KYND LIMITED

Privacy Policy

1. Introduction

KYND Limited and its affiliates ("KYND", "we", "our" or "us") take the privacy and protection of personal data seriously. This Privacy Policy explains how KYND collects and uses your personal data when you visit our website, use our platform or services, communicate with us, or otherwise interact with us. We encourage you to read it carefully.

By using our services or visiting our website, you acknowledge that you have read and understood this Privacy Policy. Where we rely on your consent as a lawful basis for processing, we will ask for it separately and explicitly, and you may withdraw it at any time by contacting us at legal@kynd.io. Our lawful bases for processing personal data are set out in full in Section 10.

If you do not agree with this Privacy Policy, please do not use our website, platform, or services.

We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and, where applicable, the EU General Data Protection Regulation (EU GDPR). For the purposes of applicable data protection law, the data controller is KYND Limited, Unit 3-4, The Grain Store, 70 Weston Street, London SE1 3QH.

2. Information Covered by this Policy

For the purposes of this Privacy Policy, our use of the term "Information" means information we receive from or about you, including information collected directly or indirectly, manually or automatically, through our website, platform, services, communications, business dealings, or third-party sources.

- "Non-Personal Information" means information that does not identify a natural person.
- "Personal Information" or "personal data" means information relating to an identified or identifiable natural person, such as names, addresses, email addresses, telephone numbers, online identifiers, and other information associated with an identifiable individual.

3. Acceptance of Terms

We obtain and use Information in accordance with this Privacy Policy. We will ask for your consent before using Personal Information in a manner that requires consent under applicable law and is not otherwise described in this Privacy Policy.

Where consent is our lawful basis, we will obtain it through a separate, clear and affirmative action. Where we rely on other lawful bases, including contract, legal obligation, or legitimate interests, those bases are explained in Section 10.

4. How We Obtain and Collect Your Personal Information

We collect Personal Information from you:

- directly from our business interactions, communications, and dealings with you, including when you register with us, contact us, send us feedback, use our services, post material to our website, complete surveys, request support, subscribe to marketing communications, or attend events in which we participate;

- indirectly when you interact with our website or use our services, including through browsing activity and the technologies explained in our Cookies Policy;
- from your employer, colleagues, customers, service providers, public sources, and other third parties where this is relevant to the services we provide; and
- incidentally in the course of cyber risk assessments, as explained in Section 6.

5. What Kinds of Personal Information We Collect

Depending on your relationship with us, we may collect the following Personal Information:

- your name, job title, employer, business contact details, company details, and marketing preferences;
- demographic information such as postcode, preferences, and interests;
- details of information, feedback, support requests, or other matters you give us by phone, email, post, website form, social media, or other communications channels;
- account, onboarding, billing, subscription, and service-administration information;
- payment and billing information, subject to appropriate payment-processing safeguards;
- information about your interest in, use of, and interactions with our products and services;
- technical information, including internet protocol (IP) address, browser type and version, browser plug-in types and versions, operating system, platform, device identifiers, files requested, referring URLs, and website or country from which you access information; and
- information about your visit to and behaviour on our website or platform, including date and time of visits, time spent on pages, page interaction information, traffic data, location data, weblogs, communication data, and information provided when requesting services or downloads.

6. Personal Data Encountered During Cyber Risk Assessments

KYND's core service involves scanning publicly accessible internet infrastructure to identify cyber risk signals on behalf of our customers. This scanning is directed at technical systems and infrastructure, not at individuals. However, in the course of this work, our platform may incidentally encounter personal data that appears in publicly accessible sources, including:

- email addresses appearing in SSL/TLS certificates, WHOIS records, DNS configurations, or other public technical records;
- names or job titles of technical contacts visible in publicly accessible system records; and
- email addresses or credentials inadvertently exposed in misconfigured or unsecured services.

KYND may retain WHOIS registrant details encountered during assessments as part of the risk intelligence record for a given domain or organisation. Where WHOIS records contain personal data relating to an identifiable individual, as distinct from purely organisational information, we rely on legitimate interests as the lawful basis for retention. The publicly accessible nature of WHOIS data is a relevant factor in our legitimate interests assessment but does not override individual rights. If you believe your personal data is held within a WHOIS record and wish to exercise your rights, please contact legal@kynd.io and we will assess your request.

Why we process this data

This personal data is not sought or targeted. It is encountered incidentally as a by-product of scanning infrastructure for technical risk indicators. Where it is encountered, we process it solely for the purpose of identifying and reporting cyber risk signals to the customer on whose behalf the scan is conducted.

We rely on legitimate interests as the lawful basis for this processing under Article 6(1)(f) UK GDPR. Our legitimate interest, and that of our customers, is to provide accurate and complete cyber risk assessments. We have assessed that this interest is not outweighed by the rights and freedoms of the individuals whose data may be incidentally encountered, given the limited nature of the processing, the fact that the data is already publicly accessible, and the limited period for which it is retained.

