SIGNAL

Signal's Commitment to Privacy

GDPR and Privacy by Design

The General Data Protection Regulation provides a new context for thinking about consumers and privacy globally. Signal works closely with our clients and partners not only to ensure compliance with GDPR and related EU regulations, but also to build meaningful privacy choices for consumers based on transparency and trust.

Signal, from the start, has followed the core principles of Privacy by Design in building its platform and its business relationships. Privacy by Design is a commitment to think about privacy first and to always look for ways to enhance the privacy features of our platform.

We continue to make enhancements that take full advantage of the advancements in transparency and choice that are evolving across the marketing ecosystem.

Signal's Role Under GDPR

Signal's primary role under GDPR is as a data processor.

Signal's clients directly control the collection and use of their first-party data within our platform. Signal maintains a secure operating environment and provides tools and processes that our clients can use when honoring their privacy policies and GDPR obligations.

Signal plays a secondary role as a data controller for its third-party cookie ID and the Signal Identity Network.

The data controller role is held by all platforms that set third-party cookies and helps brands connect data to partners. In the limited cases where Signal acts as a data controller, we provide consumers with all of the necessary rights and protections covered in the GDPR and the ePrivacy Directive.

Our Legal Basis for Data Processing

Signal requires consent before our cookie is set, and we only work with data for which there is a valid legal basis for processing. Signal is a registered participant in the IAB EU Transparency and Consent Framework. We actively participate in the implementation of the framework and technical initiatives focused on ensuring data is collected and processed only when there is a clear basis for doing so.

Tenets of Signal's Privacy by Design

Signal adheres to the following core principles in both our platform design and business practices:

Signal takes its data governance and privacy responsibilities very seriously.

Clients are in full control of their data and identity assets.	• Signal does not own or control the client's data or identity. • Signal only contracts with clients and partners who certify that they comply with all privacy laws and self-regulatory group guidelines.
Signal's clients decide:	• What types of first party data to collect. • Where to collect that data from. • Whether to sync that data with a third-party's data. • How to use that data and whom, if anyone, to share it with.

Signal employs a robust information security program to protect clients' data.

Signal provides clients with tools to help support their consumer privacy obligations, respective to Signal's role as a data processor.	• These include platform features and processes that help manage customer consent and preferences, and respond to GDPR Data Subject Rights requests.

Signal minimizes the scope of data that is collected and stored in its platform.

Signal's platform does not collect, store or use directly identifiable information – meaning someone's name, street address, email address, telephone number or other information that specifically identifies an actual person.

Signal's technology uses only pseudonymous identifiers such as cookies, device IDs and hashed values:	• Client data is transmitted and stored using industry-standard hashing protocols that replace direct identifiers with a strongly encrypted value that cannot be reversed. • Signal does not process information that can be used to match pseudonymous identifiers back to directly identifiable customers, and contractually prohibits its clients and partners from re-identification.

Signal limits the type of data stored and the length of data retention to one year. Signal's data governance policies require data deletion after retention periods have expired.

Signal participates in industry programs such as the IAB EU Transparency and Consent Framework and the Network Advertising Initiative (NAI), and proactively approaches global regulatory requirements including the GDPR.

Read our full privacy policy at **www.signal.co/privacy-policy.**

Signal's privacy team is available to answer questions. Contact your Signal account representative to get in touch.