Data Processing Agreement

Adway AB

Valid from 20250625.

1 General

The Parties have entered into an Agreement whereby the Processor undertakes to provide the Services on behalf of the Controller.

This DPA shall form an integral part of the Agreement and applies to all processing activities performed by the Processor on behalf of the Controller.

Processing shall be done solely for the purpose of delivering the Services, and in accordance with such instructions as contained in this DPA and its appendices, or that otherwise are given in writing by the Controller.

Depending on the Services used by the Controller different processing instructions applies, see Appendix 1. The Processor may update or modify the Services, provided such updates do not materially alter the agreed purposes, scope, or categories of personal data.

This DPA set out the rights and obligations of the Controller and the Processor when processing Personal Data under the Agreement. This DPA shall not exempt the Controller from any obligations the Controller is subject to pursuant to the GDPR or other Applicable Legislation.

This DPA have been designed to ensure the Parties' compliance with Article 28 (3) of the GDPR, but also other Applicable Legislation that may apply.

2 Definitions

The definitions specified in GDPR shall apply to the application of this DPA in addition to the defined terms in the DPA and any terms defined in the Agreement, including the General Terms & Conditions to the Agreement.

Agreement shall mean the SaaS agreement set out between the Controller and the Processor, under which the Processor undertakes to provide services to the Controller.

Applicable Legislation shall mean applicable legislation in the data protection and privacy area, such as, but not limited to GDPR, UK GDPR (GDPR, the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018) and CCPA (the California Privacy Rights Act of 2020).

Controller shall mean Data Controller, as defined in GDPR, and refers to Client of Adway AB.

DPA shall mean this Data Processing Agreement, as well as any appendices or signed amendments to the DPA.

GDPR shall mean 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)

Personal Data Breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processor shall mean Data Processor, as defined in GDPR, and refers to Adway AB.

Services shall mean any service the Processor provides to the Controller under the Agreement.

Sub-Processor shall mean such third parties involved by the Processor in the processing of Personal Data under this DPA.

3 Controller's Rights and Obligations

The Controller is to ensure an adequate legal basis for Processing Personal Data and that the Data Subjects are duly informed about the Processing.

The Controller has the right and obligation to make decisions about the purposes and means of the processing of Personal Data. This means that the Controller is responsible for that the processing of Personal Data under this DPA are lawful and do not violate any right of any third party.

4 Processor's Rights and Obligations

The Processor undertakes only to process Personal Data for the purpose of delivering the Services.

All processing shall be made in accordance with this DPA and its appendices, the Agreement, GDPR and other Applicable Legislation, and such written instructions that otherwise are given by the Controller.

If the Processor assesses that any instructions are insufficient, the Processor shall obtain additional instructions from the Controller.

Based on the nature of processing and insofar as this is possible, the Processor undertakes to reasonably assist the Controller with ensuring compliance with obligations such as security measures, breach notification, data protection impact assessments, as well as prior consultation with supervisory authorities where applicable.

5 Sub-Processors

The Processor shall have the right to involve Sub-Processors in the processing of Personal Data under this DPA.

The Sub-Processors access to Personal Data shall be restricted to what is necessary to maintain the Services or other products or services provided by the Processor to the Controller.

The Processor shall enter into data processing agreements with the Sub-Processors with the same obligations and undertakings as set out in this DPA.

The Processor may engage sub-processors as necessary to provide the Services. The Processor may engage new Sub-Processors for processing activities without any personal data, without prior approval from the Controller, provided:

- The Sub-Processor complies with GDPR and provides appropriate safeguards for Personal Data.
- The Processor updates the Controller through periodic updates or by maintaining an accessible list of active Sub-Processors.

For sub-processors processing Personal Data, the Processor shall provide information about the new sub-processor in advance and give the Controller a reasonable opportunity (7 days) to object. The Controller's objection shall be honoured if it is based on reasonable data protection concerns.

Sub-Processors used to provide the Services are listed in Appendix 2.

