Digital Decisions

World Federation of Advertisers

bva bondvanadverteerders

Data Processing Agreement for Advertisers

A contract template to check current and future agreements with partners

Data Processing Agreement for Advertisers | Template

This Data Protection Agreement (DPA) template for Advertisers has been drafted by Digital Decisions in collaboration with the World Federation of Advertisers (WFA) and Bond van Adverteerders (BVA | Association of Dutch Advertisers). Questions regarding this template may be directed to Ruben Schreurs, Digital Decisions, email: r.schreurs@digitaldecisions.com; Matt Green, WFA, email: m.green@wfanet.org; or Hanne Alblas, BVA, email: hanne.alblas@bva.nl.

Advertisers have expressed concerns about DPAs received by their Processor partners, as many of the agreements are one-sided, incomplete and written in the interest of the Processor. As Advertisers in their role of Data Controller are inherently responsible – and liable – in cases of non-compliance, this DPA template serves as a Controller-centric example. The terms in this template are not intended to represent the only methodology in which the contractual relationship between Controllers and Processors should be addressed. Instead, it contains a comprehensive range of terms that should be considered and discussed with partners.

Some key considerations addressed by releasing this template are: **a)** roles as defined under the GDPR (Controller, Joint Controller, Processor and Sub-Processor) can differ within a single relationship, i.e. the Advertiser is not – and should not – always be considered the Controller on all activities involving the processing of Personal Data performed by their partners. Specific processing activities where partners are tasked with the Processing of Personal Data on behalf of the advertiser should be listed in the appropriate annex of this DPA, for any non-listed or non-agreed processing activities the partner should be considered as acting autonomously, hence fulfilling the role of Controller; **b)** this template covers wider regulations outside of the GDPR and is specifically drafted to be future-proof; **c)** in case Advertisers already have a signed DPA in place with their partner(s), this template can serve as a sanity check on terms included in the current agreements; **d)** Advertisers can use this template with their (network) agency- and technology partners.

Bracketed provisions highlighted in yellow are items that require insertions or items that should be considered, completed, and/or modified when utilising this template.

Important: this template should not be considered as legal advice, and any organisation looking to adopt terms within this template should not rely upon it as such. Advertisers, or other organisations looking to implement contractual frameworks, such as this DPA, should seek legal advice. None of the collaborating parties (Digital Decisions, WFA, BVA) carry any liability for the accuracy and lawfulness of this document. Any party using this document for any purpose does so at their own risk.

Digital Decisions

WFA World Federation of Advertisers

bva
bondvanadverteerders

Introduction

This document can be used as an example Data Processing Agreement by Advertisers looking to update their contractual framework under the recently enforced and upcoming Data Protection and Privacy Regulations. As the European Commission or Data Protection Authorities have not released an 'approved' agreement at the point of releasing this template, there is no single '*approved*' agreement that should be used by Controllers in partnership with their Processors. It is, therefore, important that each Advertiser using this template carefully assess the terms in this agreement before adopting any – or all – in an agreement with their Processor(s).

This document is drafted from an Advertiser/Controller perspective. It is common for Processors to have their own DPAs that they prefer, especially enterprises/multinational companies. This document can serve as a baseline for negotiations; where articles about Processor obligations (7,8,11), Sub-processors (12), Audits (15) and Processor liability (18) are likely to be a point of discussion.

"With advertisers increasingly entering into direct contractual relationships with more and more partners to ensure they retain control of their data and direct relationship with consumers, the role of the Data Processing Agreement will become even more critical both strategically and to ensure they do not risk the reputational damage that could occur if they fail to comply with the requirements of GDPR. This template will give brands guidance to ensure they have the right level of transparency and control in their relationship."

Stephan Loerke | CEO, WFA

"In the last couple of months, it became more and more clear that from an advertiser perspective, generic Data Processing Agreements don't cover all controller issues. This is why we have taken the initiative to create a specific DPA template together with Digital Decisions and the WFA. We recommend advertisers to internally check their current (and future) DPA's to this template to know what's in their best interest to include in their DPA's"

Frenkel Denie | Chairman, BVA

"We have aimed for this advertiser-centric Data Processing Agreement template to be a useful and practical tool to advertisers globally. Many advertisers are feeling insecure about the right way to work towards GDPR compliance, and managing their partnerships is a key part of this. We are pleased to have worked together with two incredibly strong associations that provide valuable and actionable input to their members and the wider industry."

