

Policy Title: IAS Technology Solutions and Platform Privacy Policy	Original Issue Date: 02.10.2022	Version Effective Date: 02.10.2022
	Most Recent Revision Date: 02.10.2022	Policy No.: IASLG-17



IAS Technology Solutions and Platform Privacy Policy

Approved By: IAS Audit Committee
Policy Owner: IAS General Counsel
Policy Contact: IAS Global Compliance Officer

Contents

1.0	Applicability and Scope.....	3
1.1	Applicability Boiler	3
1.2	Scope.....	3
2.0	Overview and Purpose.....	3
3.0	Policy Content	3
3.1	Definitions	3
3.2	Business Requirements.....	4
3.2.1	IAS acts as a processor for the following services	4
3.2.1.1	Viewability services	4
3.2.1.2	Brand safety services.....	4
3.2.1.3	Geo-verification	4
3.2.2	IAS acts as a controller for the following services	5
3.2.2.1	Ad fraud services	5
3.2.2.2	Anonymization.....	5
3.2.3	Personal data that IAS collects	5
3.2.3.1	Personal data collected when a person uses the IAS Portal.....	5
3.2.3.2	Personal data collected by IAS Technology Solutions	5
3.2.4	IAS tools	6
3.2.5	How IAS uses the personal data that it collects	6
3.2.6	How and why IAS discloses the personal data that it collects to other parties	7
3.2.6.1	Disclosures to third parties	7
3.2.6.2	Disclosures to affiliates	7
3.2.6.3	Business disclosures	7
3.2.6.4	Disclosure to public authorities	7
3.2.7	Data subject rights and choices	7
3.2.8	Data retention.....	8
3.2.9	International transfers	8
3.2.10	Legal bases for processing.....	8
3.2.11	California Privacy Rights.....	9
3.2.12	Children.....	9
3.2.13	Changes to this privacy policy.....	9
3.2.14	How to contact IAS	9
4.0	Policy Maintenance.....	9
4.1	Authority and Delegation	9
4.2	Policy Review, Renewal and Approval	10
4.3	Procedure Review, Renewal and Approval	10
5.0	Cross References.....	10
5.1	Related Policies	10
5.2	Related Standards	10
5.3	Related Procedures	10
5.4	Related Notices.....	10
6.0	Revision History	11
7.0	Appendix	11

1.0 Applicability and Scope

1.1 Applicability

The IAS Technology Solutions and Platform Privacy Policy (hereafter referred to as this "Policy") applies to the various operations within Integral Ad Science Holding Corp. (IAS) its sales platforms, all employees and, as applicable, subsidiaries, affiliates and third parties that support IAS' business activities (collectively, "IAS Entities"). This Policy establishes the minimum requirements for IAS and its entities.

1.2 Scope

This Privacy Policy applies to Personal Data (as defined below) collected through the verification, optimization, and activation technology solutions ("Technology Solutions") that IAS provide to their customers through various channels, as well as IAS Signal at www.integralplatform.com ("IAS Portal"), which allow IAS customers and media partners ("Users") to access reporting regarding the Technology Solutions. For information regarding IAS processing practices with respect to its Websites, please see IAS website privacy policy [here](#).

2.0 Overview and Purpose

IAS empowers the advertising industry to invest with confidence and activate consumers everywhere, on every device. IAS build products, deliver solutions, and generate ideas that provide valuable functions for its customers and media partners. IAS acts with honesty, transparency, and integrity in working with each other and with its customers and media partners. As part of its role in promoting trust and transparency in digital advertising, IAS takes seriously its responsibilities with respect to privacy. This privacy policy demonstrates how the personal information and personal data that is collected from its media partners and customers is used, shared, and retained.

3.0 Policy Content

3.1 Definitions

The following acronyms and terms are used within this document.

