

Platform Privacy Notice

Xapien

Last updated: August 2026

This privacy notice explains how Xapien (“we”, “us”, or “our”) collects, uses, and protects personal information we process in the course of delivering our services to our customers. Our services involve the preparation of due diligence and background reports on individuals and organisations for our customers.

This notice should be read together with our overarching Privacy Notice and our Website Privacy Notice.

Who We Are

Xapien is the trading name of Digital Insight Technologies Limited, registered in England under company number 11241397, with a registered office at St John’s Innovation Centre, Cowley Road, Cambridge, United Kingdom, CB4 0WS, and ICO registration number ZA385612.

When we process personal data to prepare and deliver reports as part of our services, we act as a controller in respect of that processing, except where we have agreed with a customer that we act as their processor.

Whose Personal Data We Process

We process personal data about the individuals who are the subject of the reports we prepare for our customers. This may include the individuals our customers ask us to screen or research, together with other individuals connected to them where relevant to the purpose of the report.

We also process personal data about the staff of our customers and prospective customers, for example where we correspond with them or record meetings with them. Where we do so, this notice applies to that processing as well.

Personal Data We Process

Depending on the scope of the report requested by our customer, we may process the following categories of personal data:

- Identity and contact details (such as name, date of birth, nationality, and contact information)
- Professional and employment information (such as roles, directorships, corporate affiliations, and business interests)
- Publicly reported information from news and other media, including adverse media
- Regulatory, legal, and enforcement information (such as sanctions and watchlist matches, litigation, insolvency, and regulatory findings)
- Politically exposed person (PEP) status
- Information published by the data subject themselves, including on websites and social media

Some of this information may include special category data (for example, where media reporting reveals information about political opinions, religious beliefs, or health) or information relating to criminal offences and alleged offences. We only process such information where a condition under data protection law permits us to do so — for example, where the processing is necessary for reasons of substantial public interest, such as the prevention and detection of unlawful acts, fraud, money laundering, or other financial

crime, or to comply with regulatory requirements, or where the personal data has been manifestly made public by the data subject.

Where We Obtain Your Personal Data

We obtain personal data from:

- Publicly available sources, such as public registers, company filings, court and regulatory records, sanctions and watchlists, news and other media, publicly accessible websites and social media, trade and industry references, professional directories, print and broadcast media, and company websites. This information may include your name, age, contact information, employment history, family and professional affiliations, reputational background information, and sanctions or litigation involvement.
- Trusted third-party data and intelligence providers or data brokers. This information may include your name, demographic information, educational information, professional and employment-related information, and sanctions or litigation involvement.
- Information provided to us by our customers who purchase our services.
- Correspondence you send to us, including through email, messages on our online platforms, and information processed in discussions with you.
- Recordings of calls and video meetings with our staff, including the audio, a transcript and related metadata. We use these recordings to keep a record of what was discussed, for training, and to support our sales activity. We will always tell you before recording, and will ask for your consent where required.

Our Use of Artificial Intelligence

We use artificial intelligence-enabled tools, models and agents to support the creation, operation, improvement and delivery of our services. This includes assisting with the identification, collection, organisation, classification, enrichment, verification, summarisation and quality checking of information gathered from the sources described above, and with analysing or summarising recorded meetings.

All such use is subject to appropriate human oversight and review. These tools support decisions made by our people rather than replacing them, and we do not make decisions producing legal or similarly significant effects based solely on automated processing.

How We Use Your Information

We use your personal data for the following purposes:

- Preparing and delivering due diligence, screening, and background reports to our customers
- Enabling our customers to carry out due diligence, know-your-customer (KYC), anti-money laundering (AML), and sanctions checks
- Helping our customers to prevent and detect fraud, bribery, corruption, and other financial crime
- Helping our customers to assess risk and meet their legal and regulatory obligations
- Maintaining, securing, and improving our services
- Complying with our own legal and regulatory obligations

Lawful bases

We rely on the following lawful bases when processing your personal data:

Purpose / Activity	Lawful basis for processing
To provide our products and services	(a) Performance of a contract with our customers; and (b) necessity for our legitimate interests (for instance, to keep our records updated and to grow our business)
To notify you about changes to our terms or this privacy notice	Necessity to comply with a legal obligation
To make suggestions and recommendations about things similar to those you have enquired about or that may otherwise be of interest to you or our customers, or, where permitted by law, to send promotional materials from us	Necessity for our legitimate interests (namely, to grow our business)
To improve our products and services and ensure that content is presented in the most relevant and effective manner; to administer our products and services, including troubleshooting, data analytics, testing, research, and statistical and survey purposes; and to keep our products, services, business and users safe and secure. This includes our use of artificial intelligence as described above.	Necessity for our legitimate interests (for running, protecting and growing our business; for provision of administration and IT services; for network security and to prevent fraud; in the context of a business reorganisation or group restructuring exercise; to study how people use our products and services, to develop and keep them updated and relevant, to grow our business and to inform our communications strategy)
To train our staff and support our sales activities	Necessity for our legitimate interests (for running, protecting and growing our business)
To comply with applicable laws and regulations, and to protect or exercise our legal rights or defend against legal claims	Necessity to comply with a legal obligation

Where we process personal data on the basis of our legitimate interests, we consider and balance any potential impact on you and your rights. Our legitimate business interests do not automatically override your interests, and we will not use your personal data where our interests are overridden by the impact on you, unless we have your consent or are otherwise permitted or required by law.

Where we are legally required to obtain consent and have no other valid legal basis, we will do so. You may withdraw consent at any time by contacting us. Withdrawing consent does not affect the lawfulness of processing carried out before it was withdrawn.

Sharing Your Information

We may share personal data with:

- Our customers, as part of our services. We require customers to comply with applicable law.
- Service providers and sub-processors who support our services, including AI-enabled tools (such as hosting, operating system and platform providers, infrastructure, call recording and IT providers, and research providers), appointed under appropriate contractual terms
- Corporate affiliates, including in connection with corporate transactions
- Professional advisers where appropriate
- Regulators, law enforcement, and other authorities where legally required, and to protect and defend our rights or the rights of our users or the public

- Others with your consent, where we have disclosed that purpose to you at the time of collection

International Transfers

Personal data may be transferred to, stored, or processed outside the United Kingdom, the European Economic Area, or your resident jurisdiction, including in countries that may not provide the same level of protection as your own.

Where this occurs, we ensure appropriate safeguards are in place. For transfers from the United Kingdom we rely on UK adequacy regulations where they apply, and otherwise the ICO's International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses. Where the EU GDPR applies to a transfer, we use the EU Standard Contractual Clauses. In each case we carry out a transfer risk assessment and apply any supplementary measures identified.

Data Retention

We retain personal data only for as long as is reasonably necessary for the purposes set out in this notice, including to deliver our services, to enable our customers to evidence their own due diligence and meet their regulatory obligations, and to comply with our legal obligations. Retention periods are determined by the nature of the report and the applicable legal and contractual requirements, having full regard to the principle of data minimisation.

Your Rights Under the UK and EU GDPR

If you are in the United Kingdom or the European Economic Area, you have the following rights. If you are a California resident, please see the separate section at the end of this notice.

- **Right of access.** You have the right to ask us for copies of the personal data we process about you.
- **Right to rectification.** You have the right to ask us to correct personal data you believe is inaccurate.
- **Right to erasure.** You have the right to ask us to erase your personal data in certain circumstances.
- **Right to restriction.** You have the right to ask us to restrict our processing of your personal data in certain circumstances.
- **Right to object.** You have the right to object to our processing of your personal data in certain circumstances.
- **Right to data portability.** You have the right to ask that we transfer your personal data to another organisation in certain circumstances.
- **Right to complain to us.** You can raise a concern with us directly at info@xapien.com and we will look into it.
- **Right to complain to a supervisory authority.** You can complain to the Information Commissioner's Office (ICO) at ico.org.uk, or to the supervisory authority in your country of residence or work.

The ICO can be contacted at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, or on 0303 123 1113.

How to exercise these rights

Contact us at info@xapien.com or by post at the address in the Contact Us section below. You do not have to pay a fee. We will respond within one month, which we may extend by a further two months where a

request is complex or where we have received a number of requests from you — we will tell you if that happens and explain why.

We may need to verify your identity before acting on a request. You may also submit a request through an authorised agent, in which case we may ask for evidence of a power of attorney or other written authority.