6 Transfer of Personal Data

Processor shall process Personal Data only within the EU/EEA, or such third country deemed to offer an adequate level of security by the European Commission, or by such suppliers that have entered into binding agreements that comply with the lawfulness of third country transfers.

7 Security

The Processor shall use reasonable efforts to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the processing operations involved, against unauthorized access, destruction, loss, or alteration.

The Processor shall implement at least the specific security measures as mentioned in Appendix 3 to this DPA.

8 Personal Data Breach

The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach.

The notification shall include, to the extent available to the Processor, at least the following:

- The nature of the Personal Data Breach including categories and approximate number of data subjects concerned and approximate number of personal data records concerned.
- The likely consequences of the Personal Data Breach.
- The measures taken or planned to be taken to address, and, as appropriate, mitigate, the Personal Data Breach.

In the event that it is not possible to provide all of the above information, the notification may be executed in phases without undue delay.

9 Contact with Data Subjects and Authorities

In case a Data Subject, a public authority, or any third-party requests information regarding the processing of Personal Data from the Processor, the Processor shall refer the request to the Controller.

The Processor is not entitled to represent the Controller vis-à-vis a third party in matters involving the processing of Personal Data, unless the Controller has expressly instructed so. However, this shall not prevent the Processor from fulfilling its obligations in the form of cooperating with a supervisory authority under Applicable Legislation. If possible and allowed, the Processor shall notify the Controller of such cooperation without delay, unless prohibited to do so.

The Processor shall, dependent on the information available to the Processor, at the Controller's sole cost, reasonably assist the Controller in presenting such information that has been requested by a public authority, or a Data Subject.

10 Confidentiality

The Processor undertakes to limit access to Personal Data to those individuals who require such access to deliver the Services.

The Processor shall ensure that any individual with access to Personal Data are bound by confidentiality. For the avoidance of any doubt, the confidentiality obligation shall not apply to the extent the Controller has granted explicit permission to provide the information to third parties, the provision to third parties is reasonably necessary considering the nature of the assignment to Controller or the provision is legally required.

11 Audits

The Processor shall, at the request by the Controller, make available all information to demonstrate compliance with Applicable Legislation and this DPA.

Upon written notice provided at least thirty (30) days in advance the Controller shall have the right to request an audit to verify that the Processor complies with the Agreement and this DPA, and all issues reasonably connected thereto.

The Processor shall give its full cooperation to the audit and shall make available employees and all reasonably relevant information, including supporting data such as system logs.

Audits may be conducted no more than once per year, except where required by applicable law, in response to a data breach, or upon a substantiated allegation of non-compliance. The Processor shall cooperate fully with such audits and provide relevant information within a reasonable timeframe. Audits must be limited to reviewing relevant documentation or certifications, and on-site audits are subject to prior approval and operational feasibility.

All audits must be conducted during Processor's regular business hours.

All audits must be performed in accordance with the Processor's security requirements.

The Controller may appoint an independent third party reasonably approved by the Processor. Any third party auditor is required to enter into a non-disclosure agreement directly with the Processor.

The costs of audits shall be borne by each Party for themselves.

If the Controller should find qualified and significant breaches or flaws in the processing of Personal Data, the Processor shall have the right to rectify such breaches or flaws within thirty (30) days. If the Processor is unable to rectify and comply with the DPA within thirty (30) days, Controller shall have the right to terminate this DPA and the Agreement effective immediately.

12 Erasure and Return of Personal Data

Upon termination of this DPA, the Controller may request that the Processor erase or return all Personal Data to the Controller and ensure that all Sub-Processors do the same. The Processor has sixty (60) days to complete such actions.

If the Controller has neither requested to erase or return the Personal Data within sixty (60) days from the termination of this DPA, the Processor shall be entitled to delete all Personal Data it has processed on behalf of the Controller. In such event, the Processor will completely delete the Personal Data from any medium where it is stored, in a way that it cannot be restored or recreated.

