



DATA PROCESSING AGREEMENT

INTRODUCTION

This Data Processing Agreement (“DPA”) applies to all customers (“Customer” or “Controller”) who use the advntg.ai Services provided by ASOL INCORPORATED, a Delaware corporation (“ASOL”, “Provider”, or “Processor”).

This DPA forms part of any service engagement, subscription, order form, or master services agreement between the Customer and ASOL, and applies automatically whenever ASOL processes Personal Data on behalf of the Customer.

DEFINITIONS

The following definitions apply when interpreting this DPA:

CUSTOMER

Means any business, entity, or organisation that enters into a commercial relationship with ASOL INCORPORATED and uses the advntg.ai Services. The Customer determines the purposes and means of processing Personal Data.

PROVIDER” / PROVIDER

Means ASOL INCORPORATED, acting as a processor when handling Personal Data on behalf of the Customer.

SERVICES

Means the advntg.ai platform and any related technologies, APIs, dashboards, automation tools, ad-distribution infrastructure, analytics, or other functions made available by ASOL to the Customer.

MASTER SERVICE AGREEMENT (MSA) or ORDER FORM AGREEMENT (MSA) or ORDER FORM

Means any agreement, commercial terms, order form, subscription, proposal, or contract entered between the Customer and ASOL describing the Services purchased. If no separate written MSA exists, the Customer’s use of advntg.ai constitutes acceptance of the ASOL Terms of Service, and this DPA applies by reference.



CODES

Means any tracking scripts, SDKs, pixels, or other technical implementations provided by ASOL that the Customer may deploy in their systems or advertising channels.

AUTHORISED PERSONS

Means individuals within the Customer's organisation who are approved to instruct ASOL regarding processing of Personal Data.



ANNEX 2

DATA PROCESSING AGREEMENT

PARTIES

1. **CUSTOMER** and PROVIDER
2. **ASOL INCORPORATED**, a company incorporated and registered in Delaware, with its registered office at **8 The Green, STE D, Dover, DE 19901. (ASOL)**.

BACKGROUND

- a. CONTROLLER and ASOL entered into a Master Services Agreement dated commencement date stated in order form (**Master Agreement**) that requires ASOL to process Personal Data on behalf of CONTROLLER.
- b. This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which ASOL will process Personal Data when providing services under the Master Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.
- c. ASOL is based in the United States of America (**USA**) and maintains its infrastructure and its subcontractors for the purposes of Personal Data processing in the USA and EU in all cases governed by the EU-US Data Privacy Framework and similar frameworks ensuring the highest adequacy level of data protection for the purposes of the EU GDPR and other applicable data protection regimes.

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

- a. **Authorised Persons**: the persons or categories of persons that CONTROLLER authorizes to give ASOL personal data processing instructions.



- b. **Anonymous Aggregated Data:** means a data set that is derived from the combination of End User Data with other data so that its results are aggregated and anonymized in such a manner that it is not identifiable in any way to any person or entity (including CONTROLLER) and cannot be reversed in any way to enable such connections.
- c. **Business Purposes:** the services described in the Master Agreement or in Annex A hereto.
- d. **Data Subject:** means also the **End User**, i.e. the end users who have interacted with, or viewed, Customer's advertising and marketing materials, or who use or have used Customer's Applications, websites, products, and/or services.
- e. **End User Data** means such data concerning the characteristics and activities of End Users, such as technical information about End User devices (e.g., type, model, OS, language), technical identifiers (e.g., advertising ID's, IP address, device ID's), and engagement information (e.g., advertisements clicked and viewed, in-app events and purchases), all as further described in the ASOL's Privacy Policy.
- f. **Personal Data:** means any information relating to an identified or identifiable natural person that is processed by ASOL as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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.
- g. **Processing, processes and process:** either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes 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. Processing also includes transferring Personal Data to third parties.
- h. **Data Protection Legislation:** all applicable privacy and data protection laws including the General Data Protection Regulation ((EU) 2016/679) and any applicable national implementing laws, regulations and secondary legislation in the United States of America, European Economic Area and any other affected countries relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time.
- i. **Personal Data Breach:** 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.
- j. **Restricted Data:** shall mean: (i) name and contact details (e.g., address, phone numbers); (ii) financial information (e.g., bank account numbers, credit/debit card information, or any information regulated under the Gramm–Leach–Bliley Act); (iii) any health or medical information (including information regulated under the Health Insurance Portability and Accountability Act); (iv) government IDs or ID numbers (e.g., driver's license, passport, national ID, social security number, TIN or EIN numbers); (v)



any information regarding children (i.e., under the age of 16 (sixteen) or as otherwise defined by applicable children protection laws (“**Children**”)), including the Children’s Online Privacy Protect Act) including any End User Data related to Children, unless appropriate parental consent has been obtained by Customer; (vi) any information defined as ‘Special Categories of Data’ under Article 9 of the GDPR (e.g., biometric or genetic data, information about one’s religious beliefs, race, sex life or orientation); and (vii) any personally identifiable information other than End User Data that is afforded protection under specific regulation or laws.

