Inskin Media Good Data Practice

Personal information collected by Inskin

Business data

In the course of providing services Inskin needs to collect and use information about its clients, suppliers and prospects. Information we collect includes names, job titles, telephone numbers, email addresses, business addresses, business bank account details and activity on inskinmedia.com.

Advertising technology data

Inskin does not process any sensitive personal data for ad serving. We also do not process any personal data that is directly personally identifiable (e.g. name, email address). We currently process indirect personal identifiers:

- IP address
- Inskin unique user ID

Additionally, Inskin works with the following ad tech providers:

- MOAT: used for campaign ad validation, does not drop cookies or make use of any personal information, including indirect identifiers
- comScore: Inskin implements comScore's GDPR compliant tags on our network to assess actual network reach
- Lotame: used for targeting adverts to broad categories of users. All Lotame data is subject to a GDPR compliant Data Licensing Agreement that ensures that all consents and legal bases for processing have been secured.

Website visitors

Inskin uses Google analytics to track user activity on inskinmedia.com, which does not include any personal identifiable information. We also use Eloqua to track user activity on inskinmedia.com for lead generation and marketing activities.

How Inskin collects data

Inskin collects client data directly from its clients, suppliers and prospects via meetings, telephone, email, contracts/agreements and/or submission forms on inskinmedia.com. We also use data from Alf Insights for lead generation purposes. We are waiting for verification from Alf Insights that their data sources are GDPR compliant.

How Inskin uses data

Client and supplier data is used for communication to ensure that contractual obligations are met. Prospect data is used for marketing campaigns, lead generation and CRM.

Advertising technology

The limited amount of personal data (in the form of indirect personal identifiers) we use for ad serving is used solely for the originally intended purpose of ad serving. Specifically, Inskin only uses IP addresses for fraud detection and approximate geographical assessment.

Inskin's lawful ground for processing data: legitimate interest

Client data

Inskin only processes client data to fulfil contractual obligations as a service provider i.e. to run ad campaigns on behalf of agencies / brand clients.

Supplier data

Inskin only uses personal data to facilitate the receipt of services rendered by suppliers and to pay for those services.

Advertising technology

We cite legitimate interest for processing the following items of data:

- IP address for fraud detection: to combat ad fraud from IPs that are either known to host non-human traffic or where our impression and click analysis indicates potential fraud
- IP address for geographical targeting: in some cases it is a legal requirement to restrict the display of certain adverts to certain countries, for example alcohol in Saudi Arabia. We also cite legitimate interest to allow us to perform limited location targeting (to city level)
- Browser unique ID (via a cookie): to allow us to approximate the number of unique users in our network

We only use the above items of data for the purposes stated. Specifically we do not use them to offer retargeting capabilities or to create user profiles.

Inskin's lawful ground for processing data: consent

Prospect data

We cite consent for the use of data supplied directly from prospects for marketing purposes. Where data is collected directly from prospects via meetings, events, telephone, email, and submission forms on inskinmedia.com, the subsequent use of that data is made clear, either verbally or in writing. Inskin's email communications are sent on a double opt-in basis.

How Inskin safeguards data

Inskin is committed to protecting personal information from misuse, loss or unauthorised access. We have a range of appropriate technical and organisational measures in place to safeguard personal data: all data is stored on secured servers and controlled by access rights.

Advertising technology

Inskin does not process any personal data within our ad serving methods, therefore there is no risk of its misuse, loss or unauthorised access.

Where Inskin uses indirect personal identifiers:

- we record full IP addresses within our databases for 90 days before they are eventually obfuscated. This allows us to perform fraud detection analysis after an ad request has been received, and limits the amount of time this personal data is kept in any identifiable form
- the obfuscation of IP address involves setting the last octet to zero
- all data (whether personal or not) is held on secured servers with very limited access, and always transferred using secure protocols

Fair processing

Inskin treats all personal data as confidential and only processes data for contractual obligations and where an individual has consented by opting in to marketing activities.

Advertising technology

For fair and transparent processing, we inform users of the personal information that we process (IP addresses, unique user IDs), and the reasons why we process it, in our privacy policy.

Personnel handling personal data

Inskin has appointed a Data Protection Officer to ensure that there are policies and procedures in place for the handling of personal data by personnel. Access to personal data is granted to employees by authorised personnel on a need to know basis.

Advertising technology

The limited personal data that Inskin processes does not form part of our business reporting systems so does not appear in reports accessible to Inskin employees, except on a need to know basis, for example processing payments.

Inskin's back-end data systems are partitioned to allow us to limit access to the datasets that contain indirect personal identifiers, providing a greater degree of security.

Additionally, access to our back-end systems is strictly limited to a known number of developers and admins. We employ multi-factor authentication to all our back-end systems.

Data retention

Business data

Inskin safely retains all past and present client, supplier and prospect data unless the data subject requests its deletion.

Advertising technology

Following IP address obfuscation, as explained above, it is impossible to trace the data back to any individual, even with ISP records.

Data transfer

Inskin does not transfer client, supplier or prospect personal data in any form.

Advertising technology

Most of our data processing takes place within the EU, however we employ some services which are based outside of the EU. In these cases, limited personal data (only in the form of indirect identifier IP Address) is passed to a non-EU country (US).

Subject access requests

Individuals have the right to request the modification, update or erasure of the personal data held by Inskin. Upon such a request, we may ask for identity verification and seek more information about the request. Where we are legally permitted to do so, we may refuse the request and give reasons for that.

For subject access requests, if you suspect any misuse or loss of or unauthorised access to your personal information or to withdraw your consent to the processing of your personal data, contact Inskin at gdpr@inskinmedia.com or write to us at:

Inskin Media Ltd
233, High Holborn
London
WC1V 7DN

Advertising technology

As detailed in Inskin's privacy policy, data subjects are not notified of the processing of their indirect personal identifier data.

Subject access requests for IP addresses will require proof from the requestor that they own the IP address. Fulfilment of such requests may not be possible as IP obfuscation renders the data unidentifiable and therefore unavailable.

Demands for rectification and erasure are not applicable.

DPO and third party enquiries

Inskin undertakes to respond to valid data protection queries and concerns from affected parties in a timely and helpful manner.

Data Protection Officer: S Jaffer
Email: gdpr@inskinmedia.com

Sub-processors

Inskin makes use of GDPR-compliant third-party services throughout our business, some of which are used to help us process client, supplier and prospect personal data. Examples of such sub-processors are Salesforce (for contact and campaign information) and

Sage/Fastpay (for accounting/payments processing). All such sub-processors are well known, often de facto, industry-standard services with comprehensive GDPR compliance statements.

Our advertising technology makes use of secure, GDPR-compliant, third-party services, where the limited amount of personal information we have access to is processed. We do not currently have plans to change the sub-processors we use, but any future providers will only be used if we are satisfied that their services offer the security we require, including GDPR compliance.

Personal data breach

In the event of a data breach of client, supplier and/or prospect personal data, Inskin will apply appropriate measures to investigate the breach and will notify any affected individuals without undue delay and, if required, notify ICO within 72 hours.

As Inskin's advertising technology only stores indirect personal identifiers, a breach of such data would not identify specific individuals, and therefore no notification of individuals would be necessary or possible.

Last updated: 17 September 2018