Notwithstanding, the Controller may keep data for product development and statistical reasons that is anonymised in such a way that the data can no longer be considered Personal Data, i.e. data by which an individual cannot be identified directly or indirectly either alone or in conjunction with any other data held by Processor or any other party.

13 Notification

Material changes to the Services, scope, or purposes of processing, or to this Agreement, will be communicated to the Controller at least 30 days in advance, unless immediate implementation is required for operational or regulatory necessity. In such cases, the Processor shall notify the Controller without undue delay. The Controller retains the right to object or terminate the agreement if the changes materially affect their rights or obligations, provided any objection is raised within 7 days of receiving notice.

14 Liability

The Parties explicitly agree that any liability arising in connection with Personal Data processing shall be as provided in the Agreement.

15 Term and Termination

This DPA enters into force upon signature by the parties and on the date of the last signature.

This DPA shall remain in force during the time the Processor is processing Personal Data for the Controller.

16 Miscellaneous

This DPA replaces any existing data processing agreement in place between the Parties. In case of any inconsistencies, this DPA will take precedence over the provisions of the Agreement.

If one or more provisions of this DPA is declared to be invalid or unenforceable, the remaining provisions will continue in full force and effect.

The Parties agree that they will make any necessary changes and amendments to this DPA in order for it to be compliant with GDPR and/or Applicable Laws with regard to precedents, and new or updated guidelines or other practices from a relevant authority.

17 Dispute and Applicable Law

Any dispute, controversy, or claim arising out of or in connection with this DPA, or the breach, termination, or invalidity thereof, shall be settled as stipulated in the Agreement.

The laws of Sweden shall govern this DPA and any dispute regarding this DPA.

Appendix 1 – Purpose of processing, data subjects, and categories of Personal Data

General Purpose

To provide Services under the Agreement to the Controller.

Depending on which specific Services used by the Controller, the type Processing Operations, Categories of Data Subjects, Purpose of the Processing, and Type of Personal Data that is processed differs. Please refer to detailed sub-appendices below.

Please note that below detailed sub-appendices only apply, to the extent the named service is used by the Controller.

Appendix 1A – Adway Connect (Platform)

Processing Operations	Providing the platform Adway Connect.
Categories of Data Subjects	Employees of the Controller.
Purpose of the Processing	Enable access to the platform and its functions.
Processing Activities	Storing, structuring, processing, reading, using, anonymising, and deleting of Personal Data.
Type of Personal Data that is processed	Log-in credentials; Usually name, username (typically email addresses), and password.
Sensitive Personal Data	No sensitive personal data is processed.
Retention Period	Following the Controller's written notice all Personal Data shall be deleted or anonymised in such a way that the data can no longer be considered Personal Data.

Appendix 1B – Social Media Advertising

Processing Operations	Automated social media job advertising service.
Categories of Data Subjects	Employees of the Controller. Individuals on images provided by Client to be included in the campaigns.

Purpose of the Processing	Email send-outs to hiring managers regarding campaigns.
Processing Activities	Storing, structuring, processing, reading, using, anonymising, and deleting of Personal Data.
Type of Personal Data that is processed	Name and e-mail addresses, or other contact information to hiring manager, as included in the job ad. Images, as provided by Client.
Sensitive Personal Data	No sensitive personal data is processed.
Retention Period	Following the Controller's written notice all Personal Data shall be deleted or anonymised in such a way that the data can no longer be considered Personal Data.

Appendix 1D – Candidate Management

Processing Operations	Provision of automated, fully customizable candidate journey and communications via SMS & email.
Categories of Data Subjects	Candidates (applicant, potential hires, and jobseekers) of the Controller.
Purpose of the Processing	Finding the right talent through nurturing, social talents pools and smart questions.
Processing Activities	Storing, structuring, processing, reading, using, anonymising, and deleting of Personal Data.
Type of Personal Data that is processed	Depending on what information is requested by the Controller, as well as what information is submitted by the Candidate, different Personal Data is collected and processed. Such information usually consists of names, emails, photos, and videos, information from Meta and LinkedIn and other social media accounts, answers to screening questions, titles, education, and other information provided by the candidates. It is the responsibility of the Controller to ensure the lawfulness of the processing of such data.