- k. **Sub-processor:** means a third-party service provider that ASOL engages to assist in processing the Personal Data on behalf of the CONTROLLER.
- l. **Subcontractor:** means a third-party service provider that ASOL engages to assist in servicing the CONTROLLER which may or may not involve processing the Personal Data depending on the details of the specific tasks and data types given by the CONTROLLER to ASOL in accordance with the Master Agreement.

1.2 This Agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Agreement.

1.3 Annex A and B form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes Annex A and B.

1.4 A reference to writing or written includes faxes, email and electronic messaging service.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in Annex A, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in Annex A, the provision contained in Annex A will prevail;

(c) any of the provisions of this Agreement and the provisions of the Master Agreement, the provisions of this Agreement will prevail.

2. Personal data types and processing purposes



2.1 CONTROLLER and ASOL acknowledge that for the purpose of the Data Protection Legislation, CONTROLLER is the controller and ASOL is the processor.

2.2 CONTROLLER retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents or any other applicable lawful grounds for personal data processing, and for the processing instructions it gives to ASOL.

2.3 ANNEX A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which ASOL may process to fulfil the CONTROLLER's assignments in accordance with the Master Agreement.

2.4. ANNEX B is a list of Sub-processors and subcontractors engaged by ASOL to fulfill the CONTROLLER's assignments in accordance with the Master Agreement.

3. Data processing and Parties' rights and duties

3.1 In the course of providing its Services to the CONTROLLER, ASOL will accept CONTROLLER's End User Data (Personal Data) for processing in the scope and for the purposes as described by this Data Processing Agreement.

3.2 ASOL will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with CONTROLLER's written instructions from Authorised Persons. ASOL will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or Data Protection Legislation. ASOL must promptly notify CONTROLLER if, in its opinion, CONTROLLER's instruction would not comply with Data Protection Legislation.

3.3 CONTROLLER shall ensure that all End User Data provided to ASOL is either (i) anonymized in a way that prevents the identification of any individual or (ii) transferred with all applicable requirements of the Data Protection Legislation being satisfied, such as the explicit consent of the Data Subject as the case may be.

3.4 ASOL expressly reserves that it will not accept for processing any Restricted Data. Both ASOL and CONTROLLER hereby agreed that it is the CONTROLLER's duty to verify that none of the Restricted Data are provided to ASOL for processing. CONTROLLER acknowledges and agrees that regardless of its technical ability to do so, CONTROLLER shall not configure the Services or Codes to enable the collection of Restricted Data through the Services. Additionally, CONTROLLER agrees that when it becomes aware or should reasonably be aware that the End User Data may be Restricted Data, for example data collected from Children, it must configure the Codes and Services appropriately to ensure compliance with applicable data protection and privacy laws



(including the Children's Online Privacy Protection Act), for example, by implementing an opt-out from data collection when parental consent required by law is not obtained by Customer.

3.5 ASOL must promptly comply with any of CONTROLLER's requests or instruction from Authorised Persons requiring ASOL to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.6 ASOL will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless CONTROLLER or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires ASOL to process or disclose Personal Data, ASOL must first inform CONTROLLER of the legal or regulatory requirement and give CONTROLLER an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.7 ASOL will reasonably assist CONTROLLER with meeting CONTROLLER's compliance obligations under Data Protection Legislation, taking into account the nature of ASOL's processing and the information available to ASOL, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.8 ASOL must promptly notify CONTROLLER of any changes to Data Protection Legislation that may adversely affect ASOL's performance of the Master Agreement.

3.9 ASOL may use Anonymous Aggregated Data for research and analytics purposes and improvement and marketing of the Services.

4. ASOL's employees

4.1 ASOL will ensure that all employees:

- (a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;
- (b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and
- (c) are aware both of ASOL's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.



4.2 ASOL will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable law on all of ASOL's employees with access to the Personal Data.

5. Security

5.1 ASOL must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data.

5.2 In its System, ASOL must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- (d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. Personal Data Breach

6.1 ASOL will promptly and without undue delay notify CONTROLLER if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. ASOL will restore such Personal Data at its own expense.

6.2 ASOL will immediately and without undue delay notify CONTROLLER if it becomes aware of:

- (a) any accidental, unauthorised or unlawful processing of the Personal Data; or
- (b) any Personal Data Breach.