Ruben Schreurs | CEO, Digital Decisions

Table of Contents

This **Data Processing Agreement** (hereinafter referred as "**DPA**") is entered into on [May 25th, 2018] ("**Effective Date**") and forms part of the [(master) service agreement] (hereinafter referred as "**Principal Agreement**"), and is concluded between:

- [name of the company] (hereinafter referred to as: 'the Controller'), a company incorporated under the laws of [the applicable law] and having its principal office in [address];

And

Alternative A

- [independent agency] (hereinafter referred to as: 'the Processor') incorporated under the laws of [the applicable law] and having its principal office in [address];

Alternative B

- [network agency], including all relevant subsidiaries within [holding company – e.g. WPP/Publicis/Dentsu Aegis/IPG/Omnicom/Havas etc.] as listed in [Annex I (optional)] (hereinafter referred to as: 'the Processor') incorporated under the laws of [the applicable law] and having its principal office in [address];

Alternative C

- [direct supplier] (hereinafter referred as: 'the Processor') incorporated under the laws of [the applicable law] and having its principal office in [address];

Within this agreement, [company] is considered the Controller and [independent agency/ network agency/direct supplier] the Processor exclusively for the activities set forth in Annex A and henceforth throughout this DPA they are referred as the Controller and the Processor.

The Controller and the Processor are hereinafter jointly referred to as the "**Parties**" and individually as the "**Party**".

In the course of the performance of this DPA the terms of this DPA shall apply. Terms not otherwise defined herein shall have the same meaning as indicated in the Principal Agreement. Unless otherwise specified below, the terms of the Principal Agreement shall remain in full force and effect.

The Parties herewith agree that the terms and conditions as indicated within this DPA must be attached as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

The Parties agree as follows:

1. Definitions

1.1. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

1.2. “**Personal Data**” means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.3. “**Data Subject**” means identified or identifiable natural person to whom Personal Data relates.

1.4. “**Data Subject Access Request**” means the access request issued by the Data Subject to access his/her data; this request may include, but is not limited to, the copy of Personal Data processed; the purpose of Processing; the categories of Personal Data concerned, disclosure of parties that can access the Personal Data; the extent the Personal Data is used for automated decision making and mechanism used for it.

1.5. “**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.6. “**Controller**” means 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; where the purposes and means of such Processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.

1.7. “**Processor**” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

1.8. “**Sub-processor**” means any natural or legal person appointed and instructed by the Processor and authorised by the Controller to Process Personal Data on behalf of the Controller in connection with the Principal Agreement.

1.9. “**Third Party**” means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.

1.10. “**Approved Data Transfers**” means data transfers within the Territorial Scope as set out in Article 3 of the GDPR to companies within the scope of Articles 44 to 49 of the GDPR.

1.11. “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.12. “**Data Protection Impact Assessment**” means a tool to enhance compliance with the GDPR by evaluating the origin, nature, particularity and severity of that risk, where processing operations are likely to result in a high risk to the rights and freedoms of Data Subjects.

1.13. “**Supervisory Authority**” means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR.

1.14. “**Data Protection Requirements**” means all applicable laws, regulations, and other legal requirements relating to (a) privacy, data security, consumer protection, marketing, promotion, and text messaging, email, and other communications; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other Processing of any Personal Data including the GDPR; if at any time any legislative or regulatory change after the date of conclusion of this DPA is enacted, the new or amended law or regulation applies.

2. Nature and Objectives of Data Processing

2.1. This DPA applies to the Processing of Personal Data by the Processor on behalf of the Controller resulting from the services provided by the Processor under the Principal Agreement. The Processor shall only process the types of Personal Data relating to the categories of Data Subjects for the purposes of the Principal Agreement and for the specific purposes in each case as set out in Annex A, B and C to this DPA, and shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than in accordance with the Controller's documented instructions (whether in the Principal Agreement or otherwise) unless Processing is required under the Data Protection Requirements to which the Processor is subject, in which case Processor shall to the extent permitted by such requirements inform the Controller of that legal requirement before processing that Personal Data.

