Data Protection Agreement

For Direct Path Publishers in Europe

1 Background and Purpose

Adnuntius AS (Processor) and the Customer as specified in the applicable Order Form (Controller) have entered into an agreement, where Processor delivers certain services (Services) to Controller under the applicable Order Form, which may involve Processing of Personal Data.

Processor and Controller (hereafter referred to as the Parties) therefore agree to supplement the Terms and Conditions of using the Services with this Data Processing Agreement, which has as its purpose to secure adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of data subjects, to describe the relationship between Controller and Processor and specify clear instructions for Processor, and to ensure that the Parties are made accountable applicable data to Applicable Data Protection Law.

2 Definitions

"Applicable Data Protection Law" means any applicable legislation protecting data subjects' right to transparency, control and/or privacy with respect to the processing of personal data. This includes but not limited to the EU General Data Protection Regulation 2016/679, and the Implementing Decision 914/2021/EU.

"Consent", "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "Processing", and **"Supervisory Authority"** and other terms in the GDPR mean the same as what is set out in the GDPR.

"GDPR" shall mean the EU General Data Protection Regulation 2016/679, including any future amendments such as, for example, those imposed by the Implementing Decision 914/2021/EU.

"Property" means the websites, mobile applications and/or other digital media properties owned or operated by the Controller, using Adnuntius' Services.

"Standard contractual clauses" shall mean the standard contractual clauses in the currently valid version, for the transfer of personal data to data processors established in third countries, laid down by the EU Commission implementing decision of 4 June 2021.

3 Processor's Obligations

3.1 Compliance. The Processor shall, when Processing Personal Data according to this agreement, comply with Applicable Data Protection Law. The processor shall not by commission or omission of actions put the Controller in a situation where the Controller is in breach of any provision of Applicable Data Protection Law.

3.2 Processing in accordance with instructions. The Processor shall process data solely according to the instructions of the Controller, as they are described in this data processing agreement's Exhibit 1. If the Processor is required to process data by law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 Assistance. The Processor shall, taking into account the nature of the processing, provide the Controller with reasonable cooperation and assistance to ensure that the Controller complies with its requirements under Applicable Data Protection Law, among other compliance with the obligations pursuant to GDPR Articles 32 to 36 and to respond to requests for exercising the data subject's rights laid down in GDPR Chapter III.

3.4 Tools to Opt Out. The Processor shall provide the Controller with solutions enabling data subjects to opt out of sharing Personal Data. These tools shall be made available in Adnuntius' privacy policy.

3.5 Limitation. The Processing shall be limited to the categories of personal data and categories of the data subjects as specified in the documents available in this Processing Agreement's Exhibit 1.

3.6 Control. The Controller retains the formal control of and all ownership to the Personal Data processed by the Processor and any Sub-Processors hereunder. The Processor shall not process them for the Processor's own purposes, unless required to do so by law to which the processor is subject.

3.7 Breach. In case of a data breach resulting in unauthorized disclosure of personal data, the Processor shall without undue delay notify the Controller in writing. The Processor shall without undue delay restore appropriate security levels and rectify any errors resulting in the breach.

3.8 Notification. If unable to fulfil its obligations under this Data Processing Agreement, the Processor shall without undue delay notify the Controller. The Processor shall also without undue delay notify the Controller if it reasonably suspects that instructions by the Controller are in breach with Applicable Data Protection Law, or if processing requires processing activities outside what is instructed by the Controller.

4 Use of Sub-Processors

4.1 Sub-contracting. The Processor may sub-contract any of its Processing activities pursuant to article 28 paragraph 4 of the GDPR. The processor shall inform the Controller about new sub-processors, and the Controller shall have the right to refuse new sub-processors within reason, or if the use of that sub-processor cannot be avoided, terminate the license agreement for the relevant service with 30 days' notice.

4.2 Transparency. The Processor's use of sub-processors shall be described and continuously updated in this Agreement's Exhibit 2. The Processor shall, if requested, share a copy of the Data Processing Agreement between the Processor and the sub-processors. The Processor shall have the right to censor any business critical information that can be reasonably be withheld before sharing such a copy.

