

## **DATA PROTECTION AGREEMENT**

In the course of rendering services as per the Media Buying Agreement (hereinafter referred to as “**Main Agreement**”), and necessity that the Partners deal with personal data with regard to which Four Media Networks GmbH acts as a controller in terms of data protection law (hereinafter referred to as “**Customer Data**”). Four Media Network GmbH is required to demonstrate accountability for compliance with data protection laws including the General Data Protection Regulation by our parent company, affiliates, clients and through our supply chain. We have sent you this document to confirm your compliance with your legal obligations to Four Media Network GmbH by signing and returning to us this Data Protection Agreement. This DPA serves as an agreement between Media Buyer and Four Media Network GmbH to reflect Media Buyer’s responsibility with regard to the processing and protection of Personal Data, and the terms and conditions of this DPA shall complement and supplement any existing agreements between Media Buyer and Four Media Network GmbH if such agreements exist.

### **Definitions therein:**

“**Partner**” means Media Buyer. References in this document to “Partner”, “you” or “your” shall refer to the entity that is acting in the capacity of a service provider/partner/vendor to Four Media Network GmbH and to your respective subcontractors and affiliates.

“**Applicable Laws**” means laws, rules, directives, regulations issued or enacted by any government entity (including any domestic or foreign, supra-national, state, county, municipal, local, territorial or other government, which includes to the extent applicable, Directive 95/46/EC, Directive 2002/58/EC, European Commission decisions and guidance) each as transposed into domestic legislation of each Member State or other country and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR, and any industry self-regulatory principles that are applicable in the location or region where the Services are provided or received, related to the Processing of Personal Data or the interception, recording or monitoring of communications.

“**DPA**” means Data Protection Agreement.

“**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 (General Data Protection Regulation).

“**Services**” means the provision of data, media, or services.

“**Four Media Network GmbH Personal Data**” means any Personal Data collected or received by you for and on behalf of Four Media Network GmbH or its clients, whether received from Data Subjects, third parties or Four Media Network GmbH.

“**EU Model Clauses**” means the standard contractual clauses approved by European Commission on standard contractual clauses for the transfer of Personal Data to Processors or Controllers established in third countries (but which shall exclude any contractual clauses designated by the European Commission as optional in that decision), as amended or replaced from time to time by the European Commission.

“**Interest-Based Advertising**” means any of:

- The collection of data across potentially multiple digital properties or other sources for the purpose(s) of profiling and delivering advertising based on preferences or interests known or inferred from the data collected.
- The collection of data about a user’s activity on or in one digital property or source for the purpose(s) of profiling and delivering advertising based on that data on a different digital property.

“**Sub-processor**” means any third party (including any Partner affiliate) appointed by or on behalf of Partner to Process Personal Data on behalf of Four Media Network GmbH.

The terms, “**Commission**”, “**Controller**”, “**Data Subject**”, “**Member State**”, “**Personal Data**”, “**Personal Data Breach**”, and “**Processing**”, and “**Supervising Authorities**” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

## **Partner agrees to the following:**

### **Legal Compliance**

You will comply with obligations under all Applicable Laws with respect to the Processing of Personal Data where applicable.

### **Data Security**

You confirm and can evidence that you have appropriate security measures in place to protect Personal Data, including appropriate technical and organizational measures, to protect against unauthorized or unlawful Processing and against accidental loss, destruction or damage. In particular, you shall establish prior to the beginning of the processing of Customer Data and maintain throughout the term of the Main Agreement the technical and organizational measures as specified in **Annex 1** to this Addendum and ensure that the processing of Customer Data is carried out in accordance with those measures.

### **Fair Processing**

You confirm you will treat Four Media Network GmbH Personal Data as confidential and Process any Four Media Network GmbH Personal Data only in accordance with the written instructions of Four Media Network GmbH within the meaning of Art. 28 GDPR (Processing on Behalf) and will not use or Process any Four Media Network GmbH Personal Data for any purpose other than to provide the Services agreed or as otherwise agreed in writing, unless you are legally required to do so. In the latter case, you shall inform Four Media Network GmbH of that legal requirement before processing, unless taht law prohibits such information on important grounds of public interest. Four Media Network GmbH reserves the right to issue instructions about the type, extent, purpose and means of the processing of Customer Data. The subject-matter and details of the Four Media Network GmbH Personal Data being Processed shall be set out in any future agreements. If you become aware of any errors or inaccuracies in the Four Media Network GmbH Personal Data, you will notify Four Media Network GmbH promptly.