2.2. This DPA is concluded with the primary goal to ensure that the rights of Data Subjects and the protection of their data and privacy is inherent within the relationship of the Controller and the Processor as set forth in this DPA. A key intention of this DPA is to provide elaborate clarity around responsibilities and objectives for both Parties, in order to ensure that Data Subjects' rights are treated with great care and sensitivity.

3. Data Subjects

The categories of Personal Data that are processed by the Processor as instructed by the Controller are listed in Annex B. Annex B shall be updated in case of any modifications in Data Subject categories that are processed and must be agreed in writing by both parties.

4. Data Subject Rights

In accordance with any Data Processing Requirements including GDPR the Processor is obliged to implement any operational, technical or other measures to allow for Data Subjects to exercise all their rights and freedoms.

5. Data Subject Requests

5.1. The Processor shall provide its assistance to enable the Controller to respond to any such requests under the applicable Data Protection Requirements within the legally required time frame.

5.2. Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is required for the fulfilment of the Controller's obligation to respond to a Data Subject Request under the Data Protection Requirements.

5.3. If such a request is made directly to the Processor, the Processor shall immediately inform the Controller and shall advise Data Subjects to file their request to the Controller instead.

6. Types of Personal Data Processed

The types of Personal Data that are processed by the Processor as instructed by the Controller are listed in Annex C. Annex C shall be updated in case of any changes in types of Personal Data processed and must be agreed in writing by both parties.

7. The Controller and the Processor: Rights and Obligations

Controller

The Controller is obliged to:

7.1.1. Determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Processor;

7.1.2. Warrant that it has valid legal grounds to provide the Personal Data to the Processor for the Processing to be performed in relation to the Services to the extent required by the Data Protection Requirements;

Processor

The Processor is obliged to:

7.1.3. Process all Personal Data in compliance with the relevant Data Protection Requirements;

7.1.4. Only process the Personal Data on behalf of the Controller after explicit instructions to do so as set out in Article 7.1.1.;

7.1.5. Immediately inform the Controller if, in its opinion, an instruction given by the Controller infringes any of the Data Protection Requirements;

7.1.6. Assist the Controller in allowing Data Subjects to exercise their rights as set out in Article 4;

7.1.7. Implement appropriate technical and organisational measures to ensure sufficient level of security of the Processing of Personal Data as set out in Annex D;

7.1.8. Notify the Controller immediately after the Processor becomes aware of any Personal Data Breach and act in accordance with Article 14;

7.1.9. Refrain from making use of the Personal Data for any purpose other than as specified by the Controller as set out in Article 7.1.1.;

7.1.10. Inform the Controller in case of: binding request for disclosure of Personal Data by a law enforcement authority; any notice, inquiry or investigation by a Supervisory Authority with respect to Personal Data processed; any complaint or request received from Data Subjects;

7.1.11. On request, provide the Controller promptly with details regarding the measures it has adopted to comply with its obligations under this DPA;

7.1.12. Ensure confidentiality as set out in Article 10;

7.1.13. Maintain written records of Processing activities under its responsibility and demonstrate them upon a request by the Controller and/or Supervisory Authority where applicable;

7.1.14. Designate a data protection officer if required under Article 37 of the GDPR; Contact details of the data protection officer that must be published are listed in Annex E;

8. Returning or Deletion of Personal Data

8.1. Upon termination of this DPA, upon the written request by the Controller, or upon fulfilment of all purposes agreed in the context of the Services whereby no further Processing is required, the Processor shall, at the discretion of the Controller, either (a) return a complete copy of all Personal Data to the Controller by secure file transfer in such format as is notified by the Controller; and (b) delete and procure the deletion of all other copies of Controller Personal Data Processed by any contracted Processor, and certify to the Controller that it has done so.

8.2. The Processor shall notify all Sub-processors supporting its Processing of the Personal Data of the termination of the DPA and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Controller, at the discretion of the Controller.

