APPENDIX TO PUBLISHER TERMS AND CONDITIONS OF SERVICES (GTCS)

WEB PUSH NOTIFICATION NOTIFADZ (WPN NOTIFADZ)

DATA PROTECTION AGREEMENT

"AUDIENCE MONETIZATION" AND "RETARGETING " SERVICES

PREAMBLE AND DEFINITIONS

This Data Protection Agreement, including its Appendices (the "**Agreement** ") governs the rights, obligations and responsibilities of ADRENALEAD and the Partner Publisher with respect to WPN Subscribers' Personal Data processed in connection with the "Audience Monetization" and the "Retargeting" services provided by ADRENALEAD.

It is part of the General Terms and Conditions of Services applicable to the provision of these Services.

The terms defined in the General Terms and Conditions of Services have the same meaning where they are used in this Data Protection Agreement.

Unless otherwise expressly specified in this Agreement, the terms **"Supervisory Authority",** "**Personal Data**", **"Data Subjects**", **"Controller", "Processor", "Processing"** and **"Personal Data Breach"** shall, in this Agreement, have the same definitions as provided in the GDPR.

In addition, the following terms in this Agreement shall have the following definitions:

"Applicable laws and regulations on the protection of personal data"	means all national, European and international laws, regulations and other standards applicable to the Processing concerned, including in particular the GDPR and any national law of the Member States of the European Union adopted in addition to or in application of the provisions of the GDPR, as well as, where applicable, the national, European and international laws, regulations and other standards applicable to the Processing concerned.
"Data Transfer"	any transfer of Data concerned to a person, entity or service of any kind located in a country outside of the European Economic Area that does not benefit from an adequacy decision by the European Commission within the meaning of Article 45 of the GDPR, and/or any access to the Data concerned by a person, entity or service of any kind located in such a country.

"Trigger"	a campaign that triggers automatically when a WPN Subscriber follows a scenario defined by the Partner Publisher
"Master Data"	personal data relating to the WPN Subscriber processed by ADRENALEAD for the management of the WPN Subscribers and the sending of WPN, as set out in article 1.3
"Additional Data"	personal data relating to the WPN Subscriber (other than the Master Data) processed by ADRENALEAD or the Partner Publisher as part of the Services

1. GENERAL PROVISIONS

1.1. How the Platform works

The Notifadz Platform uses the Web Push Notification (WPN) technology which allows, when an Internet user visits a Partner Publisher's Site from his computer or mobile device, to request consent of the Internet user to receive notifications from this Site including editorial or advertising content.

The Platform allows for:

- the collection of consent (opt-in) from Internet users to receive Web push notifications;
- the sending of WPN to WPN Subscribers.

A web push notification opt-in is defined as the creation of a registration in the form of a browser transaction: a string of characters grouping together the URL and the ID of the unique transaction generated by the browser's trusted third party. This opt-in can only be used by the owner of the VAPID Keys.

1.2. Legal basis for operations

The legal basis for processing is **consent** from the WPN Subscriber, in accordance with article 6 of the GDPR and article 5 (3) of the e-privacy directive.

- Consent to WPN

To enable the provision of the Services, the Partner Publisher inserts into the source code of its Site a computer code (script) provided by ADRENALEAD, which triggers the mechanism for collecting the user's consent to WPN.

The consent to WPN is given through the WPN Subscriber's browser and the Parties acknowledge that they have no technical control over the appearance, ergonomic or functioning of this tool.

WPN Subscribers who no longer wish to receive WPN from a Site must unsubscribe by accessing their browser settings or directly from the notifications sent to them by clicking on the cogwheel symbol contained in the notifications.

- Consent to tracking devices

Partner Publisher undertakes to implement an ergonomic and fair information and consent mechanism for trackers (CMP or Consent Management Platform) that is user-friendly and fair, enabling it to obtain the individual consent of WPN Subscribers to the processing of data for advertising purposes by third-party partners and to withdraw this consent as easily as it was given, in accordance with the requirements and mechanism of the IAB's TCF (Transparency & Consent Framework).

Partner Publisher undertakes to reference ADRENALEAD as a "Vendor" in its CMP.

The CMP must remain constantly operational for the duration of the Services. The Partner Publisher will immediately notice ADRENALEAD in the event of a malfunction of such device.

The Partner Publisher must be able to demonstrate that the WPN Subscriber has given their consent to the installation of trackers and provide proof of this consent at any time upon request.