6.3 Where ASOL becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide CONTROLLER with the following information:



(a) description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken, or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will coordinate with each other to investigate the matter. ASOL will reasonably cooperate with CONTROLLER in CONTROLLER's handling of the matter, including:

(a) assisting with any investigation;

(b) providing CONTROLLER with physical access to any facilities and operations affected;

(c) facilitating interviews with ASOL's employees, former employees and others involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by CONTROLLER; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.5 ASOL will not inform any third party of any Personal Data Breach without first obtaining CONTROLLER's prior written consent, except when required to do so by law.

6.6 ASOL agrees that CONTROLLER has the sole right to determine:

(a) whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in CONTROLLER's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.



6.7 ASOL will cover all reasonable expenses associated with the performance of the obligations under clause 6.2 and clause 6.4 unless the matter arose from CONTROLLER's specific instructions, negligence, wilful default or breach of this Agreement, in which case CONTROLLER will cover all reasonable expenses.

6.8 ASOL will also reimburse CONTROLLER for actual reasonable expenses that CONTROLLER incurs when responding to a Personal Data Breach to the extent that ASOL caused such a Personal Data Breach, including all costs of notice and any remedy as set out in clause 6.6.

7. Cross-border transfers of personal data

7.1 ASOL (or any Sub-processor) must not transfer or otherwise process Personal Data outside the United States of America (**USA**) and the European Economic Area (**EEA**) without obtaining CONTROLLER's prior written consent.

7.2 If any Personal Data transfer between CONTROLLER and ASOL requires execution of SCC in order to comply with the Data Protection Legislation, the parties will conclude such SCC accordingly.

8. Sub-processors and subcontractors

8.1 ASOL may authorise a third party, a Sub-processor or a subcontractor, to process the Personal Data and it hereby represents and guarantees, subject to clause 14 and 15, that:

(a) ASOL enters into a written contract with the Sub-processor or subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures;

(b) ASOL maintains control over all Personal Data it entrusts to the Sub-processor.

8.2 Where the Sub-processor or subcontractor fails to fulfil its obligations under such written agreement, ASOL remains fully liable to CONTROLLER for the Sub-processor or subcontractor's performance of its agreement obligations.

8.3 Where ASOL fails to fulfil its guarantees under clause 8.1, it shall indemnify all of the CONTROLLER's arising direct and indirect damages.

8.4 The Parties consider ASOL to control any Personal Data controlled by or in the possession of its Sub-processors.



8.5 ANNEX B shall enlist all ASOL's actual Sub-processors and subcontractors to date.

9. Complaints, data subject requests and third party rights

9.1 ASOL must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to CONTROLLER as CONTROLLER may reasonably require, to enable CONTROLLER to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on CONTROLLER by any supervisory authority under the Data Protection Legislation.

9.2 ASOL must notify CONTROLLER immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 ASOL must notify CONTROLLER within 30 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 ASOL will give CONTROLLER its full cooperation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 ASOL must not disclose the Personal Data to any Data Subject or to a third party other than at CONTROLLER's request or instruction, as provided for in this Agreement or as required by law.

10. Term and termination

10.1 This Agreement will remain in full force and effect so long as:

(a) the Master Agreement remains in effect, or

(b) ASOL retains any Personal Data related to the Master Agreement in its possession or control (**Term**).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Data will remain in full force and effect.



10.3 ASOL's failure to comply with the terms of this Agreement is a material breach of the Master Agreement. In such event, CONTROLLER may terminate any part of the Master Agreement authorising the processing of Personal Data effective immediately on written notice to ASOL without further liability or obligation.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 2 (two) months, they may terminate the Master Agreement on written notice to the other party.

11. Data return and destruction

11.1 At CONTROLLER's request, ASOL will give CONTROLLER a copy of or access to all or part of CONTROLLER's Personal Data in its possession or control in the format and on the media reasonably specified by CONTROLLER.

11.2 On termination of the Master Agreement for any reason or expiry of its term, ASOL will securely delete or destroy or, if directed in writing by CONTROLLER, return and not retain, all or any Personal Data related to this Agreement in its possession or control, except for one copy that it may retain and use for 3 (three) years for audit purposes only.

11.3 If any law, regulation, or government or regulatory body requires ASOL to retain any documents or materials that ASOL would otherwise be required to return or destroy, it will notify CONTROLLER in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 ASOL will certify in writing that it has destroyed the Personal Data within 30 days after it completes the destruction.

12. Records

12.1 ASOL will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for CONTROLLER, including but not limited to, the access, control and security of the Personal Data, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5.1 (**Records**).



12.2 ASOL will ensure that the Records are sufficient to enable CONTROLLER to verify ASOL's compliance with its obligations under this Agreement and ASOL will provide CONTROLLER with copies of the Records upon request.