### **Handling of Personal Data**

You will take reasonable steps to ensure the reliability of any employees, affiliates, subcontractors, or agents (“Personnel”) engaged in the Processing of Personal Data. You confirm that any Four Media Network GmbH Personal Data to which you have access will be accessible only to your Personnel who:

- Are required for business reasons to have access.
- Are adequately trained on appropriate handling of Personal Data.
- Are subject (or will be subject to in the future) to contractual obligations of privacy, security, and confidentiality in respect of such Personal Data.

### **Consent & Acquisition**

You confirm that if you are an operator of a digital property (including for example websites and apps) through which Four Media Network GmbH collects Personal Data you have in place and can evidence, mechanisms for obtaining appropriate consent to such collection of Personal Data by means and for the purposes used by Four Media Network GmbH as set out in this DPA; and include a clear and unambiguous link to an easy-to-use mechanism that provides the Data Subject the ability to opt out, including where applicable the ability for a Data Subject to opt out of Interest-Based Advertising. You confirm that if you facilitate the provision to Four Media Network GmbH of Personal Data from digital properties operated by third parties you shall have in place legally enforceable obligations with such third parties requiring them to obtain appropriate consent and to enable you to

provide evidence of such consent to Four Media Network GmbH, for the means and for the purposes required for Four Media Network GmbH's use of such Personal Data as set out in this DPA. You will be responsible for providing any third party with any relevant information set out in this DPA and/or otherwise provided by Four Media Network GmbH in writing. You confirm that if you are a data provider to Four Media Network GmbH you have proof of appropriate consent (where applicable) of any Data Subject, whose Personal Data you share with Four Media Network GmbH and in all cases, such Data Subjects were provided with a clear and unambiguous option to an easy-to-use mechanism to opt-out, including where applicable the ability for a Data Subject to opt out of Interest-Based Advertising.

## **Data Use**

If your Services are provided in connection with Four Media Network GmbH's media planning or buying activities and you are uncertain of the technology we use in relation to Personal Data (including when collecting it) and how we will use Personal Data provided by you, please submit a request to Four Media Network GmbH for further information at [GDPR@4media-network.com](mailto:GDPR@4media-network.com).

Generally, Four Media Network GmbH uses Personal Data for purposes related to its online advertising activities, including without limitation:

- Interest-Based Advertising and modelling.
- Bidding, optimization, forecasting, audience planning, creative strategy, and custom ad creation.
- Providing inventory and other product offerings.
- Visualization, analytics and reporting, in each case on its own behalf and on behalf of its respective customers and always subject to the terms of the applicable Agreement.

## **Privacy Policy & Opt-out**

If you are an operator of a digital property through which Personal Data is collected and provided to us you will ensure that you have a privacy notice that complies with Applicable Laws. You will name Four Media Network GmbH as a party for and/or by whom Personal Data is collected through your digital property. If you facilitate the provision to Four Media Network GmbH of Personal Data from digital properties operated by third parties you will contractually require your relevant contracting parties to ensure that each relevant digital property has a privacy notice that complies with Applicable Laws. If applicable, you will require that such third parties name Four Media Network GmbH as a party for and/or by whom Personal Data is collected through such third party digital property. If you are a data provider to Four Media Network GmbH you warrant and represent that all parties collecting or receiving Personal Data from Data Subjects which is made available by you to Four Media Network GmbH ("Partner Data") have a privacy notice, that clearly and unambiguously discloses the collection, provision and usage of Partner Data, including without limitation descriptions of data collection for Interest-Based Advertising by Four Media Network GmbH, in compliance with Applicable Laws and provides an easy-to-use mechanism that enables the Data Subject to opt out (including where applicable the ability for a Data Subject to opt out of Interest-Based Advertising) through the services provided by Partner or its data sources. If you Process Four Media Network GmbH Personal Data you will ensure that you have an accessible, up-to-date privacy notice explaining the technology that you use and how you Process Personal Data.

## **Breach of Personal Data**

You confirm that in the event of a Personal Data Breach which involves Four Media Network GmbH Personal Data you will:

- Promptly take all necessary and appropriate corrective action to remedy the underlying causes of the Personal Data Breach and make reasonable commercial efforts to ensure that such Personal Data Breach will not recur.
- Notify Four Media Network GmbH without delay, and in any event within twenty-four (24) hours, providing reasonable detail of the Personal Data Breach and likely impact on Data Subjects.
- Take any action required by Applicable Law and/or at the reasonable request of Four Media Network GmbH.