ADRENALEAD undertakes to respect the choices of WPN Subscribers expressed in the form of the 'Transparency and Consent String' and to transmit this Consent String to its partners without altering or modifying it.

Each Party undertakes to perform this Agreement in accordance with the Applicable laws and regulations on the protection of personal data, and to comply at all times with its obligations in this regard.

1.3. Personal data processed for the sending of WPN

The Personal Data collected or created in the database by ADRENALEAD relating to a WPN Subscriber (referred to as "**Master Data**") are as follows:

- Operating System (OS)
- Browser Type
- Geolocation information from IP (Country, zip code, city)
- ISP
- Connection type (mobile or fixed access point)
- Opt-in date
- Opt-in transaction information
- URL of the site (domain name) at the time of opt-in
- User Browser Agent
- IP Hash (IP address that has been subject to some form of encryption)

ADRENALEAD also processes the TCF String (or Consent String), a machine-readable encoded string of characters that contains all information about the WPN Subscriber's consent choices regarding cookies and trackers, as well as information about data processing activities and the legal basis for processing.

1.4. INSTALLATION OF TRACKERS COMMON TO ALL SERVICES (see list of trackers in Appendix 2)

ADRENALEAD places analytics cookies and cookies to limit the frequency of display of an opt-in request, exempt from consent. No personal data is processed on this occasion.

2. "AUDIENCE MONETIZATION" SERVICE

2.1. Service description

WPN Subscribers of the Partner Publisher Site are included in ADRENALEAD Base. ADRENALEAD sends these WPN Subscribers Advertising Campaigns on behalf of Principals, identified as originating from the Partner Publisher's Site.

2.2. Parties qualification

ADRENALEAD and Partner Publisher act as **joint Controllers** for the processing of the Master Data carried out for the sending of WPN to the ADRENALEAD Base. Both Parties agree that ADRENALEAD is solely responsible for determining the general purposes and means of such processing, without prejudice to the Partner Publisher's obligations hereafter.

2.3. Respective obligations of ADRENALEAD and Partner Publisher as joint controllers

2.3.1. Obligation to inform the WPN Subscriber

ADRENALEAD informs WPN Subscribers of the terms and conditions of the WPN and the data processed by publishing a privacy policy, which is available on its website and on each WPN.

The Partner Publisher is required to provide access to this privacy policy on its own Site.

2.3.2. Exercise of WPN Subscribers rights

The information held by ADRENALEAD relating to a WPN Subscriber (Master Data) does not allow the identification of a natural person. The purposes for which ADRENALEAD processes such personal data do not require the identification of the data subjects.

In this case, in accordance with Article 11 of the GDPR, ADRENALEAD is not required to maintain, acquire or process additional information to identify the data subject for the sole purpose of complying with the GDPR, and the rights of access, rectification, erasure, limitation and portability of data subjects (Articles 15 to 20 of the GDPR), as far as they relate to Master Data, are applicable only to the extent that the data subject provides additional data to ADRENALEAD allowing a connection between the data subject and the Master Data relating to him/her.

2.3.3. Security and confidentiality of operations

The measures taken by ADRENALEAD to secure the Notifadz platform in order to ensure an adequate level of security for the operations concerned and to protect data against accidental or unlawful destruction, accidental loss, alteration, disclosure or unauthorised access are described in Appendix 1.

The Partner Publisher undertakes to ensure the security of its Site by applying appropriate security measures in accordance with best practices.

2.3.4. Personal data breaches

Each Party shall notify the other of any personal data breach as soon as possible after becoming aware of it.

Depending on the circumstances of the breach, ADRENALEAD and the Partner Publisher shall consult with each other to determine whether notification of the data breach to the Supervisory Authority or to the Data Subjects is necessary, and who will make such notification.

2.3.5. Data processors

ADRENALEAD uses data processors listed in Appendix 1, which the Partner Publisher accepts.

2.3.6. Data transfers to third countries

The Master Data is not transferred to third countries.

2.3.7. Purposes of the processing of Master Data

Master Data are processed for the sending of Advertising Campaigns to WPN Subscribers.

3. SERVICE « RETARGETING SOLUTION SAAS » (APPENDIX 3)

As an ancillary service to the Audience Monetization Service, the Partner Publisher may use the Notifadz Platform for the Retargeting Service, for the purpose of sending its own WPN to its base of WPN Subscribers (the Publisher Base).

