IS IAS A "CONTROLLER" OR "PROCESSOR" UNDER THE GDPR?

The GDPR draws a distinction between processing of personal data carried out by "controllers" and by "processors". Controllers determine the purposes for which personal data is processed and the means by which personal data is processed: essentially, a controller decides "why" and "how" personal data will be processed. By contrast, a processor processes personal data only on the instructions of and on the behalf a controller. While a processor may have some role in determining precisely "how" personal data is processed, the decisions about the purposes of processing ("why" personal data is processed) remain with the controller.

The GDPR requires that there is a lawful basis for all processing activities. However, this only applies to controller. Therefore, IAS is only required to have a lawful basis for processing personal data where IAS is a controller. Similarly, IAS's Customers are responsible for having their own respective lawful basis for processing personal data as a controller in their own right, including in the circumstances in which a Customer appoints IAS to act as a processor on that Customer's behalf. To the extent that a Customer's lawful basis for processing personal data is their legitimate interests or the legitimate interests of a third party in accordance with Article 6(1)(f) GDPR, then such Customer is responsible for carrying out any legitimate interests assessments relevant to its subsequent use of services in relation to which IAS acts as a processor.

IAS provides a number of different services to its Customers, and in line with regulatory guidance has assessed that it acts as a controller and a processor depending on the processing being carried out.

IAS acts as a **processor** in respect of:

- **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 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;

- **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 client's needs when an impression on that site is received. IAS does not use information collected from impressions for purposes other than ensuring a client's ads are not served on sites or mobile applications that do not meet that client's requirements; and

- **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 the approximate (but not precise) location of that IP address. IAS only uses this information to provide geo-verification to the specific client that has requested it, and not for any other purpose, so again only acts on its specific client'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 with Customers.

By contrast, IAS is a controller in respect of:

- **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 analyses 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 blacklists. 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, and is a controller in relation to personal data used for these services. IAS shares the ad fraud blacklists 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.

- **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, using any means reasonably available to IAS, to identify an individual or Customer. 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.

IAS also offers Online Conversion Lift services, but these are not available to Customers in EMEA at this time. When IAS begins to offer these services to Customers in EMEA, this document will be updated to reflect IAS's position as a controller or processor in respect of that service.