Four Media Network GmbH shall make the final decision on notifying (including the contents of such notice) Four Media Network GmbH's clients, employees, service providers, Data Subjects and/or the general public of

such Personal Data Breach, and the implementation of the remediation plan, to the extent Four Media Network GmbH Personal Data is concerned.

### **Holding and destroying Personal Data**

You will ensure that any Four Media Network GmbH Personal Data in your possession is returned to Four Media Network GmbH or destroyed, each at Four Media Network GmbH's election, when it is no longer required for the performance of the Services agreed, or within a reasonable time taking into consideration the type of Personal Data.

### **Rights of Data Subjects**

You confirm you have the means and will take all reasonable action to allow us to comply with reasonable requests from Data Subjects (in relation their rights under Article 12-22 of GDPR) if we have shared their Personal Data with you.

### **Sensitive/ Special Personal Data**

You confirm you will not share any sensitive/special categories of Personal Data, as defined in Article 9 and 10 of GDPR, with Four Media Network GmbH unless expressly agreed in writing.

### **Transfers**

You confirm you will not transfer, and will ensure that any subcontractor does not transfer, Four Media Network GmbH Personal Data out of the country in which it is provided to you, except **1.** between member states of the European Economic Area ("EEA"); or **2.** on the written instructions of Four Media Network GmbH. If you transfer Four Media Network GmbH Personal Data outside of the EEA, you will promptly enter (or require, in the case of a transfer by or to a subcontractor, that that subcontractor promptly enters) into an agreement with the relevant parties on appropriate EU Model Clauses or equivalent. Any transfer by you of Personal Data to Four Media Network GmbH agencies outside of the EEA will be made on relevant EU Model Clauses.

### **Third-party enquiries & DPO**

You confirm that you will have a Data Protection Officer (or a designated employee) who will be responsible for ensuring the lawful management of Personal Data and all related issues and who will be available to help Four Media Network GmbH, in a timely manner, should there be any enquiries received from Data Subjects or any competent data protection or privacy authority, in relation to Personal Data Processed by you. You confirm, you will give Four Media Network GmbH such assistance and information as it may reasonably request, in a timely manner, to assist Four Media Network GmbH to comply with its obligations under GDPR, in relation to any Four Media Network GmbH Personal Data.

### **Sub-processors**

Four Media Network GmbH authorises you to appoint Sub-processors in accordance with this section and Article 28 of GDPR. You may continue to use those Sub-processors already engaged by you as of the date of this DPA, subject to Partner in each case, as soon as practicable, meeting the obligations set out in this section and Article 28 of GDPR. Please list all existing Sub-processors in **Annex 2**. You shall give Four Media Network GmbH prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor.

With respect to each Sub-processor, you shall:

- Before the Sub-processor first Processes Four Media Network GmbH Personal Data carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Four Media Network GmbH Personal Data required by Applicable Laws and this DPA.
- Ensure that the Sub-processor executes a written contract including terms which offer at least the same level of protection for Four Media Network GmbH Personal Data as those set out in this DPA and meet the requirements of Applicable Law.
- Upon reasonable request provide to Four Media Network GmbH for review such copies of the agreements with Sub-processors (which may be redacted to remove confidential commercial

information not relevant to the requirements of this DPA) as Four Media Network GmbH may reasonably request from time to time.

- Be liable for the acts and omissions of its Sub-processors to the same extent Partner would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

## **Auditing**

You confirm that you will cooperate fully with any reasonable requests for information from Four Media Network GmbH and/or Four Media Network GmbH clients about your Processing of Personal Data. To the extent necessary to enable all parties to comply with their obligations under Applicable Laws you will permit Four Media Network GmbH and/or Four Media Network GmbH clients to conduct an audit of your compliance with this DPA and Applicable Laws.

## **Data Protection Impact Assessment**

You shall provide reasonable assistance to Four Media Network GmbH with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Four Media Network GmbH reasonably considers to be required by Article 35 and/or 36 of the GDPR or equivalent provisions of any other Applicable Law, in each case solely in relation to Processing of Four Media Network GmbH Personal Data by, and taking into account the nature of the Processing and information available to, the Partner.