3.1. Qualification of the Parties

The Partner Publisher is the Controller and ADRENALEAD is the Processor of the Personal Data on behalf of the Controller in the context of the Retargeting Service.

For the sole purpose of performing the Retargeting Service, the Controller authorises the Processor to carry out the Processing in question on its behalf, the terms of which are described in **Appendix 3**.

3.2. Tracking devices

The Partner Publisher may choose to place tracking devices on the WPN Subscriber's terminal from its Site, with the consent of the WPN Subscriber, in order to track the WPN Subscriber's behaviour and provide personalized notifications to the WPN Subscriber.

The Partner Publisher is solely responsible for the processing of the personal data relating to the WPN Subscriber's behaviour.

3.3. Data processing agreement

"Data concerned"	means all Personal Data processed by the Processor on behalf of the Controller in the context of the Processing concerned
"Processing concerned"	means the Processing of Personal Data carried out by the Processor on behalf of the Controller in the context of the performance of the Agreement

3.3.1. Processing on the documented instructions of the Controller

The Processor shall process the Data concerned only on documented instructions from the Controller, including with regard to Data Transfers outside the EU, unless the Processor is required to do so by Union or member state law to which it is subject. In such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

The Parties expressly agree that this Agreement constitutes documented instructions from the Controller within the meaning of the preceding paragraph.

3.3.2. Assistance provided to the Controller

- General assistance

The Processor assists the Controller in ensuring compliance with its obligations under the Applicable laws and regulations on the protection of personal data and more particularly the GDPR, including:

- its obligations related to the security of the Processing concerned and the confidentiality of the Data concerned,
- its obligations to notify the Supervisory Authority of Personal Data Breaches,
- and its obligations to carry out prior impact assessments (PIAs) and to consult, where necessary, the Supervisory Authorities prior to the implementation of a Processing.

- Assistance with exercise of rights

The Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights but shall not itself respond to such requests.

The Processor will redirect to the Controller, without undue delay, any such request that it receives in connection with the Processing concerned and will not respond to such a request itself.

It is recalled that the processing operations carried out by the Processor on behalf of the Controller relate to non-directly identifying data and that the purposes of this processing do not require the identification of Data Subjects.

Consequently, unless the data subject provides additional information, the Processor will not be able to make a connection between the data subject and the Master Data relating to him/her.

3.3.3. Security of Processing

The Processor undertakes to take and maintain all appropriate technical and organizational measures taking into account the risks presented by the Processing concerned, in order to ensure an adequate level of security of the Processing concerned and to protect the Data concerned against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, in particular when the processing involves the transmission of data by network, and against any other unlawful forms of processing. These measures are set out in Appendix 1.

3.3.4. Confidentiality of the Data concerned

Processor ensures that persons authorised to process the Data concerned have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3.5. Information and audit rights

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations imposed on it as a processor and allow for and contribute to audits.

Such information is confidential and the Controller undertakes not to communicate it to third parties, except to any competent authority or court for the sole purpose of demonstrating the compliance of the Processing concerned with the Applicable laws and regulations on the protection of personal data.

The Controller has a right to have a certified independent auditor (a "**Third-Party Auditor**") audit the Processor to verify the Processor's compliance with its obligations under this Data Protection Agreement, including, but not limited to, its obligations related to the security of the Processing concerned.

The audit may only be carried out once every 12 months, except for important grounds, during normal office opening hours, and subject to one (1) week's written notice to the Processor including the designation of the persons or entities commissioned by the Controller to conduct the audit. Operations carried out in the offices and with the staff of the Processor may not last more than three (3) working days.

The Controller undertakes that any person who participates in the audit operations be bound by appropriate confidentiality obligations with respect to the information collected during such operations, whether by means of confidentiality commitments or agreements or by application of legal or regulatory confidentiality or secrecy obligations applicable to such persons.

The Processor shall have the right to oppose the appointment of a Third-Party Auditor if, for compelling reasons relating to its specific situation, the performance of the audit by this Third-Party Auditor manifestly presents a risk of causing damage to the Processor. Under no circumstances shall the exercise of the above-mentioned option have the object or effect of preventing any audit from being carried out.

A copy of the audit report is remitted to the Processor.

3.3.6. Personal data breaches

The Processor notifies the Controller of any personal data breach as soon as possible after having become aware of it.