5 Technical and Organizational Security Measures

5.1 Measures. The Processor shall implement and maintain appropriate technical and organizational security measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. These measures shall ensure a level of security appropriate to the risk presented to the processing and the nature of the personal data to be protected having regard to the state of the art and the cost of their implementation. The measures are described in this Agreement's Exhibit 3.

5.2 Limitation of access. The Processor shall limit access to Personal Data to relevant personnel who is committed to confidentiality.

5.3 Responsible person. The Processor shall have a responsible person and data protection officer taking responsibility for ongoing compliance with Applicable data protection law. The responsible are listed in this Agreement's Exhibit 4.

6 Audits

6.1 Audits. The Controller shall be allowed to perform annual audits. If the Controller chooses to perform such an audit, it shall be signaled to the Processor no less than 90 days in advance. The Controller shall perform such audit without causing significant interruptions to the Processor's regular operations.

6.2 Secrecy. The audit shall not grant the Controller access to trade secrets or proprietary information unless required to comply with Applicable Data Protection Law. The Controller shall ensure its personnel conducting such audit are subject to adequate secrecy obligations.

6.3 Auditor. If the parties agree that an audit is to be performed by external auditors, such external auditor is to be appointed by the Controller. The Processor may only oppose the appointment if such auditor is a competitor of the Processor. Upon security audits performed by an external auditor, both parties shall be entitled to receive a copy of the audit report.

6.4 Remediation. If the audit reveals non-compliance with this Data Processor Agreement, the Processor shall (and, if relevant, shall procure that the relevant Sub-processor shall) without undue delay remedy such inadequacy or non-compliance.

6.5 Cost. Each party shall cover its own costs associated with an audit.

7 Data Locations and Transfer

7.1 Transparency. The Processing activities shall take place on the locations specified in the documents available in this Exhibit 2.

7.2 Transfer. The Processor may transfer data if this is required by EU law or by any EU member state law to which the processor is subject, provided that the Processor informs the Controller of that legal requirement

before processing, unless that law prohibits such information on important grounds of public interest. Transfers can only be made to countries outside the EEA if such a transfer is in accordance with GDPR Chapter V.

9 Liability and Limitation of Liability

9.1 Liability. Each party is liable to the other for any direct loss, damage, cost, claim, fine and/or expense (any such a "Loss") incurred by the other Party, which arise from the first mentioned party's direct breach of its obligations under this Data Processing Agreement or acts of omissions in breach of applicable law. The Parties' respective liability is for direct Loss only and under no circumstance for indirect loss, such as loss of profit or opportunity or otherwise.

9.2 Limitation of liability. Each party shall hold each other harmless from and against any and all claims by third parties, including Supervisory Authorities, arising from the claim that Applicable Data Protection Law has been broken.

10 Term and Termination

10.1 Term. This Data Processing Agreement shall be effective from the Effective date on the applicable Order Form. This Agreement expires when cancelled by either Party in accordance with the General Terms and Conditions.

10.2 Removal of tracking mechanisms. Upon termination of the Data Processing Agreement the Controller shall immediately remove any tracking mechanisms used to send Personal Data for Processing. The Processor shall immediately cease to process the personal data, and shall if requested by the Controller delete Personal Data unless required by Applicable Data Protection Law to store such data, in which case the data shall not be actively used for any purpose other than required by law.

11 General Provisions

11.1 Governing law. The Data Processing Agreement shall be governed by and construed in accordance with the provisions of governing law set out in the General Terms and Conditions, save for mandatory provisions in Applicable Data Protection Law. Any dispute arising out of this Data Processing Agreement shall be resolved in accordance with the provisions on jurisdiction and dispute resolution set out in the General Terms and Conditions.

11.2 Changes. Adnuntius shall have the right to, from time to time, make changes to this Data Processing Agreement and its attachments under the condition that no such change violate Applicable Data Protection Law. Any change shall be communicated to Customer in writing no less than 30 days before the change takes place.

Exhibit 1: Processing Purposes

The Controller instructs the Processor to undertake the following Processing activities.