Sensitive Personal Data	Depending on what information is requested by the Controller, as well as what information is submitted by the Candidate, Sensitive Personal Data may be collected and processed. Sensitive Personal Data may consist of information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are considered as sensitive categories of personal data. Processing of sensitive Personal Data shall be made with extra care and security. If the Controller processes sensitive Personal Data using the Services, the Controller shall inform the Processor. It is the responsibility of the Controller to ensure the lawfulness of the processing of such data.
Retention Period	Following the Controller’s written notice all Personal Data shall be deleted or anonymised in such a way that the data can no longer be considered Personal Data. Any candidate data is stored 365 days as standard.
Privacy Policy	Controller is responsible for providing a link to Controller's Privacy Policy containing information on how Candidate Personal Data is processed by Controller.

Appendix 2 – Technical and Organisational Security Measures

The Processor shall implement at least the following specific technical and organisational security measures:

Technical Measures

1. **Data Encryption**: All data is encrypted both at rest and in transit to ensure confidentiality and integrity of personal data. All encryption is made in accordance with industry standards, including NIST SP 800-57.

2. **Access Controls**: Only authorized individuals can access Personal Data, based on the principle of least privilege. This means that only individuals requiring access to perform their job functions are granted access.

3. **Secure Authentication**: Multi-factor authentication (MFA) is enabled where possible and a strong password policy is implemented. All Adway employees and contractors uses secure password management systems to secure compliance with the password policy.

4. **Data Backup and Recovery**: Data backup is done daily, and recovery test, including a test of backup restoration processes, are done at least annually to ensure the availability and resilience of processing systems.

5. **Network Security**: Firewalls, anti-virus and malware, and centralised computer management to protect against unauthorized access are implemented.

6. **Regular Security Assessments**: Security assessments and vulnerability scans are conducted regularly to identify and mitigate risks.

Organizational Measures

1. **Data Protection Policies**: Comprehensive data protection policies and procedures are implemented.

2. **Employee Training**: Regular training on data protection and security awareness for all employees involved in data processing activities are implemented.

3. **Data Processing Records**: Detailed records of data processing activities, including the purpose of processing, data categories processed, and data recipients, is maintained and updated regularly.

4. **Incident Management and Reporting**: Procedures for managing data breaches, including detection, reporting, and investigation of personal data breaches are implemented.

5. **Vendor Risk Management**: Due diligence and risk assessments for third-party vendors and sub-processors are conducted regularly to ensure they comply with relevant data protection and security standards.

6. **Privacy by Design and Default**: Data protection principles are integrated into our processing activities and systems from the design phase and throughout the lifecycle.

Compliance Measures

1. **ISO 27001 Compliance**: Adway is ISO 27001 certified.

2. **GDPR Compliance Review**: Reviews assuring compliance with GDPR and Applicable Legislation, including data protection impact assessments for high-risk processing activities, is performed regularly.

3. **Data Protection Officer (DPO)**: Adway has an appointed DPO, to ensure compliance with data protection laws. DPO can be contacted at privacy@adway.ai.

Appendix 3 – Sub-Processors

Adway uses Sub-Processor in order to provide the Services to Controller, they may differ depening on the purpose of the services provided.

Sub-Processor	**AWS (Amazon Web Services) hosting by Amazon Web Services EMEA SARL**
Processing Location	EU
Processing Purpose	Web server hosting
Comments	Web server hosting is an online service that allows you to publish your website. No data storage.
ISO 27001 / SOC2	ISO 27001 & SOC2
DPA	Yes, standard DPA

Sub-Processor	**Atlas by MongoDB, Inc.**
Processing Location	EU
Processing Purpose	Data hosting
Comments	Data hosting, i.e. storage
ISO 27001 / SOC2	ISO 27001 & SOC2
DPA	Yes, standard DPA https://www.mongodb.com/legal/dataprocessing-agreement

