Data Processing Contract Template

This template and the references in it are not legal advice. Any DMA (UK) member organisation or any other organisation using it needs to take their own independent legal advice from their usual data protection and contract law advisers.

There are particular issues with the GDPR

1. The UK is implementing the GDPR through a Data Protection Bill which is currently (April 2018) going through the final stages of Parliamentary approval but is not yet an Act.
2. The UK Information Commissioner’s Office (ICO) has not issued the final version of its guidance on Controller and Processor liabilities under the GDPR/new UK Data Protection Act. The ICO consulted on a draft version of the guidance which is referenced in the template
3. There has been no guidance issued at European level on Controller and Processor liabilities under the GDPR
4. The template is designed to be used supplementary to a main outsourcing contract which details the other contractual and commercial terms. The template only deals with the data protection terms

This Supplementary Agreement ("Agreement") dated \_\_\_\_\_\_\_ 201[ ] is between:

1. **[EDITOR’s NOTE – insert full company registered name, address of registered office and company registration number]** ("the Controller) and
2. **[[EDITOR’s NOTE – insert full company registered name, address of registered office and company registration number]** ("the Processor")

Whereas:

1. 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 GDPR in respect of the Data Processing.
2. Recital 81 and Article 28of the GDPR place certain obligations upon a Controller to ensure that the Processor it 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 GDPR including for the security of processing
3. 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 [[1]](#footnote-1)
4. This Agreement exists to ensure that there are sufficient guarantees in place as required by the GDPR and that the processing complies with the obligations imposed on both the Controller and the Processor under the GDPR.

1. Definitions

"Data" shall mean [List the categories of the data that is being processed and the categories of data subjects this processing relates to]

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

“EEA” means the European Economic Area – the 28 Member states of the European Union plus Iceland, Lichtenstein and Norway

“GDPR” means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council

“Incident” has the same meaning as a personal data breach in Article 4 (12) of the 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."

2. Application

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.

3. Purpose of Processing

1. The Processor shall process the Data it processes on behalf of the Controller, solely for the provision [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 EEA) 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.[[2]](#footnote-2)
2. The Controller confirms and warrants that the Processing of the Data, including the transfer of the Data to the Processor, has been and will continue to be carried out in accordance with the relevant provisions of the GDPR and does not violate the relevant provisions of the EEA country in which the Controller is established

4. Duration of processing

1. The Processor shall process the Data for as long as the separate outsourcing agreement for the provision of {xxx} services dated **[EDITOR’S NOTE date/month/ year of outsourcing agreement]** remains in full force and effect.[[3]](#footnote-3)

5. Type of Personal data

The Processor will process the following types of personal information

**[EDITOR’S NOTE – insert types of information. A non – exhaustive list of examples is provided below**

* personal details
* family details
* lifestyle and social circumstances
* goods and services
* financial details
* employment and education details
* details of complaints, incidents and grievances
* visual images, personal appearance and behaviour
* responses to surveys
* behavioural data
* profile data
* social media data
* tracking data from web activity

5. Categories of data subjects

The Processor will process information about the following categories of data subjects

**[EDITOR’s NOTE - insert types of information. A non – exhaustive list of categories of data subjects is provided below**

* customers
* prospective customers
* witnesses
* employees
* students
* suppliers
* complainants or their representatives
* subject of a complaint or their representatives
* individuals contacted when responding to a complaint or enquiry
* service providers
* lobbyists
* offenders and suspected offenders
* applicants for a licence or registration
* authors publishers and other creators,
* individuals captured by CCTV images
* consultants and advisers
* survey respondents
* journalists and the media] [[4]](#footnote-4)

6. Security and Confidentiality of Data[[5]](#footnote-5)

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.
2. Both the Controller and Processor shall take into account the following when determining the measures:
3. the state of the art, and
4. the cost of implementation of the measures, and
5. the nature, scope context and purposes of processing, and
6. the risk of varying likelihood and severity for the rights and freedoms of individual Data Subjects
7. The Controller and Processor agree that the measures security measures taken in accordance with Clause 6 (a) of this Agreement after assessment with the requirements of the GDPR are appropriate to protect Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of 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 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,
8. The measures taken shall include amongst others the following items, where appropriate, from the non- exhaustive list below:
9. the pseudonymisation and encryption of Data
10. the ability to ensure the ongoing confidentiality, integrity and availability and resilience of processing systems and services
11. the ability to restore the availability and access to Data in a timely manner in the event of a physical or technical Incident
12. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
13. The Controller and the Processor may use adherence to an approved code of conduct as referred to by Article 40 of the 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 clause 6) (b) (c) and (d) of this Agreement [[6]](#footnote-6)
14. 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 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.
15. The Processor shall not divulge the 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 Data and are subject to the binding obligations referred to in Clause 6 (e) of this Agreement above).