Term	Definition
Controller	"The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. [General Data Protection Regulation (GDPR)].
Data subjects	"Identified or identifiable natural person[s]" (GDPR). Data subjects are people from whom or about whom information has been collected in connection with a business and its operations
Invalid traffic (IVT) / Impression fraud	The management of ad serving, ad display, or traffic activity such that ad impression measurements are shown inappropriately because the

	ads cannot be viewed by a user, are not served within operationally viewable parameters, or were displayed as a result of fraudulent machine-generated traffic.
Personal Data	Business contact information collected from visitors and clients who wish to obtain information or support, or to purchase their Technology Solutions. Contact information includes first name, last name, business email address, job title, name of the organization, country, business phone number, and organization type.
Processor	The entity that actually performs the data processing on the controller's behalf. (GDPR).
User	Someone who is using the IAS portal, or its Technology solutions and services, i.e. IAS customers and media partners.

3.2 Business Requirements

For clarity, this policy applies when IAS acts as a “Controller” (as defined in the General Data Protection Regulation (the “GDPR”), and the versions of the GDPR retained in U.K. law (the “UK GDPR”) and Switzerland). Note that IAS may also process Personal Data of its Users’ employees and other individuals in connection with IAS provision of services to entities which have contracted for IAS’s services (“Customers”). In this case IAS is the “Processor” of Personal Data. “Personal Data” means any information that identifies or relates to a particular individual and also includes information referred to as “personally identifiable information” or “personal information” under applicable data privacy laws, rules, or regulations (collectively the “Data Protection Laws”). If IAS is the Processor for someone’s Personal Data (i.e., not the controller), they may contact the controller to address their rights with respect to such data.

3.2.1 IAS acts as a processor for the following services

3.2.1.1 Viewability services

IAS collects personal data from pixels and tags in ads, as well as from SDKs integrated into ad servers, video players, and mobile applications, and reports back to the specific Customer the information about whether that Customer’s ads have had the opportunity to be seen by real people. IAS only uses personal data collected from a particular Customer’s ads or ad space to report to that Customer, so is acting only on that Customer’s instructions.

3.2.1.2 Brand safety services

IAS’s brand safety services involve the comparison of individual Customers’ brand safety needs against the IAS internal database of information about particular sites and mobile applications, which is used to ensure that Customers’ ads won’t be displayed on sites which do not meet an individual Customer’s needs when an impression on that site is received. IAS does not use information collected from impressions for purposes other than ensuring a Customer’s ads are not served on sites or mobile applications that do not meet that Customer’s requirements.

3.2.1.3 Geo-verification

IAS Customers can verify the non-precise location of viewers of a particular webpage or mobile application to ensure they do not serve ads irrelevant to or inappropriate for a particular jurisdiction. To do this, IAS obtains information from a device or browser to allow it to determine the approximate (but not precise) location of that IP address. IAS only uses this information to provide geo-verification to the specific Customer that has requested it, and not for any other purpose, so again only acts on its specific Customer’s instructions. When acting as a processor and carrying out the above-mentioned processing

activities, IAS does not share any of the personal data collected from one Customer with other Customers.

3.2.2 IAS acts as a controller for the following services

3.2.2.1 Ad fraud services.

In addition to identifying invalid traffic which includes specific attempts at ad fraud for individual Customers, IAS collects information from pixels embedded on all of its Customers' ads, as well as SDKs integrated into ad servers, video players and mobile applications, and analyzes them to identify anomalies that indicate non-human traffic, including ad fraud. This information is collected across all IAS channels, Customers, and platforms, and is aggregated together to create scalable detection models, which allow IAS to distinguish real human behavior from bot behavior, and is also used to create ad fraud exclusion lists. As IAS combines information from all of its Customers' ads to develop its own ad fraud detection models, it is determining how to use the personal data collected in relation to each of its Customers for its own internal purposes. Accordingly, IAS is a controller in relation to personal data used for these services. IAS shares the ad fraud exclusion lists with certain Customers (e.g., DSPs and Ad Exchanges) to enable such Customers to avoid serving their respective clients' ads to "bad" or fraudulent IP Addresses.