Sub-Processor	**Sendgrid by Twilio, Inc**
Processing Location	US (DPF (EU-U.S. Data Privacy Framework) & EU SCC (Standard contractual clauses))
Processing Purpose	E-mail and SMS send-outs
Comments	Notifications of new campaigns going live etc
ISO 27001 / SOC2	SOC2

DPA	Yes, standard DPA https://www.twilio.com/enus/legal/dataprotection-addendum

Sub-Processor	**Auth0 by Auth0 Inc.**
Processing Location	EU
Processing Purpose	To provide SSO – Single Sign-On to Adway Connect.
Comments	Usually only name and email, but depending on what Client's internal settings
ISO 27001 / SOC2	ISO 27001 & SOC2
DPA	Yes, standard DPA

Sub-Processor	**DataDog by Datadog, Inc.**
Processing Location	EU
Processing Purpose	Logs over published campaigns.
Comments	Personal Data processed is generally limited to contact details to recruiter, as contained in the job ad.
ISO 27001 / SOC2	SOC2
DPA	Yes, standard DPA https://www.datadoghq.com/legal/data-processing-addendum/

Sub-Processor	**CloudAMQP - RabbitMQ by 84codes AB**
Processing Location	EU
Processing Purpose	Event queue system where all internal service messages are sent and received.
Comments	
ISO 27001 / SOC2	SOC2

DPA	Yes, standard DPA https://www.cloudamqp.com/legal/terms_of_service.html#dataprocessingagreement

Sub-Processor	**Vercel by Vercel Inc.**
Processing Location	EU (Function region)
Processing Purpose	Front-end apps hosting and caching.
Comments	Front-end apps hosting and caching.
ISO 27001 / SOC2	SOC2
DPA	Yes, standard DPA https://vercel.com/legal/dpa

Sub-Processor	**Algolia by Algolia, Inc.**
Processing Location	Multiple regions (EU SCC (Standard contractual clauses))
Processing Purpose	Search index service
Comments	Job and recruiter data used for search on Adway Explore (listing site)
ISO 27001 / SOC2	ISO 27001 & SOC2
DPA	Yes, standard DPA https://www.algolia.com/pdf/DPA-latest.pdf

Sub-Processor	**Twilio by Twilio, Inc.**
Processing Location	US (DPF (EU-U.S. Data Privacy Framework) & EU SCC (Standard contractual clauses))
Processing Purpose	SMS send out system
Comments	Used to send SMS reminders to candidates in Adway Convert.

ISO 27001 / SOC2	SOC2
DPA	Yes, standard DPA https://www.twilio.com/en-us/legal/data-protection-addendum

Sub-Processor	**Snowflake**
Processing Location	EU
Processing Purpose	Data warehouse
Comments	Collection of data and aggregation of data to be used in reports or analytics.
ISO 27001 / SOC2	ISO 27001 & SOC2
DPA	Yes, standard DPA https://www.snowflake.com/legal/data-processing-addendum/

Sub-Processor	**Intercom by Intercom R&D Unlimited Company**
Processing Location	EU
Processing Purpose	Support ticket system
Comments	Used for handling support tickets.
ISO 27001 / SOC2	ISO 27001 & SOC2
DPA	Yes, standard DPA https://www.intercom.com/legal/data-processing-agreement

Sub-Processor	**OpenAI API by OpenAI, LLC**
Processing Location	Multiple regions (EU SCC (Standard contractual clauses))

Processing Purpose	ISCO (International Standard Classification of Occupations) classification of job posts Automatic language detection for jobpost Image tag categorizing CV Parsing
Comments	
ISO 27001 / SOC2	SOC2
DPA	Yes, standard DPA https://openai.com/policies/data-processing-addendum

Sub-Processor	**Scrapin.io by VISUM SAS**
Processing Location	EU
Processing Purpose	Cleaning, correcting, synchronizing, enriching and organizing public Data from URL's offered by the Candidate
Comments	
ISO 27001 / SOC2	
DPA	Yes, standard DPA https://www.scrapin.io/data-processing-agreement