How long we keep it
Personal data encountered incidentally during assessments is retained for a minimum of 90 days from the date of discovery and then permanently and securely deleted, unless a longer period is required by law, necessary to investigate or evidence a security issue, or otherwise specified in a customer contract. It is not used for any purpose other than the assessment in which it was encountered, and it is not shared with any third party other than the organisation on whose behalf the scan was conducted, our contracted service providers acting on our instructions, or where required by law.

Your rights
If you believe KYND has encountered your personal data in the course of an assessment and you wish to exercise your rights, including the right to access, erasure, objection, or restriction, please contact us at legal@kynd.io. We will respond within the timeframe set out in Section 16.

7. Cookies
We may store and retrieve information on and from your browser by placing small text files called cookies on your computer, smartphone, or other device. Cookies help us operate our website and services, analyse website traffic, remember preferences, improve our services, and understand how users interact with our website.

For more information about the cookies and similar technologies we use, the purposes for which we use them, and how you can manage your preferences, please see our Cookies Policy.

8. Non-Personal Information
Non-Personal Information may be collected, processed, and used in accordance with applicable law for our internal business purposes, including to improve our services and website, to improve marketing and promotional efforts, to improve customer service, and to tailor content and service offerings to customers' needs. We may also use aggregated or anonymised information, which does not identify you, for analytics, reporting, research, product development, and other lawful business purposes.

9. What We Do with the Personal Information We Collect
We use Personal Information where necessary or appropriate for the following purposes:

- to create, manage, and administer our business relationship with you or the organisation you represent;
- to provide, operate, support, maintain, and improve our website, platform, and services;
- to provide and report cyber risk assessments to our customers;
- to communicate with you about our services, your use of our website or platform, service updates, support requests, billing, and administrative matters;
- to respond to requests you make;
- to process payments, issue invoices, resolve fee disputes, and provide associated billing services;
- to develop, improve, and test services, products, features, functionality, and performance;
- to comply with legal and regulatory obligations;
- to monitor compliance with our contractual terms, rulebooks, and acceptable-use requirements;

- to better understand our customers and how they use and interact with our website and services;
- to enhance security, prevent fraud, monitor and verify identity or service access, combat spam, malware, or other security risks, and protect our business;
- to deliver marketing communications and service update notices where permitted by law;
- to facilitate events in which we participate and communicate with you about those events;
- to enforce agreements with third parties; and
- to establish, exercise, and defend our legal rights.

We may create anonymised information from Personal Information by excluding information that makes the data personally identifiable. We may use anonymised information for internal purposes, including analysing usage patterns and improving our website and services, and may disclose anonymised information to third parties where lawful.

10. Lawful Bases of Our Use of Your Personal Information

We rely on one or more of the following lawful bases when processing Personal Information:

- performance of a contract, where processing is necessary to perform a contract with you or to take steps at your request before entering into a contract;
- legal obligation, where processing is necessary to comply with our legal or regulatory obligations;
- legitimate interests, where processing is necessary for our legitimate interests or the legitimate interests of others, and those interests are not overridden by your interests, rights, and freedoms;
- consent, where we ask you for separate and explicit consent for a specific processing activity; and
- vital interests or public interest, where applicable in limited circumstances.

Where we rely on legitimate interests, we undertake a balancing assessment to ensure that those interests are not outweighed by your interests or fundamental rights and freedoms. Where we rely on consent and you later change your mind, you may withdraw your consent at any time by contacting us using the details in Section 20.

11. Marketing Activities

We may collect and use Personal Information for marketing activities by email, telephone, and post, where permitted by law. We may send marketing communications, including electronic marketing communications, to existing customers, where it is in our legitimate interests to do so for marketing and business development purposes, or where we have obtained consent if required by law.

We will obtain your consent to direct marketing communications where required by law, for example where you have provided a personal email address and consent is required, or if we intend to disclose your Personal Information to a third party for that third party's own marketing purposes.

You may opt out of marketing communications at any time by using the unsubscribe link in our emails or by contacting us using the details in Section 20.

12. Security and Confidentiality

We have put in place commercially reasonable and appropriate technical and organisational measures designed to protect Personal Information from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access. These measures include physical, electronic, and managerial procedures to safeguard and secure Personal Information.

However, no method of transmission over the internet or electronic storage is completely secure, and we cannot guarantee absolute security. We will notify affected individuals and any applicable regulator of a personal data breach where legally required to do so.

13. To Whom We May Disclose Your Information

Except as otherwise stated in this Privacy Policy, we will not disclose or share your Personal Information with third parties unless you ask or authorise us to do so, or unless disclosure is permitted or required by law.

We may disclose Personal Information to:

- our subsidiaries and other companies under common control, provided they are required to handle Personal Information in accordance with this Privacy Policy or equivalent safeguards;
- your employer and colleagues within the organisation you represent, where relevant to the services we provide;
- the customer on whose behalf a cyber risk assessment is conducted, where the information forms part of the risk assessment output;
- legal, regulatory, law-enforcement, governmental, or public authorities where required or permitted by law;
- business partners, third-party service providers, processors, and suppliers who work on our behalf to provide, operate, improve, understand, customise, support, analyse, and secure our website, platform, and services;
- analytics and search engine providers that assist us in improving and optimising our website and services;
- professional advisers, including lawyers, auditors, insurers, and accountants;
- third parties involved in a merger, acquisition, financing, reorganisation, sale of assets, insolvency, or similar business transaction; and
- other third parties where we believe in good faith that disclosure is necessary to comply with law, respond to legal process, respond to an emergency, protect and defend KYND's rights or property, or protect the security and integrity of our services.