3.2.2.2 Anonymization

IAS develops its own models and benchmarking reports using information collected from pixels and SDKs used by multiple Customers. However, IAS only uses this information in anonymized form, i.e., in such a form that that information cannot be used to identify an individual or Customer by any means reasonably available to IAS. IAS uses various methods, including deleting identifiers and aggregation, to ensure that this information is appropriately anonymized. For the purposes of processing personal data to anonymize it, IAS is using personal data it collects for its own internal purposes, and is a controller. However, after the anonymization process is complete, IAS is no longer a "controller" as the information is no longer personal data.

For more information about how IAS acts as a controller or processor, see IAS [Data Protection Portal](#).

3.2.3 Personal data that IAS collects

3.2.3.1 Personal data collected when a person uses the IAS Portal

When a person creates an account with IAS, they may provide IAS with their contact details, such as their name, phone number, physical address, and email address to enable IAS to provide their services to them. They may also be asked to provide a username and password to use as identity verification credentials to access their IAS Portal. Through the IAS Portal, Users may access reporting services in connection with use of IAS suite of Technology Solutions.

IAS may also automatically collect certain data about a User when they access or use the IAS Portal. Collectively, IAS refers to this information as "Usage Information." The methods that may be used on the IAS Portal to collect Usage Information include:

- **Log Information.** Log information is data about the User's use of the IAS Portal, such as IP address, browser type, referring/exit pages, operating system, date/time stamps, and related data, and may be stored in log files.
- **Information Collected by Cookies.** First party technical, functional, and performance cookies may be used to collect information about interactions with the IAS Portal or IAS emails. The cookies utilized in the IAS Portal do not create profiles regarding individuals and are only for purposes of ensuring the technical functionality of the IAS Portal.

3.2.3.2 Personal data collected by IAS Technology Solutions

IAS accredited Technology Solutions serve both advertisers and media sellers by providing independent, third-party verification and measurement services. By analyzing information about ad

impression delivery and website traffic, IAS verifies whether the media has met or failed to meet expectations based on characteristics that include the brand safety of a webpage, the viewability of the ad placement, the existence of ad fraud, as well as additional contextual variables. Measurement is available across both browser and app environments for mobile and desktop devices. IAS collects and surfaces this data to increase trust and transparency for IAS Customers. The data collected can be used by Customers to proactively prevent advertising on undesirable and/or low-quality inventory, monitor overall quality performance, and make future media planning decisions.

In order to provide Technology Solutions to its Customers, IAS use pixels and other similar technologies (see “IAS Tools” below) that place small pieces of HTML code on a webpage to collect information about advertising impression opportunities and displayed ads or website/mobile app traffic. The following categories of Personal Data are collected when these technologies are deployed when providing Technology Solutions to IAS Customers:

- **Browser and computer environment information:** This information is necessary to determine the viewability of an advertisement, which includes information such as the ad’s location in the browser viewport, size of the browser viewport, ad size, size of the display, application in focus, the browser tab in focus, and other data.
- **Standard HTTP header information:** This includes IP address, referring URL, user agent data (data transmitted by the User’s browser about itself when submitting an HTTP request), and other data including browser configuration parameters, browser type and language, session storage and local storage settings, and characteristics of the User’s device such as the CPU class and time zone setting.
- **Information contained within an advertisement:** This is known as an “ad tag,” that includes information used to identify the advertiser displaying the ad and the media property that sold the impression.

3.2.4 IAS tools

Pixels (also sometimes referred to as beacons or web beacons) and tags are elements included in web pages to enable companies to collect data, serve advertising, and provide related services, such as measuring ad effectiveness or preventing fake ad traffic. They do this by allowing communication between a web browser and a server. A beacon is a small transparent image that is placed on a web page. A tag is a small piece of website code that is run by the web browser. Pixel tags are small, invisible images on a web page or other document.