## **Order of Precedence**

You acknowledge and agree that the terms and conditions of this DPA shall complement and supplement any existing agreements between Partner and Four Media Network GmbH. Nothing in this DPA reduces your obligations under any other agreements as aforementioned in relation to the protection of Personal Data, nor permits you to Process (or permit the Processing of) Personal Data in a manner which is prohibited under previously existing agreements with Four Media Network GmbH. In the event of any conflict or inconsistency between this DPA, the EU Model Clauses and a pre-existing Agreement with regards to data protection, the order of precedence shall be:

1. Model clauses.
2. This DPA.
3. Any previously existing agreement.

## **Changes in Applicable Laws**

Four Media Network GmbH may:

- By at least 30 (thirty) calendar days' written notice to you, make any variations to the EU Model Clauses which are required as a result of any change in, or decision of a competent authority under Applicable Law to allow those restricted data transfers to be made without breach of that Applicable Law
- Propose any other variations to this DPA which Four Media Network GmbH reasonably considers to be necessary to address the requirements of any Applicable Law.

If Four Media Network GmbH gives such a notice Partner shall promptly co-operate (and ensure that any affected Sub-processors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place with Sub-processors.

## **Acceptance of Partner**

Partner agrees that the terms and conditions of this DPA shall take effect and shall complement and supplement any existing agreements between Partner and Four Media Network GmbH, or where no such agreement exists, the terms and conditions of this DPA shall act as binding contractual commitments entered into in consideration of the mutual cooperation between Four Media Network GmbH and Partner to facilitate both parties compliance with Applicable Law.

Partner Name XXXX

Signed .....

Name .....

Title .....

Date .....

## Annex 1 - Security Requirements

### GENERAL REQUIREMENTS

1. You must not carry out any act or make any omission which has, or could reasonably be expected to have, an adverse impact on the Four Media Network GmbH's systems or personal data.
2. You further undertakes to:
  - a. comply with the level of security stipulated in this appendix;
  - b. secure personal data when processing it on behalf of the Four Media Network GmbH in relation to the provision of the service in such a way as to prevent destruction, alterations, blocking, unauthorized disclosure or access, copying, distribution or any other kind of unauthorized processing

### SECURITY STANDARDS

3. You must, if Section 4 below is not applicable, be certified and/or accredited by the [Mail your choice of standard from the list below to [gopr@4media-network.com](mailto:gopr@4media-network.com)] standard/accreditation when providing the service under this Data Processing Agreement to the Four Media Network GmbH. In cases where you have chosen to certify and/or accredit only parts of its Information Security Management System (ISMS) or infrastructure, you must provide assurance that the parts used to provide the service to the Four Media Network GmbH are included in the scope of certification/accreditation.

| Global standards  | Standard                       |  |  |
|---|--------------------------------|--|--|
|   | United States                  | Asia-Pacific   | Europe                                     |
| CSA (Cloud Security Alliance)<br>ISO 27001<br>ISO 27017<br>ISO 27018<br>PCI DSS<br>SOC 1<br>SOC 2 | FIPS<br>FISMA<br>HIPPA<br>NIST | IRAP (Australia)<br>K-ISMS (Korea)<br>MTCIS Tier 3 (Singapore) | C5 (Germany)<br>Cyber Essentials Plus (UK) |

### IN LIEU OF SECURITY STANDARDS

4. If you are not certified and/or accredited against any of the standards mentioned in Section 3 above, you must be able to demonstrate the following:

### RISK MANAGEMENT

5. You must have a risk assessment process that defines the criteria for performing a risk assessment, as well as the risk acceptance criteria. The risk assessment process must be repeatable and produce concise and valid results.
6. The risk assessment process must identify the appropriate risk owners (for each risk) and identify risks associated with the loss of confidentiality, integrity, availability and accountability.
7. The results of the risk assessment must form the basis for the risk treatment plan, in accordance with the risk criteria set by you. The risk treatment plan must identify the risk treatment options and define the controls used to address the identified risks.

### INFORMATION SECURITY POLICY

8. You must have an information security (IS) policy, which is approved by management, published and communicated to all employees and relevant external parties. The policy must be kept updated and must be reviewed on an, at least, annual basis.

## **ORGANIZATION OF INFORMATION SECURITY**

9. You must define and assign information security responsibilities within the organization. You can assign the responsibility for information security to a single role or multiple roles, but you must provide a single contact point for any information security communication between you and the Four Media Network GmbH.

