

HOW INTEGRAL AD SCIENCE COMPLIES WITH THE GENERAL DATA PROTECTION REGULATION (“GDPR”)

Integral Ad Science’s (“IAS”) data and technology solutions promote trust and transparency in the digital advertising ecosystem by empowering the advertising industry to invest with confidence. As part of its role in promoting trust and transparency in digital advertising, IAS takes its responsibilities with respect to privacy seriously.

This document summarizes IAS’s approach to privacy and data protection, and the steps we have taken to ensure that information IAS processes in providing its services is treated in a manner consistent with our legal obligations, including those set out in the GDPR.

IAS’S USE OF ‘PERSONAL DATA’ UNDER THE GDPR

The GDPR has established requirements on companies that collect, use, and share data related to individuals located in the European Economic Area. Under the GDPR, personal data is defined very broadly, and includes all data and information related to a specific individual, who can either be identified:

- directly using that information (for example a name, social security number, phone number); and / or
- indirectly, using a combination of pieces of information which are available to IAS or its Customers using any means reasonably available. Information is considered to be personal data if it allows an individual to be singled out.

IAS does not collect or process information that is directly identifiable information concerning natural persons (for example individuals’ names). However, in the course of providing services to its Customers, IAS does collect IP addresses and user agent string, as well as other information which is linked to those pseudonymous identifiers, such as device type, operating system, browser configuration parameters, including browser type and language and session storage and local storage settings, and characteristics of your device such as the CPU class and time zone setting, which allow us to single out particular devices. This is generally considered to be personal data under the GDPR, and we treat it in line with our obligations under the GDPR.

IAS’S GDPR COMPLIANCE

IAS carried out a compliance project prior to GDPR coming into full effect, and we continue to work proactively with industry leadership and expert counsel to ensure ongoing compliance with GDPR. This ongoing compliance effort includes the following elements.

1. Identification of personal data usage and assessment of the impact of the GDPR

IAS has carried out an assessment of its services’ use of personal data, to establish the compliance impact of the GDPR. In particular, IAS has carried out an assessment of whether it acts as a ‘controller’ or ‘processor’ under the GDPR in relation to each of the services we provide. Details on IAS’s role in relation to its services can be found in the document *‘Is IAS a ‘controller’ or ‘processor’ under the GDPR?’* at <https://integralads.com/legal-portal/is-ias-a-controller-or-processor-under-the-gdpr/>.

2. Revisions to documentation

IAS maintains an up to date [privacy policy](#), in order to ensure that individuals are aware of how IAS processes their personal data to the extent that we act as a controller of that personal data in accordance with the requirements of the GDPR.

IAS has prepared documentation for its Customers found at <https://integralads.com/ias-data-protection-portal/>, so that Customers are aware of, among other things, the contractual terms IAS’s processing of personal data is subject to, details of IAS sub-processors, and details of the security measures IAS has in place for personal data. IAS contracts include a requirement for its Customers to notify individuals about IAS’s processing of their personal

data. The relevant suggested information to be provided by Customers can be found at <https://integralads.com/legal-portal/suggested-customer-privacy-policy-language/>.

3. **IAB Transparency and consent framework & Lawful basis for processing**

To ensure that IAS is able to understand when we are permitted to process personal data in order to provide our services, we have registered for and received approval from IAB Europe as a global vendor. Our global vendor number is 287 and we are included on the [IAB vendor list](#). For more information on the IAB Transparency and Consent Framework, visit <https://iabeurope.eu/transparency-consent-framework/>.

Where IAS acts as a processor on behalf of our Customers, those Customers are required to determine the appropriate lawful basis for their processing of personal data in the context of IAS's services.

To the extent that we act as a controller of personal data, IAS relies on our 'legitimate interests' in processing personal data it obtains. We have taken various steps (including those detailed in this document) to ensure that the rights and freedoms of individuals do not outweigh our clear legitimate business interest in providing our services.

IAS uses pixels and tags, which in addition to being subject to the GDPR, are subject to European e-Privacy rules, set out in Directive 2002/58/EC and its implementations in EU Member States. IAS considers that the pixels and tags we use are necessary for services provided by our Customers, and in any event are analogous to 'first party analytics' pixels and tags, which the European data protection supervisory authorities have indicated are considered as being unintrusive from a privacy perspective. In line with this guidance, IAS considers that prior consent is not required before these pixels and tags are used.

4. **Updated data minimization and retention policies**

IAS has taken steps to ensure that the level of personal data we collect is limited to what is adequate, relevant and necessary for any processing activities which we carry out. In particular, as set out above, IAS does not collect or process information that is directly identifiable information concerning natural persons, and the personal data it collects is limited to information linked to IP addresses and the user agent data.