8.3. To the extent that is required under the Data Protection Requirements or other applicable legislation, the Processor may preserve Personal Data for such a period as set out in applicable Data Protection Requirements or legislation, and the Processor is obliged to ensure confidentiality of all Personal Data as set out in Article 10, and shall ensure that such Personal Data is only Processed as necessary for the purposes specified in Data Protection Requirements.

9. Data Protection Impact Assessment

The Processor shall provide reasonable assistance to the Controller with any Data Protection Impact Assessments which are required under Article 35 of the GDPR and with any prior consultations to any Supervisory Authority of the Controller or any of its affiliates which are required under Article 36 of the GDPR, in each case in relation to Processing of Personal Data by Processor on behalf of the Controller and taking into account the nature of the Processing and information available to the Processor.

10. Confidentiality

10.1. The Processor shall treat all Personal Data as strictly confidential.

10.2. The Processor shall inform all its employees, agents and/or approved Sub-processors engaged in Processing the Personal Data about the obligation of confidentiality of the Personal Data.

10.3. The Processor shall ensure that all such involved persons or entities are bound by a legal requirement to ensure confidentiality.

10.4. Any information of whatever kind (whether technical, commercial, financial, operational or otherwise) and in whatever form, which may be disclosed in any form or matter by one Party to the other Party, in connection with this DPA, shall be deemed confidential.

11. Security

11.1. The security requirements for the Processing of Personal Data are described in Annex D.

11.2. The Processor shall at all times have in place an appropriate written security policy with respect to the Processing of Personal Data, outlining in any case the measures set out in Annex D.

11.3. The Processor has to evaluate the measures as implemented in accordance with Annex D on an on-going basis and has to update these measures in order to maintain compliance with these requirements.

11.4. Without prejudice to any other security standards agreed upon by the Parties, the Processor shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk and shall take all measures required pursuant to Article 32 of the GDPR.

12. Sub-processors

12.1. All currently engaged Sub-processors are listed in Annex F. If the Processor wishes to engage a new Sub-processor, written approval from the Controller is required and Annex F should be updated.

12.2. The Processor is allowed to engage Sub-processors in case the Controller does not respond to the approval request as set out in Article 12.1 within a period of 30 days. If this is the case, the request can be deemed to be approved by the Controller until at any point in the future Controller retracts the approval in writing.

12.3. The Controller may, at any point in time, request for the Processor to cease working with any of the Sub-processor(s). In such case, the Processor shall end all Processing activities with the concerned Sub-processor(s) within a period of [30 days (example)]and act in accordance with Article 8.2.

12.4. The Processor shall remain fully liable to the Controller for the performance of any Sub-processor that fails to fulfil its legal obligations, including the Data Protection Requirements.

12.5. With respect to each Sub-processor approved by the Controller; the Processor shall include terms in its contracts with each Sub-processor which are the same as those set out in this DPA, and the Processor shall supervise compliance thereof. Upon request, the Processor shall provide a copy of its agreements with Sub-processors to the Controller for its review.

12.6. In case a Sub-processor is engaged, the Processing must be carried out in accordance with the applicable Data Protection Requirements and all terms set forth in this DPA.

12.7. In case a Sub-processor is engaged, the same audit rights as set out in Article 15 apply to the Sub-processor.

13. International Data Transfers

13.1. The Processor and any involved Sub-processor are not allowed to conduct transfers of any Personal Data other than Approved Data Transfers.

13.2. Any international data transfers that do not fall under Article 13.1. should be authorized in writing by the Controller. Current international transfers for which the Controller has granted authorisation are listed in Annex G.

14. Data Breaches

14.1. The Processor shall notify the Controller immediately when the Processor or any Sub-processor becomes aware of a Personal Data Breach affecting the Controller Personal Data, providing the Controller with sufficient information to allow each Controller group member to meet any obligations to report or inform Data Subjects and Supervisory Authority of the Personal Data Breach under the Data Protection Requirements.

14.2. Notice must be given to the address set out in Annex H. This notification must contain at least the following information:

14.2.1. The nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

14.2.2. The name and contact details of the data protection officer or other contact point where more information can be obtained;

14.2.3. The likely consequences of the Personal Data Breach;

14.2.4. The measures taken or proposed to be taken by the controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;

14.3. In situation where it is not possible to provide the information at the same time, the information may be provided in phases without undue delay.