7. Incident Reporting

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

* Security breach or fraud
* Misuse of relevant system storing Controller’s Data
* Misuse, loss or corruption of the Controller’s Data
* Unauthorised access to, use of, alteration, amendment or deletion of Controller’s Data
* Physical security incident
* Any unapproved requirement to disclose Controller’s Data to a third party

1. 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.
2. The Processor will assist the Controller in informing Data Subjects if there has been an Incident involving the Processor.
3. The Processor will assist the Controller in informing any relevant supervisory authority of an Incident.

8. Processor’s appointment of a sub - processor

1. The Processor will not engage a sub processor to process the Controller’s Data, without the prior specific or general or written authorisation of the Controller.
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.
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 8 (b) 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)
4. The Processor, upon receipt of a notice under Clause 8 (c) 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 8(b) of this Agreement and the Controller will have the right to object in accordance with clause 8 (c) of this Agreement
5. The Processor shall ensure by written contract that any agent or sub-processor employed by the Processor to process Data to which this Agreement relates:
6. imposes the same contract terms as listed in Clause 6 – Security and Confidentiality of Data and Clause 7 Incident reporting of this Agreement on any agent or sub- processor [[7]](#footnote-7)
7. 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
8. The Processor will immediately inform the Controller of any Incident involving any of its’ permitted sub-contractors or sub-processors in accordance with Clause 7 Incident reporting of this Agreement.
9. 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 7 Incident reporting of this Agreement.
10. The Processor will assist the Controller in informing any relevant supervisory authority of an Incident.

9. Data Subjects rights[[8]](#footnote-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:
2. information rights under Articles 13 and 14 of the GDPR
3. right of access by the Data Subject under Article 15 of the GDPR
4. right to rectification under Article 16 of the GDOR
5. right to erasure under Article 17 of the GDPR
6. right to restriction of processing under Article 18 of the GDPR
7. notification regarding the right of rectification and/or erasure of personal data and/or restriction of processing under Article 19 of the GDPR
8. right to data portability under Article 20 of the GDPR

10. Assisting the Controller[[9]](#footnote-9)

1. The Processor will assist the Controller, taking into account the nature of the Processing and the information available to the Processor, to meet the Controller’s obligations
2. to keep Data secure in accordance with Article 32 of the GDPR
3. to notify Incidents in accordance with Article 33 of the GDPR
4. to advise Data Subjects when there has been an Incident in accordance with Article 34 of the GDPR
5. to carry out data protection impact assessments (DPIAs) in accordance with Article 35 GDPR
6. to consult with the Controller’s supervisory authority where a DPIA indicates there is an unmitigated high risk in accordance with Article 36 of the GDPR
7. The Processor will immediately pass on any notices, requests or other communications from a Data Subject. The Processor will not act on any request from a Data Subject, without the full written authority of the Controller.
8. If a privacy impact assessment indicates that there is an unmitigated high risk to the rights and freedoms of the Data Subject, the Processor will assist the Controller in consulting with the relevant supervisory authority or authorities

11. Audit, inspections and legal processing[[10]](#footnote-10)

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
2. The Processor must submit and contribute to audits and inspections conducted by the Controller or another auditor mandated by the Controller.[[11]](#footnote-11)

[**EDITOR’S NOTE An example of a simple audit right clause is below**

1. **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 inserted] 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.**
2. **If the Controller reasonably believes that the Processor is in breach of any of its obligations under this Agreement or in which case 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.}**
3. **The Processor shall inform the Controller if any instruction that the Controller gives, infringes the GDPR or other EU, or EEA member state data protection provisions.}**

12. Processor’s responsibilities and liabilities under the GDPR

1. 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 GDPR.
2. 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 GDPR, it may be subject to an administrative fine.
3. The Processor is aware that if it fails to meet its obligations under GDPR, it may be subject to a penalty under Article 84 (Penalties) of the GDPR.
4. The Processor is aware that if it fails to meet its obligations under GDPR, it may have to pay compensation to individual Data Subjects under Article 82 (right to compensation and liability) of the GDPR.
5. The Processor will appoint a data protection officer, if required in accordance with Article 37 (designation of the data protection officer) of the GDPR.
6. 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 GDPR .