1 Personal Data Stored in Device Cookies

Purpose: Enable Controller to identify Data Subjects across multiple sessions and page views, and to build a history of advertisements shown to and interacted with by a Data Subject. The purpose of Processing is to enable advertisements to be controlled by frequency (how many times an ad has been shown to and interacted with by a Data Subject), and to target ads to Data Subjects based on their historic actions on Digital Properties where the Cookies are set.

All information is declared under https://delivery.adnuntius.com/.well-known/deviceStorage.json. The table below is provided for easier reading.

Device Cookies

Aa Name	Expiry	Purpose	Type
usi	30 days	Identify the user across multiple sessions (TCF: 1, 2, 4, 7)	Cookie
sessionId	Length of browser session	Identify the user session across multiple requests (TCF: 1, 2, 4, 7)	Cookie

Name	Expiry	Purpose	Type
i	30 days	Records a history of advertisements shown to the user (TCF: 1, 2)	Cookie
c	30 days	Records a history of advertisements shown to the user (TCF: 1, 2)	Cookie
v	30 days	Records a history of advertisements shown to the user (TCF: 1, 2)	Cookie
s	30 days	Records a history of advertisements shown to the user (TCF: 1, 2)	Cookie
r	30 days	Records a history of advertisements shown to the user (TCF: 1, 2)	Cookie
t	30 days	User retargeting. Records data about the user when they are browsing an advertiser's website, and then uses this data to select advertisements when the user is browsing a publisher's website. (TCF: 1, 4)	Cookie
cnv	30 days	Records the most recent time that a specific advertisement was seen by the user. Used to track conversions e.g. if the user subsequently performs an eligible action, such as purchasing a product, on the advertiser's website. (TCF: 1, 4)	Cookie
consent	No expiry	(*Deprecated*) Replaced by IAB TCF string and no longer read or written	Cookie
noCookies	No expiry	Records user cookie preference specified here: http://delivery.adnuntius.com/consent (TCF: 1)	Cookie
doNotTrack	No expiry	Records user tracking preference specified here: http://data.adnuntius.com/consent (TCF: 5)	Cookie
adn.metaData	Null	Stores the cookie data detailed above in the browser web storage (TCF: 1, 2, 4, 7)	Web

2 Viewing History Stored in Databases

Purpose: To allow control of how many times, per unit time, that an advertisement is shown to a Data Subject ("frequency capping"). For example: show an advertisement no more than twice per week to each Data Subject. This data replicates what is also stored in device cookie storage, but is also stored on the Adnuntius servers to allow cross-device frequency capping.

Personal information: User Identifier, list of advertisements, and timestamps.

Expiry: 30 days after last update.

Storage: See the sub-processor section.

3 Named Locations Derived from IP Addresses

Purpose: Enable advertisements to be targeted to Data Subjects' country, region, city and/or post/zip code.

Expiry: All information is discarded immediately after looking up and matching the information to a named location.

Storage: No location data is stored under this Purpose. The IP addresses are checked against named locations stored on our servers. No data is sent to any external party.

Storage: Adnuntius uses Maxmind, who supplies us with a file mapping IP addresses to named locations. This file is stored on Adnuntius servers (Hetzner) as described under "Sub-Processors".

4 Location from Longitude and latitude

Please note: this data is only processed if actively sent by the owner of the Digital Property showing the ad.

Purpose: Enable advertisements to be targeted to Data Subjects' exact location.

Expiry: All information is discarded immediately after any advertisements are matched to the location.

Storage: No location data is stored under this Purpose.

Storage: None.

5 Device Targeting

Data: As the user agent string is sent to Adnuntius with ad requests the following data is processed:

- Name, supplier and version of browser (example: Mobile Safari)
- Family, model, supplier and name of hardware (example: iPad Pro 9.7)
- Name, supplier and version of platform (example: Apple)
- Type of device (example: Desktop)
- Operating system (example: Android)

Purpose: Enable advertisements to be targeted to the Data Subjects' device.

Expiry: All information is discarded immediately after looking up and matching the collected information to device information stored on our servers.