This also includes ensuring that information may only be used to identify a particular individual for a limited period of time. IAS has a data retention policy in place, under which we maintain full IP addresses for only 30 days to enrich our invalid traffic detection and prevention processes. Invalid traffic is comprised of both general invalid traffic and sophisticated invalid traffic. For more information on IAS' invalid traffic services, see <https://integralads.com/capabilities/ad-fraud/>. After this 30-day period has expired, IAS will truncate IP addresses to the extent that they can no longer be used to identify an individual using any means reasonably available to IAS. A small sample of IP addresses (1%) will be maintained in salted one-way hash format for look-back analysis. These pseudonymized IP addresses will be deleted after 14 months.

5. **Honoring Data Subject Access, Erasure, and Data Portability requests**

IAS respects and acknowledges that data subjects frequently desire to exercise their rights over their personal data. Although IAS has no direct relationship with data subjects whose personal data we process on behalf of our customers, we have put in place internal processes to allow us to respond appropriately to requests from data subjects to exercise their rights, including the rights to access personal data, to correct, amend, or delete such data.

Data subjects that wish to exercise their rights in relation to personal data which IAS processes as a processor should direct his or her query to the specific client of IAS that has processed that personal data. If requested by a client to provide assistance with such requests, we will respond within 30 days. If IAS receives requests directly from a data subject, we will action them to the extent we act as a controller of any personal data relating to that data subject.

6. Privacy by Design

IAS has introduced enhanced risk management controls, in particular by introducing a Privacy Impact Assessments into product development, new business and partnership due diligence processes where required by the GDPR. The process of carrying out Privacy Impact Assessments helps us ensure that we consider GDPR compliance and data protection principles from an early stage in these areas.

7. Employee training and awareness

IAS carries out regular training for our employees, including training in relation to data protection matters. In particular, relevant employees are trained on the processes for responding to requests from individuals to exercise their rights, and on the steps to take in the event that they become aware of an actual or potential security incident affecting personal data.

8. Data Protection Officer

IAS has appointed a data protection officer to advise and assist us with compliance with obligations under the GDPR.

9. Data Security

IAS has an SOC 2, Type 1 report, in which independent auditors attest that its information security policies and practices met the SOC 2 requirements at January 31, 2018. This evaluation has determined that IAS takes commercially reasonable steps to ensure the ongoing confidentiality, integrity, availability and resilience of our systems and services processing personal data.

A summary of the security measures which IAS has in place to protect personal data can be found here <https://integralads.com/ias-data-protection-portal/ias-technical-and-organizational-security-measures/>.

10. Management of security incidents

IAS has an established incident response management process. This process ensures that IAS will notify Customers for which it acts as a processor about personal data breaches (as defined by the GDPR) without undue delay, and also ensures that, in relation to personal data which IAS processes as a controller, IAS is able to notify data protection supervisory authorities in the event of a personal data breach within 72 hours of becoming aware of that personal data breach.

IAS's incident response management process also includes a disaster recovery and business continuity plan, to ensure that we can continue providing our services in the event of a security incident.

11. Third parties

IAS subcontracts some processing of personal data to third party vendors ("sub-processors"). As set out above, IAS has a process in place to ensure that appropriate Privacy Impact Assessments are conducted as part of the partnership due diligence process. This involves taking steps to ensure that any third parties which are engaged by IAS provide sufficient guarantees that they are able to comply with their obligations and IAS's standards with respect to the protection of personal data.

IAS also takes steps to ensure that its contracts with sub-processors contain all the terms required by the GDPR in such contracts.

A list of the sub-processors currently engaged by IAS can be found here <https://integralads.com/legal-portal/ias-list-of-subprocessors/>.

12. Cross border transfers of personal data

As a global company working with international Customers, IAS may process personal data which is subject to the GDPR in locations outside the EEA, in particular the USA, where IAS is based. This will involve international transfers

of personal data from the European Economic Area to countries which are not considered by the European Commission to provide an adequate level of protection, we agree in our contracts with Customer to comply with the Standard Contractual Clauses for international data transfers adopted by the European Commission.

There are two types of Standard Contractual Clauses, one for international transfers to IAS as a controller, and one for international transfers to IAS as a processor. Copies of the Standard Contractual Clauses which IAS will comply with are available here <https://integralads.com/ias-data-protection-portal/>.

13. **Audit and Accountability**

IAS reviews its GDPR compliance practices on a regular basis.

CONTACT US

For further information or for any additional questions, please privacy@integralads.com.