12.3 CONTROLLER and ASOL must review the information listed in the Annex to this Agreement once a year or earlier subject to mutual consent to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 Shall CONTROLLER reasonably believe that a Personal Data Breach occurred or is occurring, or ASOL is in breach of any of its obligations under this Agreement or any Data Protection Legislation, ASOL will give CONTROLLER all reasonable assistance to conduct an audit. The assistance may include:

- (a) remote electronic access to, and copies of the Records and any other relevant information held at ASOL's premises or on systems storing Personal Data;
- (b) access to any of ASOL's personnel reasonably necessary to provide all explanations and perform the audit effectively; and
- (c) remote inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

13.2 If a Personal Data Breach occurs or is occurring, or ASOL becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, ASOL will:

- (a) promptly conduct its own audit to determine the cause;
- (b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;
- (c) provide CONTROLLER with a copy of the written audit report; and
- (d) promptly remedy any deficiencies identified by the audit.

13.3 At least once a year, ASOL will conduct audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.



13.4 ASOL will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by ASOL's management.

14. Warranties

14.1 ASOL warrants and represents that:

(a) its employees, Sub-processors, subcontractors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation relating to the Personal Data;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

- the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
- the nature of the Personal Data protected; and
- comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

14.2 CONTROLLER warrants and represents that:

(a) the End User Data (Personal Data) is provided to ASOL in a manner compliant with Clauses 3.3 and 3.4 of this Data Processing agreement; and

(b) the Business Purposes, the configurations of the Services and the instructions of the CONTROLLER will comply with the Data Protection Legislation.



15. Indemnification

15.1 ASOL agrees to indemnify, keep indemnified and defend at its own expense CONTROLLER against all costs, claims, damages or expenses incurred by CONTROLLER or for which CONTROLLER may become liable due to any failure by ASOL or its employees, Sub-processors, subcontractors or agents to comply with any of its obligations under this Agreement or the Data Protection Legislation.

15.2 CONTROLLER agrees to indemnify, keep indemnified and defend at its own expense ASOL against all costs, claims, damages or expenses incurred by ASOL or for which ASOL may become liable due to any failure by CONTROLLER or its employees, Sub-processors, subcontractors or agents to comply with any of its obligations under this Agreement or the Data Protection Legislation.

16. Data Subjects' Requests

The CONTROLLER's email address to be used by Data Subjects to submit any requests they may have in line with the Data Protection Legislation shall be: [REDACTED]

The CONTROLLER agrees that ASOL may provide this email to Data Subjects without prior notice.

17. Notice

17.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For CONTROLLER: [REDACTED], [REDACTED]

For ASOL: Anastasiia Solonovich, ceo@advntg.ai

17.2 Clause 17.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This agreement has been entered into on the date stated at the beginning of it.



ANNEX A

Personal Data Processing Purposes and Details that may be subject to Processing under the instructions of the CONTROLLER

Subject matter of processing:	Operation inside ASOL's System
Duration of Processing:	During the Term of the Master Agreement or of the respective Order Form
Nature of Processing:	Copying in the System, bulk computational analysis, advertisement campaigns
Business Purposes:	Automation of advertisement case management
Personal Data Categories:	<ol style="list-style-type: none">1. Basic Identifying Information<ul style="list-style-type: none">- Full Name- Date of Birth- Gender- Nationality- Address2. Contact Information<ul style="list-style-type: none">- Phone Number- Email Address- Social Media Handles3. Online & Technical Data<ul style="list-style-type: none">- IP Address- Device IDs- Cookies & Tracking Data- Browsing History4. Behavioral & Preference Data<ul style="list-style-type: none">- Purchase History- Interests & Hobbies- Communication Preferences
Data Subject Types:	Individuals



ANNEX B

LIST OF SUB-PROCESSORS AND SUBCONTRACTORS ENGAGED

	THIRD PARTY SERVICE	TYPE OF SERVICE	ENTITY COUNTRY	WEBSITE
1	AWS Amazon	Data Hosting in Germany (for EU/EEA clients) and in other countries (for non-EU/EEA clients)	Luxembourg	https://aws.amazon.com/
2	Google Cloud Platform	Data Storage, Data Analytics	EU Ireland	https://cloud.google.com/
2	Google Ireland Limited	Google Workspace	EU Ireland	www.google.com
3	Google Ireland Limited	Ads Provider	EU Ireland	www.google.com
4	Meta	Ads Provider	US	https://www.meta.com/
5	Slack Technologies Limited	Corporate internal workspace	EU Ireland	https://slack.com/intl/en-gb/
6	Microsoft	Digital Infrastructure	US	https://www.microsoft.com/
7	Hotjar	Behavior Analytics	EU Malta	https://www.hotjar.com/
8	Mixpanel	Digital Analytics	US	https://mixpanel.com/
9	Amplitude	Digital Analytics	US	https://amplitude.com/



10	AppLovin	Ads Provider	US	https://applovin.com/
11	Unity	Ads Provider	US	https://unity.com
12	Mintegral	Ads Provider	Singapore	https://www.mintegral.com/en