14.4. The Processor shall cooperate with the Controller and take such reasonable steps as are assigned by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

14.5. The Processor is liable for any damages caused by the Processor, his/her employees, agents or appointed Sub-contractors as a result of the Data Breach.

15. Audits

15.1. Subject to Articles 15.2 to 15.3, Processor and relevant Processor Affiliate(s) shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by [company] and its group members or an auditor mandated by the Controller in relation to the Processing of Personal Data by the Processor.

15.2. Information and audit rights of the Company Group Members only arise under Article 15.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Requirements (including, where applicable, Article 28(3)(h) of the GDPR).

15.3. [company] and its group members or a mandated auditor undertaking an audit shall give Processor or the relevant Processor Affiliate(s) reasonable notice of any audit or inspection to be conducted under Article 15.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

16. Duration and Termination

16.1. This DPA will terminate upon the termination of the Principal Agreement.

16.2. Termination or expiration of this DPA shall not release the Processor from its confidentiality obligation.

16.3. The Processor may process the data only until the termination/expiration date and such data must be returned or destroyed on instruction of the Data Controller unless required otherwise by applicable Data Protection Requirements.

17. Governing Law

17.1. The parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

17.2. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

18. Liability

The Processor shall fully compensate the Controller and holds the Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Controller and arising directly or indirectly out of or in connection with a breach of this DPA and/or the applicable Data Protection Requirements by the Processor or any of its Sub-processors.

Signed by;

Name______________________________ **Position**______________________________

As an Authorized representative for and on behalf of

[name of the company]

Date______________________________

Name______________________________ **Position**______________________________

As an Authorized representative for and on behalf of

[name of the independent agency/network agency/direct supplier]

Date______________________________

Annex A

Activities, Legal Grounds and Purposes of Personal Data Processing

Activity where [company] is considered the Controller and [the independent agency/ network agency/direct supplier] the Processor	Legal Grounds of Personal Data Processing	Purposes of Personal Data Processing
[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]

Annex B

Data Subject Categories

Data Subject Categories involved in the Data Processing Activities are as follows:

- [Employees];
- [Customers];
- [Prospective clients];
- [Insert].

Annex C

Types of Personal Data Processed

Personal Data that will be processed in the scope of the Service Agreement:

- [Names];
- [Contact information (email, phone, fax, physical address etc.)];
- [IP addresses];
- [Biometric data];
- [Insert].

Special Categories of Personal Data that will be processed in the scope of the Service Agreement:

- [Health related data];
- [Sexual orientation related data];
- [Religious data];
- [Insert].

Annex D

Security of Processing

Both Parties undertake to adopt necessary security measures in order to protect the Personal Data processed appropriate to the risk.

The implemented measures to maintain appropriate organizational and technical security include, but are not limited to:

- [The pseudonymisation and encryption of Personal Data];
- [The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services];
- [The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident];
- [A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing];
- [Efficient implementation of information security policy];
- [Regularly review our information security policies and measures and, where necessary, improve them];
- [insert].

The Processor shall document the implementation of the technical and organizational measures in accordance with any Data Protection Requirements, including the GDPR.

Annex E

Data Protection Officer Contact Details

Contact information of the [data protection officer] of the Processor:

[Contact information]

Annex F

Sub-processors

Nr.	Details of Sub-processors
1.	[Insert]
2.	[Insert]
3.	[Insert]
4.	[Insert]

Annex G

International Data Transfers Authorized by the Controller

[Insert the details of the international data transfers which are authorized by the Controller]

Annex H

Contact Details

Controller

- Name: [insert]
- Position: [insert]
- Telephone: [insert]
- Email: [insert]
- Address: [insert]

Processor

- Name: [insert]
- Position: [insert]
- Telephone: [insert]
- Email: [insert]
- Address: [insert]

Annex I (optional in case of network agency)

Network Agency Subsidiaries covered by the terms of this agreement

Nr.	Details of network agency entities involved in Data Processing Activities considered as Processors and covered by the terms of this agreement
1.	[Insert]
2.	[Insert]
3.	[Insert]
4.	[Insert]