3.2.5 How IAS uses the personal data that it collects

IAS uses the personal data its collects to deliver its Technology Solutions, including:

- Examining impression data of advertising opportunities, using IAS technology and Customer parameters, to determine if clients’ advertisements should or should not be displayed.
- Detailing contextual information about advertisements displayed in order to ensure its compliance with terms of IAS Customer or partner’s contracts, insertion orders that detail Customer campaigns, and/or Customer parameters that Customers make in IAS systems.
- Reporting viewability metrics of advertisements that indicate qualified « Viewed Impressions » according to industry standards and/or Customer’s criteria, time in which advertisements are displayed on consumers’ browsers, and properties of creative elements that are displayed on consumers’ browsers.
- Analyzing website and mobile app visitation characteristics such as visitor quality, fraud identification, invalid traffic detection, and other quality characteristics necessary to determine agreement compliance.
- Providing Customer with the highest quality services in IAS Technology Solutions and IAS Portal.
- Personalizing and enhancing Customer’s experience within IAS Technology Solutions and IAS Portal.
- Managing and improving IAS Technology Solutions and IAS Portal.

IAS Technology Solutions include the detection and elimination of general invalid and sophisticated invalid traffic, including ad impression fraud, which it defines in this policy as the management of ad serving, ad display, or traffic activity such that ad impression measurements are shown inappropriately because the ads cannot be viewed by a user, are not served within operationally viewable parameters, or were displayed as a result of fraudulent machine-generated traffic. IAS fraud and invalid traffic services are intended to address fraud for advertising measurement purposes.

Additionally, IAS uses advertising impression information, mobile app information, and website traffic information including IP address and browser header information to:

- Identify traffic sources by their non-precise geographic location and determine if the location is correct and located within the advertiser's campaign parameters or traffic settings.
- Determine if traffic acquired is fraudulent, or if traffic acquisition practices are out of compliance with an advertiser's guidelines or contractual requirements.
- Determine if middleware is attempting to misrepresent its operating characteristics to prevent the identification of fraud or other invalid traffic.
- Determine if traffic or ad impressions are originating from a server farm unlikely to be responsible for human-generated browsing activity.

IAS leverages AI and Machine Learning in order to automate the process of detecting invalid traffic and fraudulent activity.

3.2.6 How and why IAS discloses the personal data that it collects to other parties

3.2.6.1. Disclosures to third parties

Like many businesses, IAS hire other companies to perform certain business-related services. IAS may disclose Personal Data to certain types of third-party companies, but only to the extent needed to enable them to provide services to IAS. The types of companies that may receive personal data and their functions are: direct marketing assistance (including disclosure to IAS distributors for direct marketing of Technology Solutions), billing, user service, data storage, hosting services, disaster recovery services, and credit card processors. All such third parties function as IAS agents, performing services at its instruction and on its behalf pursuant to contracts which require they provide at least the same level of privacy protection as is required by this Privacy Policy and implemented by IAS.

3.2.6.2 Disclosures to affiliates

IAS may also disclose personal data to its affiliates in order to support marketing, sale, and delivery of its Technology Solutions. Personal Data may be transferred from IAS subsidiaries located within the EU to IAS in the U.S. IAS has executed European Commission's Standard Contractual Clauses to legally transfer such data.

3.2.6.3 Business disclosures

In the event of a merger, dissolution, reorganization, or similar corporate event, or the sale of all or substantially all of IAS assets, IAS may transfer any Personal Data that it has collected to the surviving entity in a merger or to an acquiring entity. All such transfers shall be subject to IAS commitments with respect to the privacy and confidentiality of Personal Data as set forth in this privacy policy. This policy shall be binding upon IAS and its legal successors in interest.

3.2.6.4 Disclosure to public authorities

IAS is required to disclose Personal Data in response to lawful requests by public authorities, including in response to law enforcement requirements. IAS may also disclose Personal Data to other third parties when compelled to do so by government authorities or required by law or regulation including, but not limited to, in response to court orders and subpoenas.

3.2.7 Data subject rights and choices

The law in some jurisdictions provides individuals in those jurisdictions with certain rights regarding their Personal Data. Subject to certain exceptions, data subjects have the right to ask IAS to:

- Provide them with information about IAS processing of its Personal Data and give data subjects access to their Personal Data.