13. Liability[[12]](#footnote-12)

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

1. Subject to Clause 14 (b) either Party may terminate this Agreement upon giving [**EDITOR’**S **NOTE number of months to be inserted] [**XXX] months prior written notice to the other. **{EDITOR’s NOTE – the notice period here should be the same as in the main outsourcing contract}** Upon the date of termination of this Agreement, the Processor shall return or delete at the Controller’s choice any Data received from the Controller to the Controller

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

1. already been deleted in the normal course of events or
2. the Processor is required to retain by law.
3. 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 6 of this Agreement – Security and Confidentiality of Data – and Clause 7of this Agreement- Incident Reporting shall continue indefinitely.

15. Assignment

This Agreement shall not be transferred or assigned by either party except with the prior written consent of the other.

16. Jurisdiction

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 Signed for and on behalf of the Processor

………………………………………………. ……………………………………………….

Name of person signing the Agreement Name of person signing the Agreement

………………………………………………... ………………………………………………...

Position of person signing the Agreement Position of person signing the Agreement

……………………………….. ………………………………

Date of signature Date of signature

1. see Recital 81 of the GDPR and page 13 of ICO GDPR guidance: Contracts and liabilities between controllers and processors <https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf>

   (Reference checked 19/04/18) [↑](#footnote-ref-1)
2. this is a requirement of Article 28.3 and see page 13 of I ICO GDPR guidance: Contracts and liabilities between controllers and processors <https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf>

   Reference checked 19/04/18 [↑](#footnote-ref-2)
3. clause 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 [↑](#footnote-ref-3)
4. source of Clauses 3, 4 and 5 is Article 28.3 of the GDPR – see pages 12 – 13 of ICO GDPR guidance: Contracts and liabilities between controllers and processors [https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf](https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf%20)  [↑](#footnote-ref-4)
5. The above is required by Article 28.3 (c) of the GDPR and is a summary of the Article 32 GDPR requirements – see page 14 of ICO GDPR guidance: Contracts and liabilities between controllers and processors <https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf> Reference checked 19/04/18

   [↑](#footnote-ref-5)
6. no code of conduct has been approved yet under Article 40 or an approved certification mechanism under Article 42. FEDMA is working on updating its current Code of Conduct which was approved under the 1995 Data Protection Directive and submitting it for approval under the GDPR [↑](#footnote-ref-6)
7. These are the contract terms required by article 28.3 of the GDPR. See page 14 of ICO GDPR guidance: Contracts and liabilities between controllers and processors <https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf>

   [↑](#footnote-ref-7)
8. This is a requirement under Article 28.3 GDPR. The ICO will issue further guidance on this in due course – see page 15 of ICO GDPR guidance: Contracts and liabilities between controllers and processors

   <https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf> [↑](#footnote-ref-8)
9. The Processor’s obligations to assist the Controller is not infinite it is limited by “taking into account the nature of processing and the information available to the Processor.” This is a requirement under Article 28.3 (f) GDPR. The ICO will issue guidance on the specific requirements of each of the GDPR articles listed in Clause 10 (a) above} [↑](#footnote-ref-9)
10. The ICO Guidance {page 16 of ICO GDPR guidance: Contracts and liabilities between controllers and processors <https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf> ( Reference checked 19/04/18) suggests that the Data Processor could do this by providing the Data Controller with the necessary information or by submitting to an audit or inspection. The Data Processor will need to keep records of the Processing of the Data it carries out on behalf of the Data Controller [↑](#footnote-ref-10)
11. The GDPR does not mandate such audits but it is clearly best practice for audit rights to be granted. [↑](#footnote-ref-11)
12. it is up to the parties to negotiate a limitation of liability based on the commercial terms of the contract. Possible starting points could include i) the amount of money the Data Controller has paid to the Data Processor for the Data Processing services in the immediately preceding calendar year, although this may not be appropriate in the case where there is a law value but high data protection risk or ii) the maximum level of fines under the GDPR} [↑](#footnote-ref-12)