Storage: No device data from Data Subjects is stored under this Purpose.

6 Segment Targeting: Page Content

Please note: this data is only processed if actively sent by the owner of the Digital Property showing the ad, or by the Controller (if they are not the same).

Data: Controller may send data such as page domain name, content categories and keywords of the page, device type used to view the page, and user (non-exact) location when viewing the page.

Purpose: Enable advertisements to target segments (Data Subjects grouped by their common behavior and/or characteristics) based on their consumption of pages on content owners', Controller's or its clients' Properties, and enable targeting based on these behaviors and characteristics.

Expiry: 30 days.

Storage: See the sub-processor section.

7 Segment Targeting: Profile Fields

Please note: this data is only processed if actively sent by the owner of the Digital Property showing the ad, or by the Controller (if they are not the same).

Data: Controller may send data such as firstName, lastName, title, dateOfBirth, age, gender, status, language, description, company, website, rank, level, type, emailPrivate, emailWork, phone, mobilePhone, addressLine1, addressLine2, state, city, areaCode, zipCode, postCode, region, country, educationName, educationType, educationDegree, educationSchool, educationField, educationStartYear, educationEndYear, skills, facebook, instagram, snapchat, twitter, avatar, transactions, lastLogin, logins, products, favouriteTopics, and personalInterests.

Purpose: Enable advertisements to target segments (Data Subjects grouped by their common behavior and/or characteristics) based on their submitted information on on content owners', Controller's or its clients' Properties, and enable targeting based on these behaviors and characteristics.

Expiry: 180 days.

Storage: See the sub-processor section.

8 Segment Targeting: Pre-Built Segments

Please note: this data is only processed if actively sent by the owner of the Digital Property showing the ad, or by the Controller (if they are not the same).

Data: User identifiers, segment identifiers and segment names and descriptions, as they are all defined by Controller or its clients, or the content owner displaying the advertisement.

Purpose: Enable advertisements to target segments (Data Subjects grouped by their common behavior and/or characteristics) based on information stored in another system.

Expiry: 30 days after last update.

Storage: See the sub-processor section.

9 CRM matching

Please note: this data is only processed if actively sent and activated by the Controller.

Data: Device cookies where applicable, or other user identifiers such as phone numbers or email addresses.

Purpose: To enable two parties to use a common identifier to identify Data Subjects, so that segments from one party can be used to show ads to those segments on the other party's Digital Property.

Example: The following description is an example to support better understanding of how CRM matching is performed. The example uses the scenario where a publisher ("Publisher") and an advertiser ("Sporting Goods Store" or SGS) wish to engage in CRM matching (in this example using email addresses to match IDs) so that SGS can target ads for slalom boots to Data Subjects who have previously purchased slalom skis from SGS.

1. Publisher sends email addresses and any other data as wanted to Adnuntius in accordance with tab 3.4 in this document, along with Publisher's Folder ID (always required in order for the data to be safely stored in a cleanroom available to Publisher alone). A Folder ID is an identifier unique to Publisher and only available to them. More information: https://docs.adnuntius.com/adnuntius-data/user-interface-guide/segmentation/folders
2. SGS sends email addresses and the relevant purchase information in accordance with section 3.4 in this document, along with SGS' Folder ID (always required in order for the data to be safely stored in a cleanroom available to SGS alone).
3. SGS sends its Folder ID to Publisher in an email or similar. The Folder ID can be found here: https://admin.adnuntius.com/folders. The common user identifier is used to identify a Data Subject across domains, and the Folder ID is to confirm that such cross-domain identification is authorized.
4. Publisher implements the Folder ID in its consent tool (CMP) to ensure that only users who consent will be matched. When a request for an ad is sent from Publisher then SGS' segment identifier (a unique identifier for the segment created) is sent with the ad request, so that ads can match the request.
5. When steps 1-4 are set up and an ad request is sent from Publisher's pages to Adnuntius, any Segment ID that the user belongs to will be sent along with the ad request so that SGS' ads can be targeted. No user data is shared between the parties.