In order to assist the Controller in its notification obligations to the Supervisory Authority, this notification will include the following information, provided that the Processor has this information and that the Controller does not already have it:

(a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of persons affected by the breach and the categories and approximate number of personal data records concerned;

(b) the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

(c) the likely consequences of the personal data breach;

(d) a description of the measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Given the nature of the personal data processed by the Processor that constitute non directly identifying personal data, the Processor will not be able to assist the Controller in the event that communications of a personal data breach are to be made to data subjects.

3.3.7. Data processing

The Controller is informed that the Processor itself uses sub-processors, as listed in Appendix 1, and accepts it. The Controller gives the Processor a general authorization to use sub-processors.

The Processor undertakes to notify the Controller in advance in the event that it wishes to replace or add an existing sub-Processor or subcontract all or part of its obligations under the Service Agreement. The Controller may raise written reasoned objections within 8 (eight) working days.

Where the Processor uses sub-processors, the same data protection obligations as those set out in this Agreement are imposed on that sub-processor by contract, in particular with regard to providing sufficient guarantees as to the implementation of appropriate technical and organisational measures so that the Processing meets the requirements of the GDPR. Where such sub-processor fails to comply with its data protection obligations, the Processor shall remain fully liable to the Controller for the performance by the sub-processor of its obligations.

3.3.8. Data Transfers

None of the Data concerned may be subject to a Data Transfer without the prior written consent of the Controller.

3.3.9. Deletion/Return of Personal Data

The Processor undertakes, at the end of the Service Agreement and upon closure of the Controller's account, to proceed with the definitive and irreversible deletion of all the Data concerned still in its possession or to return all the Data concerned to the Controller in an intact and reusable format, and to order all of its Processors to proceed with this deletion or restitution, as instructed by the Controller.

In the absence of documented instructions from the Controller, the Processor will prefer, under the previous paragraph, the deletion of the Data concerned.

3.3.10. Warning from the Controller

In the event that the Processor considers that a documented instruction from the Controller concerning the Processing concerned could be considered unlawful under the Applicable laws and regulations on the protection of personal data, or could lead to a breach or violation thereof, the Processor undertakes to immediately inform the Controller, it being specified that the latter remains the sole judge between the Parties of the validity of the instructions given concerning the Processing concerned and will indemnify the Processor against all and any prejudice resulting from an unlawful instruction.

In the event of a conflict between the provisions of this Agreement and those of the Terms of Service, the Parties agree that the provisions of this Agreement shall prevail.

APPENDIX 1

TECHNICAL AND ORGANISATIONAL MEASURES PUT IN PLACE BY ADRENALEAD

ADRENALEAD Organizational Security	
The organisation includes at least one safety manager for all areas contributing to the smooth running of the service.	François GERMAIN – Partner CTO
Any employee involved in the Partner Publisher-related activity has signed a personal confidentiality agreement as part of their employment contract.	Employees Technical Team Employees Product Team Employees Account Management Team Direction
Physical Security of Data Centers	
Please see Amazon Web Service Physical Security Policy	
Physical Security of ADRENALEAD's Premises	
ADRENALEAD's premises are equipped with protective equipment	• Protection against intrusion and burglary; • Intrusion and burglary detection;
The means of protection against intrusion and supervision must make it possible to physically identify people regardless of the conditions.	Video surveillance system
Security of the AWS Cloud Solution and the associated IS ADRENALEAD	
Access to ADRENALEAD information system	Passwords consist of at least 8 characters that combine at least uppercase and lowercase letters as well as numbers or special or accented characters.
Access to resources and network ADRENALEAD	Each person who accesses computer resources or network has an individual account which can be: • Either a nominative personal account that will only be used by this person throughout the life of the account; • Either an individualized account that can be assigned to various people during the life of the account while still being assigned to only one person at a time.

Sub-processors:

Name of	**Purpose of the**	**Place from which the service entrusted is carried**	**Supervision of transfers outside the EU**

Subprocessor	subcontracting	out	
Amazon	Notifadz Platform Hosting (AWS)	EU, France, Paris	No transfers outside the EU

APPENDIX 2

TRACKING DEVICES COMMON TO ALL SERVICES

First-party cookies placed where the Internet user visits the Partner Publisher's Site:

Tracking device Name	**Temporality**	**Description of the tracking device and purpose**
nadz_dailyVisits	Placed on the 1st visit of the Internet user on the Site as soon as the nadz-sdk script is loaded	Purpose: counting the unique daily visits to the Site in an anonymised manner on the ADRENALEAD servers and calculating the opt-in rate Duration : 1 calendar day
SA	Placed after an opt-in request has been displayed if the Internet user has not interacted with it	Purpose: limiting the opt-in request display frequency to one in a predefined period of time, by default 24h Variable lifespan but by default 24 hours

No personal data is collected through these cookies.