## **HUMAN RESOURCE SECURITY**

10. In case where you process sensitive personal data on behalf of the Four Media Network GmbH, you must utilize background checking for employees that will handle the Four Media Network GmbH's sensitive personal data. The candidate must be informed in advance of the obligations undertaken by you on behalf of the Four Media Network GmbH and agree to operate within the defined framework.
11. You must have a training and awareness program that covers your information security policy and your obligations against the Four Media Network GmbH.
12. You must have an established process for termination or change of employment duties. The process must ensure that access to the Four Media Network GmbH's data is removed as soon as the employee terminates their contract with you or the employee moves to a position that is not related to the tasks undertaken by you on behalf of the Four Media Network GmbH.

## **ASSET MANAGEMENT**

13. You will maintain an inventory of assets related to the processing of the Four Media Network GmbH's personal information. The Four Media Network GmbH reserves the right to request this inventory to be produced in cases where the Four Media Network GmbH needs to demonstrate to the regulatory authority that personal information is kept in documented assets.
14. You should have documented rules for the acceptable use of the assets that process personal data. The documentation should also define an asset owner for each of the assets that process personal information.
15. You must have documented processes for the destruction of media that contain personal information. These processes must also define rules for secure media transfer if applicable.

## **ACCESS CONTROL**

16. You must have a document access control policy. The access control policy must define: 1) How access is provided to the system(s) that manage the Four Media Network GmbH's data, 2) Who approves the access, 3) How access is monitored. Access must be allocated in accordance with the principle of least privilege.
17. Access to the system(s) that process personal information on behalf of the Four Media Network GmbH must be allocated through the use of individual identifiers (e.g. usernames). You must be able to account for any activity undertaken by your employees.
18. Access to the system(s) that process personal information on behalf of the Four Media Network GmbH must be reviewed in regular intervals. Any deviations identified must be immediately notified to the Four Media Network GmbH.
19. You must use well-known and established authentication methods to authenticate the users of the system(s) that process personal. If you do not provide any 2FA/MFA <sup>1</sup> mechanisms for authentication, then the passwords must satisfy sections 5.1.1.1 and 5.1.1.2 of the NIST 800-63B guideline<sup>2</sup>.

---

<sup>1</sup> 2FA: 2-factor authentication, MFA: Multi-factor authentication

<sup>2</sup> <https://pages.nist.gov/800-63-3/sp800-63b.html>



## **CRYPTOGRAPHY**

20. You should, and where sensitive data is being processed on behalf of Four Media Network GmbH must, utilize encryption to protect the Four Media Network GmbH's data while in transit and at rest. The encryption mechanism chosen should not be developed by you, unless it has been peer-reviewed and approved for use by a reputable authority / institution. The encryption algorithms used must be in accordance with FIPS 140-2 Annex A<sup>3</sup>.
21. When you utilize SSL/TLS technology, you must ensure that all communications take place over TLS v1.2 (or higher). The digital certificates used must be issued by a reputable Certificate Authority (CA)<sup>4</sup>.

## **PHYSICAL AND ENVIRONMENTAL SECURITY**

22. You must define secure areas for all locations (offices, information processing facilities) where the Four Media Network GmbH's personal information are being processed. The secure areas must be protected by appropriate entry controls and must protected against external and environmental threats.
23. You should apply a policy for clear desks and clear screens, for the parts of your organization that processes personal information on behalf of the Four Media Network GmbH.
24. You must establish a process for secure disposal of information and re-use of equipment. You must be able to demonstrate that the retention periods defined by the Four Media Network GmbH are observed and that the Four Media Network GmbH's data are securely disposed if you decide to re-use equipment for activities not related to the tasks undertaken on behalf of the Four Media Network GmbH.