10 Reporting

Data: Impressions, viewable impressions, unique users, clicks, and other interactions that Data Subjects make with the advertisements.

Purpose: Enable insights on performance, and to calculate money spent.

Expiry: No expiry. However, if raw logs are enabled for the Controller, the raw logs will be stored for 24 hours so that they can be transferred to the Controller's servers, before being deleted.

Storage: See the sub-processor section.

11 Login Information

Data: Name and email address.

Purpose: Enable the Controller's authorized persons (e.g. employees) to log into the system.

Expiry: No expiry.

Storage: See the sub-processor section.

Exhibit 2: Sub-Processors

Exhibit 2: Sub-Processors

Aa Company	Contact	Role	Server Locations	Transfer Basis
Hetzner Online GmbH	Industriestrasse 25, 91710 Gunzenhausen, Germany - info@hetzner.com - +49 (0)9831 505-0	Hetzner is Adnuntius' supplier of servers in Europe, and stores data about all users	Germany and Finland.	EU standard clauses.

Company	Contact	Role	Server Locations	Transfer Basis
		tracked by any of the tracking mechanisms specified in this document.		
Amazon Web Services	https://pages.awscloud.com/compliance-contact-us.html	Snapshots of Adnuntius data are periodically saved to Amazon Simple Storage Service (AWS S3)'s Frankfurt data center. All data is encrypted with AES prior to leaving the Hetzner data centers (Germany and Finland) and sent to this Frankfurt data center, is transmitted via a secured channel, and is stored in its encrypted form in a private S3 bucket.	Germany and Ireland.	EU standard clauses.
Cloudflare, Inc	101 Townsend Street San Francisco, CA 94107, USA; Emily Hancock, Data Protection Officer, legal@cloudflare.com	Cloudflare terminates prebid requests at the edge, decrypts it, and tunnels it to our adservers for a fast ad response.	Worldwide points of presence. For EU companies: to ensure that only European servers are used, just send the GDPR ad tag parameter (gdpr: 1) with the ad request as explained here.	EU standard clauses.

Exhibit 3: Security Measures

Exhibit 3: Security Measures

Category	Measure
System security	We have an upgrade path for any third party software we use, and upgrade to later versions as time permits.
System security	We continually upgrade our software to the latest versions of dependencies where applicable.
System security	We regularly check for newer versions of any java thirdparty components we can upgrade to, and do that.
System security	We have an process to keep all Ubuntu machines up to date with latest patches, and we have alert monitoring which lets us know when a machine requires updating.
Application security	Where appropriate we filter input for javascript before persisting.
Application security	We remove personal information when testing the software in test environments.
Application security	All communication between layers of our architecture is via secure protocols.
Application security	We use an active-active configuration across multiple regions for handling ad serving. The api uses an active-passive configuration which requires manual failover to another region.
Application security	Our production, staging and test environments are completely separate. If we employ production data in tests, its manually reconstructed via UI or tooling.
Application security	Any vulnerabilities discovered are swiftly patched (we roll out new releases to production sometimes several times per day, if we discover an issue we can roll out a fix promptly).