Appendix 3

RETARGETING SERVICE

1. Description

Purpose of the Services	Provision of ADRENALEAD's Notifadz Platform for the collection of WPN Subscribers and the sending of web push notifications by Partner Publisher to WPN Subscribers on Partner Publisher's Site.
Purpose(s) of the processing carried out by the Controller	1. Setting Advertising Campaigns using Master Data relating to device (computer or mobile), browser, location, or subscription Site 2. Setting Advertising Campaigns based on a trigger determined by the Partner Publisher based on the behaviour of the WPN Subscriber (e.g. visit to a specific page) or time (e.g. following the date of the last visit) 3. Sending of Advertising Campaigns by the Partner Publisher to the Publisher Base 4. Performance tracking: measurement of Advertising Campaign conversion (sales, leads, etc.).
Categories of data subjects	o WPN Subscribers of the Partner Publisher's Site
Types of Personal Data processed by the Processor	**"Master Data" used for setting and sending WPN, not communicated to the Controller:** • Operating System (OS) • Browser Type • Geolocation information from IP (Country, zip code, city) • ISP • Connection type (mobile or fixed access point) • Optin date • Opt-in transaction information* • Website URL (domain name) at the time of opt-in* • Browser's User Agent • IP Hash (IP address that has been subject to some form of encryption) **"Additional Data" collected through tracking devices by the Controller and used to set personalised WPN campaigns.**

Recipients	Amazon Web Services Hosting
Processors and Partners	Amazon Web Services (WPN subscriber database and working servers)
Retention period(s)	**Master Data**: by default duration of the Service Agreement or to be determined by the Controller If the WPN Subscriber unsubscribes, the Master Data shall be retained for a maximum period of one year for statistical purposes. **Additional Data**: by default duration of the Service Agrement or to be determined by the Controller If the WPN Subscriber unsubscribes, the Additional Data are retained for a maximum period of one year for statistical purposes.
Data Privacy and Security	Our technical infrastructure is hosted on AWS: https://aws.amazon.com/fr/compliance/data-center/controls/ See above the table "Technical and organizational measures put in place by the Processor"
Name and contact details of the DPO	François GERMAIN francois@adrenalead.com 06 51 36 12 82

2. Tracking devices implemented for the Retargeting Service

Tracking devices placed in the LocalStorage by ADRENALEAD related to Triggers / automated campaigns:

Placed only if the Triggers script has been embedded and the cookie accepted by the WPN Subscriber via Partner Publisher's CMP.

Name of Tracking device	Description and purpose

campaigns	list of **'Triggers' campaigns** for the site in question (linked to siteId)
validatedCampaigns	Trigger campaigns validated by the WPN Subscriber (allows you to know if to send a CREATE, UPDATE or DELETE signal and avoids over-soliciting our architecture)
checkAgain	Allows you to restart the sending of a campaign that could not be completed during a visit. Retry on next page load.
userProfile	key/value map to store tags about the WPN Subscriber. o **Fixed elements:** § ids: siteId of the Partner Publisher § pushSubscription : information regarding optin (keys, endpointId, endpoint url, and optinInfo ADRENALEAD : browser, os, countryCode, postalCode etc) o **Dynamic elements:** depends on the tagging carried out via our script/sdk (example: *_nAdzqTriggers.push(['addValue', 'cartProducts', 'productA']);* to tag **'basketProducts'** with the value **'productA'**)

3. Examples of retargeting campaigns:

welcomePush

- Date of optin
- pushSubscribtion(OPTIN: Endpoint, p256 key, and auth key)
- Date last exchanges with the server (date of last visit to the site)

shopping cart

- Last Product
- Date of optin
- pushSubscribtion(OPTIN)
- Date Last Exchanges with Server

visit

- Date of visit
- URL visited
- Date of optin
- pushSubscribtion(OPTIN)
- Date Last Exchanges with Server