Automated Decision-Making

Xapien does not make decisions producing legal effects, or similarly significant effects, concerning data subjects based solely on automated processing.

Children

Xapien does not knowingly process personal data about a child as defined by applicable law. If you believe we may have processed personal data about a child, please contact us.

Security

Xapien implements appropriate and reasonable technical and organisational measures to protect personal data against unauthorised access, alteration, disclosure, or destruction, and to help ensure that personal data is reliable and accurate. No data storage system or transmission of data can be completely guaranteed. Information collected by third parties may not have the same security protections as information you submit to us, and we are not responsible for the security of such information.

Changes to This Notice

We may update this privacy notice from time to time. The updated version will be indicated by the “Last updated” date at the top. We encourage you to review this notice periodically.

Contact Us

If you have questions about this privacy notice or our data practices, please contact us at:

info@xapien.com

St John’s Innovation Centre, Cowley Road, Cambridge, United Kingdom, CB4 0WS

Additional Information for California Residents

This section applies to California residents and supplements the information above. It explains your rights under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the “CCPA”).

Categories of personal information

In the course of providing our services, we may process the following categories of personal information about California residents. Where our reports include information about political or religious beliefs, health, or criminal history, this may constitute sensitive personal information.

Categories of personal information collected	Identifiers, such as name and contact details. Characteristics of protected classifications under California or federal law, including race and gender, where revealed in media reporting. Professional, education, or employment-related information. Inferences drawn from the above.
Purposes for which those categories are collected or used	To provide our diligence and research services, as described in “How We Use Your Information” above.
Purposes for which those categories are disclosed or sold	Disclosed to the customer who commissioned the relevant report, to our service providers and sub-processors, to professional advisers, and to regulators or authorities where legally required.

We collect this information from the sources described in “Where We Obtain Your Personal Data” above.

Categories of third parties

Personal information may be disclosed or sold, as those terms are defined in the CCPA, to the following categories of third parties, all of whom are either our customers or provide services to us:

Consumer products and services companies	Casinos and gambling companies	Data analytics organisations	Government organisations
Not-for-profit organisations	Public entities	Business-to-business organisations	Entertainment companies
Universities and academic institutions	Law firms	Operating systems and platforms	Banks and financial institutions
Internet service providers	Accountancy firms	Manufacturing companies	Business services and agencies
Communications services companies	Marketing companies		

Requests received

Requests received under the California Consumer Privacy Act for the calendar year January to December 2025:

Type of request	Number received
Request to opt out	0
Request to know whether personal information is sold or shared	0

Type of request	Number received
Request to know what personal information is collected	0
Request to delete	0
Request for access	0
Request to limit use or disclosure of sensitive personal information	0
Total	0

Your rights under the CCPA

Subject to verification and to the limits described below, California residents have the right to:

- **Right to know.** You may request the categories and specific pieces of personal information we have collected, the sources we collected it from, the purposes for collecting it, and the categories of third parties to whom we disclose it.
- **Right to delete.** You may request deletion of personal information we have collected from you.
- **Right to correct.** You may request correction of inaccurate personal information.
- **Right to opt out.** You may opt out of the sale or sharing of your personal information.
- **Right to limit.** You may direct us to limit the use and disclosure of sensitive personal information to what is necessary to provide our services.
- **Right to non-discrimination.** You will not receive discriminatory treatment for exercising any of these rights.

How to exercise these rights

Contact us at info@xapien.com or by post at the address in the Contact Us section above. We will respond within 45 days, which we may extend by a further 45 days where reasonably necessary — we will notify you within the first 45 days if we need to do so.

We will take steps to verify your identity before responding and may need to request additional information for that purpose. You may use an authorised agent to submit a request on your behalf, in which case we may require proof of the agent's authority.

Limits on these rights

Because our services support customer due diligence, anti-money laundering, fraud prevention, and similar regulated activities, certain rights may not apply, or may be limited, where an exemption under the CCPA applies. For example, this may be the case where retention or processing is necessary to detect security incidents, to protect against fraudulent or illegal activity, to comply with a legal obligation, or to exercise or defend legal claims.

Where we act as a service provider to a customer, we will direct your request to that customer or assist them in responding to it.