- Update or correct inaccuracies in data subject's Personal Data.
- Delete their Personal Data.
- Transfer a machine-readable copy of their Personal Data to a data subject's or a third party of their choice.
- Restrict the processing of their Personal Data.
- Object to IAS processing of their Personal Data for direct marketing purposes.
- Obtain information about and object to IAS reliance on its legitimate interests as the basis for processing of data subject's Personal Data.

Data subject may exercise some of these rights and choices through certain Technology Solution features, for example, by editing their settings when they are logged in. Additionally, they can submit these requests via IAS Privacy Request Portal [here](#). If a data subject is an employee, prospective employee, or contractor of IAS, they should instead email it at privacy@integralads.com. IAS may request specific information from them to help IAS confirm their identity prior to processing their request. Applicable law may require or permit IAS to decline the data subject's request. If IAS declines the data subject's request, IAS will tell them why, subject to legal restrictions. IAS commits to resolving complaints about data subject's privacy and IAS collection or use of their Personal Data. EU individuals with inquiries or complaints regarding this Privacy Policy should first contact Integral Ad Science at privacy@integralads.com. If they have questions regarding their Personal Data processing or if they would like to submit a complaint, they may contact IAS at privacy@integralads.com. They may also contact IAS Data Protection Officer at the contact information below. IAS will do its best to resolve any questions or concerns that a data subject may have. They may also submit a complaint to the data protection regulator in their jurisdiction.

To the extent that IAS acts as a data processor, it may direct a data subject to the data controller for handling of their request under applicable data protection law.

3.2.8 Data retention

IAS will retain Personal Data for as long as it is needed to fulfill the purpose for which it was collected or as required by law. To determine the appropriate retention period, IAS will consider the amount, nature, and sensitivity of the data; the potential risk of harm from unauthorized use or disclosure of the data; the purposes for which IAS processes the data and whether IAS can achieve those purposes through other means; and applicable legal requirements. Unless otherwise required by law, at the end of the retention period IAS will remove personal data from its systems and records or take appropriate steps to properly anonymize it.

3.2.9 International transfers

The IAS Portal and Technology Services are hosted and operated in the United States through IAS and its service providers. If a User does not reside in the U.S., laws in the U.S. may differ from the laws where they reside. By using the IAS Portal and Technology Services, the User acknowledges that any Personal Data about them, regardless of whether provided by them or obtained from a third party, is being provided to IAS in the U.S. and will be hosted on U.S. servers, and the User authorizes IAS to transfer, store, and process their information to and in the U.S. The User hereby acknowledges and agrees with the transfer of their data to the U.S. IAS relies on the European Commission Standard Contractual Clauses for transfers of data outside of the U.K., Switzerland, and the European Union, pursuant to the recent decisions of the European Commission, the U.K. Information Commissioner's Office, and Swiss Federal Data Protection and Information Commissioner.

3.2.10 Legal bases for processing

IAS processing of a data subject's Personal Data is carried out pursuant to the following legal bases:

- The processing is necessary for IAS to provide a User with the products and services they request, or to respond to their inquiries.
- IAS has a legal obligation to process their Personal Data, such as compliance with applicable tax and other government regulations or compliance with a court order or binding law enforcement request.
- To protect a User's vital interests, or those of others.

- IAS has a legitimate interest in carrying out the processing activity. In particular, IAS has a legitimate interest in the following cases:
 - To analyze and improve the safety and security of the Service. This includes implementing and enhancing security measures and safeguards and protecting against fraud, spam, and abuse.
 - To maintain and improve the Service.
 - To operate the Service and provide the User with certain information and communications tailored to, and in accordance with, their preferences.
- The User consented to the processing of their Personal Data. When they consent, they may change their mind at any time.