Category	Measure
Application security	We have extensive regression test coverage which makes the release process reasonably bullet proof.
Application security	We separate our deployment network into dev, staging and production segments. Each of these requires different access credentials. For example, users who do not require production access won't get it. Within Adnuntius itself we deploy 3 different versions, one each to the 3 above mentioned environments. Each of these has a different authentication store. So users who have access to dev, will require a separate account to access production if they need it. Within Adnuntius itself we have roles and permissions, so that we can provide users with only the permissions they need to do their job.
Network security	Customer data is logically separated from each other.
Network security	We have monitoring setup to detect egress of excessive outbound bytes, this will alert us very quickly if an attacker is attempting to exfiltrate db data for instance.
Network security	We log all authentication attempts.
Network security	User accounts within the organization are unique, assigned to a specific person and get monitored for malicious usage (e.g. compromised logins, suspicious activity like repeated login attempts).
Network security	Failed login attempts to our API and UI will lock the relevant account after 5 failed attempts.
Network security	Security updates are continuously performed on servers.
Network security	We use a third party solution (cloudflare) to mitigate DDOS attacks.
Data access	Access to privileged accounts is restricted to appropriate personnel and tightly controlled.
Data access	Access to backups is restricted to authorized personnel.
Data access	Access permissions are reviewed on a regular schedule and restricted to a minimum.
Data access	We enforce a minimum length of 8 characters and prevent the use of the most common bad passwords > 8 characters and we lock accounts after 5 failed login attempts.
Data access	We regularly rotate passwords.
Data access	All passwords stored in the adnuntius saas solution are hashed and salted.
Data access	Oauth2 tokens are required for authentication, and they have a limited lifespan.
Data access	All access to our machines in data centres is secured using 2FA + SSH pass phrase. Even if a machine were compromised, it is not possible to SSH from one machine to another in our production, test and staging environments.
Data access	We use bitwarden to store any required shared secrets and where possible enable 2FA for as many services as support it.
Data access	Access to customer data by Adnuntius employees is only granted to defined employees with a demonstrated need for it.
Data access	We have version history of objects (creatives, line items, assets, etc) which for example, would allow analysis of who changed a component that introduced a vulnerability.
Data access	We use access controls for access to the system.
Data security	The Adnuntius Data product only accepts input data via https. Similarly all data that is available from our platform will be returned via https. The X.509 certificates for the TLS sessions are provided by Let's Encrypt and Cloudflare.
Data security	All communication between services and databases is secured using TLS. All communication between data centres is secured using VPN tunnels.
Data security	We use at rest encryption for any PIR data stored in our data stores.
Data security	We encrypt PII fields in our data stores. We encrypt our database backups.
Workstation security	We maintain hot standbys of all data in separate DCs from our primary data.

Category	Measure
Workstation security	We backup data using multiple data centers (across Germany and Finland) and have multiple failovers in place to secure smooth transfer to backup servers in case of downtime. While our recovery services are automated we have 24/7 on-call engineers that (1) receive notifications about any incident, and (2) are competent to resolve issues. Our availability is openly accessible here: status.adnuntius.com.
Workstation security	There is a central back-up server to save backed-up data. The RAID-1 hard disk system reduces the likelihood of data loss.
Workstation security	All employees are required to install anti-virus software on their computers.
Workplace security	Prints and hard copies shall only be applied if strictly necessary, and shall be destroyed after its purposes are fulfilled.
Workplace security	Offices are accessible only with keycards issued to employees only.
Workplace security	All employees are required to activate password protected screesavers on their computers.
Data center security	A modern fire detection system is directly connected to the fire alarm center of the local fire department.
Data center security	Direct free cooling allows for the environmentally-friendly cooling of hardware. Climate control is effected via a raised floor system.
Data center security	A generated password enables on-site personnel to authenticate and issue a transponder key for the interlocking doors to the rack.
Data center security	Visits are logged, and the footage recorded is archived in the administration interface for monitoring purposes.
Data center security	The uninterrupted power supply (USV) is ensured with a 15-minute backup battery capacity and emergency dieselgenerated power. All UPS systems have redundant design.
Data center security	All movements are recorded and documented. Ultramodern surveillance cameras provide 24/7 monitoring of all access routes, entrances, security door interlocking systems and server rooms.
Data center security	A video-monitored, high-security perimeter surrounds the entire data center park. Entry is only possible via electronic access control terminals with a transponder key or admission card.
Data center security	All European customer data is held in a highly secure ISO 27001 certified data center. Physical security is maintained with the measures described in https://www.hetzner.com/assets/Uploads/downloads/Sicherheit-en.pdf.
People security	All employees expected to manage personal data receive training (how to manage information and what to do if a breach occurs).
People security	All employees commit themselves to confidentiality upon hiring.
People security	Background checks are performed in countries that allow for them, and where such checks are deemed necessary.

Exhibit 4: Contact Persons

Exhibit 4: Responsible Persons

Responsibility	Name	Email
Contact Person	Stian Remaad	stian@adnuntius.com
Data Protection Officer	Stian Remaad	stian@adnuntius.com