## **OPERATIONS SECURITY**

25. You must have a change management program in place. Any changes to the organization, business processes and information processing facilities that affect the tasks undertaken on behalf of the Four Media Network GmbH must be documented, tested and controlled. At a minimum, you must:
  - Maintain a record of proposed, rejected and executed changes.
  - Document the purpose of the change, the time, the requester, the approver and the back-out plan (in case of failure).
  - Document the outcome of the change.
26. You should have a capacity program in place in the context of the service provided to the Four Media Network GmbH. The capacity management program should monitor for current utilization, produces reports and create projections for the future of the service.
27. You must have separate environments for development, testing and operation purposes. Access to these environments should be allocated based on the principle of least privilege.
28. You must have detection, prevention and recovery controls to protect against viruses, malware, Trojans or any other type of malicious code.
29. You must maintain back-ups that will allow the restoration of the service in case of an incident. Any data provided by the Four Media Network GmbH can be excluded from the backup process upon approval from the Four Media Network GmbH. Unless the Four Media Network GmbH provides a written approval for exclusion from backup of the Four Media Network GmbH's data it's implied that these data will be part of the backup process.
30. You must have an event logging facility that records user activities, exceptions, faults and information security events. The Four Media Network GmbH maintains the right to request access to the event logs that are relevant to the service provided by you.

---

<sup>3</sup> <https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf>

<sup>4</sup> <https://ccadb-public.secure.force.com/mozilla/CACertificatesInFirefoxReport>

31. You must have a technical vulnerability management program that identifies vulnerabilities on the system(s) used to provide the service to the Four Media Network GmbH. The vulnerability management program must: 1) Identify vulnerabilities in a timely fashion, 2) Assess the exposure, 3) Propose remediation activities.

#### **COMMUNICATION SECURITY**

32. You must establish network controls to protect access to systems and applications that process data on behalf of the Four Media Network GmbH (e.g. firewall, web application firewall, IDS, etc.).
33. You should segregate the network that offers services to the Four Media Network GmbH for networks used for other Data Controllers or your own processes. In the case where you decide to not employ network segregation, the you must demonstrate to the Four Media Network GmbH how segregation of information is achieved.
34. You in cooperation with the Four Media Network GmbH must document the appropriate and relevant communication channels, both for the execution of the services as well as the management of the service. The documentation must include the names (or roles) of people who are allowed to request changes to the service.

#### **SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**

35. You must have a secure development policy that applies to all areas of your organization that operate within the software development areas.
36. You must establish, document, maintain and apply principles for engineering secure systems for all the information processing systems that process data on behalf of the Four Media Network GmbH.
37. You must supervise and monitor all activities related to outsourced development (sub-contractors of you).
38. You must perform testing of security functionality during the development process. The Four Media Network GmbH reserves the right to request a report from you that demonstrates that security testing has been successfully passed.
39. You must not use “live” (production) data for the development or testing activities. Any data used for the development and testing activities must be anonymized.

#### **INCIDENT MANAGEMENT**

40. In addition to what is stated in the Data Processing Agreement regarding data breach, you must establish responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and data breaches.
41. You must report any information security incidents or data breaches to the Four Media Network GmbH, as soon as the incident or breach is identified and within 24 hours by the latest. The communication channels, in order of preference are: 1) Email to xxx, 2) Open a ticket in xxx, 3) Call xxx
42. In the case of an incident / breach, you must collect all relevant evidence and make them available to the Four Media Network GmbH.

#### **BUSINESS CONTINUITY**

43. You must have a business continuity / disaster recovery plan that ensures that the service provided to the Four Media Network GmbH can be restored as soon as possible.

44. You must verify, review and evaluate the business continuity / disaster recovery plan. The Four Media Network GmbH reserves the right to request access to the results of the plan verification.

#### **COMPLIANCE**

45. You must process the data in accordance with the data retention periods defined by the Four Media Network GmbH.
46. In accordance with what is stated in the Data Processing Agreements, you must assist the Four Media Network GmbH with any Data Subject Access Requests received by the Four Media Network GmbH and require access to information known only to you to be fulfilled.
47. You must ensure that all information provided to the Four Media Network GmbH in relation to the service, at the time of signing remain accurate and updated (e.g. location of data processing, technology used, etc.).
48. You should commission independent reviews of their information security posture on timed intervals or when significant changes take place.

**Annex 2 – Sub-processors**

| <b>Name of Sub-contractor</b> | <b>Role</b> | <b>Services</b> | <b>DPA</b> | <b>More Information</b> | <b>URL referring to GDPR</b> |
|-------------------------------|-------------|-----------------|------------|-------------------------|------------------------------|
|                               |             |                 |            |                         |                              |
|                               |             |                 |            |                         |                              |
|                               |             |                 |            |                         |                              |
|                               |             |                 |            |                         |                              |
|                               |             |                 |            |                         |                              |

Mail your List of Sub-contractors to [gpr@4media-network.com](mailto:gpr@4media-network.com).