3.2.11 California Privacy Rights

If a User is a California resident, they should review IAS's California Consumer Privacy Act ("CCPA") Privacy Notice [here](#), which describes their rights under California law and provides information regarding IAS's collection, use, and disclosure of "personal information" (as that term is defined in the CCPA).

3.2.12 Children

IAS does not knowingly collect any Personal Data from children under the age of thirteen through its IAS Portal, or Technology Solutions. If a person is under 16, they should not give IAS any Personal Data. IAS encourages parents and legal guardians to monitor their children's Internet usage and to help enforce IAS Privacy Policy by instructing their children never to provide Personal Data to IAS without their permission. If a person has reason to believe that a child under the age of 16 has provided Personal Data to IAS, they should contact IAS at privacy@integralads.com, and IAS will endeavor to delete that Personal Data from its databases.

3.2.13 Changes to this privacy policy

This Privacy Policy is effective as of the date stated at the top of this Privacy Policy. IAS may change this Privacy Policy from time to time, and will post any changes its Technology Solutions or IAS Portal as soon as they go into effect. By accessing its Technology Solutions or IAS Portal after IAS makes any such changes to this Privacy Policy, the User is deemed to have accepted such changes. Users should refer to this Privacy Policy on a regular basis.

3.2.14 How to contact IAS

If someone has questions about this Privacy Policy, please contact us in one of the following ways:

E-mail IAS at: privacy@integralads.com
 Or write to IAS at: Integral Ad Science, Inc.
 95 Morton Street, 8th Floor
 New York, NY 10014
 Attn: Global Compliance Officer

If someone is a EU resident and wish to escalates their inquiry after contacting the privacy team, they are welcome to contact IAS Data Protection Officer, Lucid Privacy Group.

E-mail IAS DPO at: dpo@integralads.com
 Or write to them at: Lucid Privacy
 1556 Shrader Street
 San Francisco CA 94117
 Attn: Integral Ad Science

4.0 Policy Maintenance

4.1 Authority and Delegation

The IAS Audit Committee (AC) has approved this Policy. The IAS AC hereby delegates to the General Counsel ("Policy Owner") responsibility for this Policy and its maintenance,

including authority to review and approve procedures established in accordance with this Policy.

Any authority granted by the IAS AC and any responsibility they assign to the Policy Owner under this Policy may be delegated at his/her discretion, except as otherwise provided in this Policy.

4.2 Policy Review, Renewal and Approval

Approval: The IAS AC shall review and approve all material revisions to this Policy. The IAS AC approval shall be documented in the meeting minutes of this governing body.

Periodic Renewal: The IAS AC shall renew this Policy periodically, but no less frequently than annually.

Periodic Review: The Global Compliance Officer shall review this Policy on an annual basis to evaluate its effectiveness and accuracy. Any resulting revisions shall be submitted for review and approval as outlined in the Approval section above and documented in the Revision History section of the Appendix. If no revisions are needed, the Global Compliance Officer or assigned delegate shall communicate the outcome of the review to the General Counsel.

Additional Triggers: Certain events, including but not limited to audit findings or changes in business activities, shall trigger unscheduled additional review and revision to this Policy.

4.3 Procedure Review, Renewal and Approval

All related procedures are expected to be in compliance with the spirit and letter of this Policy. The General Counsel has delegated to the Global Compliance Officer to review and approve all material revisions to related procedures. The Global Compliance Officer must review and renew all related procedures no less frequently than annually.

In addition, any related procedures created by functions outside of Information Technology requires approval from the function leader most closely aligned with the procedure subject matter. Only those procedures that reflect material deviations from this Policy must be raised to the attention of the Global Compliance Officer or his/her delegate for review.

5.0 Cross References

5.1 Related Policies

IAS Website Privacy Policy

5.2 Related Standards

None

5.3 Related Procedures

None

5.4 Related Notices

None

6.0 Revision History Required

Version	Approval Date	Effective Date	Description of Revisions:
1.0	02.10.2022	02.10.2022	Retired privacy policy and created two separate polices for website and technical platform. Reformatted into IAS policy template format

7.0 Appendix

None