controller with all the information that is needed to show that both the Processor and the Controller have met their obligations under Article 28 of the GDPR.

11.2. The Processor must submit and contribute to audits and inspections conducted by the Controller, or another auditor mandated by the Controller.

11.3. The Processor shall, allow the Controller and/or its auditors, or their representatives, to have access to and audit relevant processes, procedures, documentation, and/or any premises of the Processor. Such access may take place on [EDITOR's NOTE – number of days' notice to be days' prior written notice to the Data Processor. The Controller agrees to reimburse the Processor any reasonable charge for the audit, at the hourly rates agreed within the Controller's contract with the Processor.

11.4. If the Controller reasonably believes that the Processor is in breach of any of its obligations under this Agreement the Controller shall not be obliged to give such prior notice and the Processor shall ensure that a Processor appointed representative shall provide full co-operation and assistance to the Controller and/or its representatives, auditors at no additional charge to the Controller.

11.5. The Processor shall inform the Controller if any instruction that the Controller gives, infringes the UK GDPR data protection provisions.

## 12. Transfer outside the UK

12.1. The Processor may not transfer or authorise the transfer of Data to countries outside the UK without the prior written consent of the Company. If personal data processed under this Agreement is transferred to a country outside the UK, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, check that an adequacy decision exists for the receiving country, or rely on the IDTA (UK International Data Transfer Agreement), or Addendum (the International Data Transfer Addendum), or other mechanism approved and authorised by the ICO.

## 13. Liability

13.1. The Processor's liability to the Controller for any loss or damage of whatsoever nature suffered or incurred by the Controller or for any liability of the Controller to any other person for any loss or damage of whatsoever nature suffered or incurred by that person shall to the extent permitted by law not exceed [EDITOR's NOTE: To Be agreed between the parties].

## 14. Termination

14.1. Subject to Clause 14.2. either Party may terminate this Agreement upon giving [EDITOR'S NOTE number of months to be inserted] months prior written notice to the other. Upon the date of termination of this Agreement, the Processor shall return or delete at the Controller's choice any Personal Data received from the Controller to the Controller.

14.2. The Processor shall not be obliged to return or delete any Personal Data received from the Controller which has:

14.3. already been deleted in the normal course of events or
14.4. the Processor is required to retain by law.

14.5. Notwithstanding termination of this contract, the provisions of this Agreement shall survive the termination of this Agreement and shall continue in full force and effect for a period of 2 years from the date of termination of the Agreement. The obligations contained in Clause 7 of this Agreement – Security and Confidentiality of Data – and Clause 9 of this Agreement- Data Incidents shall continue indefinitely.

## 15. Jurisdiction

15.1. This Agreement shall be governed by and construed in accordance with the law of England and Wales and the parties shall submit to the exclusive jurisdiction of the Courts of England and Wales.

IN WITNESS WHEREOF, each of the Parties hereto has caused the Agreement to be executed by its duly authorised representative.

.................................................................

Signed for and on behalf of the Controller

.................................................................

Name of person signing the Agreement

.........................................................

Position of person signing the Agreement

.................................................................

Date of signature

.................................................................

Signed for and on behalf of the Processor

.................................................................

Name of person signing the Agreement

.........................................................

Position of person signing the Agreement

............................................................

Date of signature

## SCHEDULE 1: DATA PROCESSING

| Description | Details |
|---|---|
| Subject matter of the Processing | |
| Duration of the Processing | |
| Nature and purposes of the Processing | Describe the processing and what the processing seeks to achieve. (Fuller details should be covered by a separate outsourcing agreement/contract) |
| Type(s) of Personal Data | Non-exhaustive list of examples include:<br>• personal details<br>• family details<br>• lifestyle and social circumstances<br>• goods and services<br>• financial details<br>• employment and education details<br>• details of complaints, incidents and grievances<br>• visual images, personal appearance and behaviour |

| Description | Details |
|---|---|
|  | • responses to surveys<br>• behavioural data<br>• profile data<br>• social media data<br>• tracking data from web activity |
| Categories of Data Subject | Non exhaustive list of examples include:<br>• customers<br>• prospective customers<br>• witnesses<br>• employees<br>• students<br>• suppliers<br>• complainants or their representatives<br>• subject of a complaint or their representatives<br>• individuals contacted when responding to a complaint or enquiry |

| Description | Details |
|---|---|
|  | • service providers<br>• lobbyists<br>• offenders and suspected offenders<br>• applicants for a licence or registration<br>• authors publishers and other creators, individuals captured by CCTV images<br>• consultants and advisers<br>• survey respondents<br>• journalists and the media |