We do not sell Personal Information. We do not grant our service providers an independent right to use Personal Information except as necessary to provide services to us, comply with law, or support our legitimate business interests under appropriate contractual safeguards.

Third parties you interact with, including your employer, may have their own privacy policies. KYND is not responsible for those third parties' operations or personal information practices. We encourage you to review their privacy practices.

14. Links to Other Websites

Our website may contain links to other websites of interest that are not owned or controlled by us. The provision of such links does not signify our endorsement of those websites or their content. We do not control, review, or take responsibility for the privacy policies, terms of use, content, or protection and privacy of information you provide while visiting other websites. You should exercise caution and review the privacy policy applicable to the website in question.

15. Access to, Correcting, or Deleting Your Personal Information

If we hold Personal Information about you, you may request that we correct, amend, or delete information where it is inaccurate or where applicable law gives you that right. Before fulfilling a request, we may ask you to provide information so that we can verify your identity.

Subject to applicable law, we may decline requests that are manifestly unfounded or excessive, present a risk to the privacy of another individual, may jeopardise the confidentiality of another party, would require disproportionate technical changes, or where we are required or permitted to retain the information. Please contact us using the details in Section 20 if you need assistance updating or reviewing your information.

16. What Are Your Rights

Under applicable UK and EU data protection law, you may have the following rights:

- the right to be informed about our collection and use of your Personal Information;
- the right to access the Personal Information we hold about you;
- the right to have incomplete or inaccurate Personal Information corrected;
- the right to ask us to delete or otherwise dispose of your Personal Information;
- the right to restrict the processing of your Personal Information;
- the right to object to our use of your Personal Information for particular purposes;
- the right, in some circumstances, to request that we port your Personal Information in a portable and reusable format to another organisation, where technically feasible;
- the right to withdraw consent where consent is our lawful basis for processing; and
- the right not to be subject to certain decisions based solely on automated processing, where applicable.

We will respond to rights requests within 30 calendar days of receipt. Where a request is complex or you have made numerous requests, we may extend the response period by up to a further two months, where permitted by law. If we extend the period, we will tell you within the first 30 calendar days and explain why the extension is necessary.

Certain Personal Information may be exempt from such requests in particular circumstances, for example if we need to keep using the information to comply with legal obligations or to establish, exercise, or defend legal claims. If an exception applies, we will tell you when responding to your request. We may ask you to provide information necessary to confirm your identity before responding.

Further information about your rights may be obtained from the Information Commissioner's Office (ICO) or your local Citizens Advice Bureau. If you have a complaint about our use of your Personal Information, you have the right to lodge a complaint with the ICO. The ICO can be contacted via https://ico.org.uk/make-a-complaint.

17. How Long We Retain Your Personal Information

We keep Personal Information only for as long as necessary for the purposes for which it was collected and processed, including to provide services, comply with legal and regulatory obligations, resolve disputes, enforce agreements, and establish, exercise, or defend legal claims. Our retention periods are determined by the nature and sensitivity of the data, the purposes for which it is processed, contractual requirements, legal and regulatory requirements, and the risk of harm from unauthorised use or disclosure.

Unless a longer period is required by law, contract, regulatory requirement, or legal claim, our standard retention periods are:

- customer account, platform-user, service-administration, and support data: for the duration of the customer relationship and up to 6 years after the relationship ends;
- business contact and CRM data: for as long as we have an active business relationship or legitimate business reason to retain the data, and up to 3 years after the last meaningful interaction unless you opt out earlier;
- marketing preference and suppression records: for as long as necessary to honour your preferences and demonstrate compliance;

- billing, payment, tax, and accounting records: up to 7 years from the end of the relevant financial year, or longer where required by law;
- contractual records and related correspondence: up to 6 years after termination or expiry of the relevant contract;
- website analytics and cookie-derived data: as set out in our Cookies Policy;
- security logs, access logs, and audit records: generally up to 12 months, unless needed for security investigation, legal compliance, or dispute resolution;
- personal data incidentally encountered during cyber risk assessments: a minimum of 90 days from discovery and then permanently and securely deleted, unless a longer period is required by law, necessary to investigate or evidence a security issue, or otherwise specified in a customer contract;
- aggregated or anonymised data: retained indefinitely where it no longer identifies an individual; and
- data processed in connection with legal claims, complaints, investigations, or regulatory matters: for as long as necessary to resolve the matter and comply with applicable limitation periods.

We periodically review the Personal Information we hold and delete, anonymise, or securely archive it when it is no longer required.

18. How and Where We Store and Transfer Your Personal Information

We primarily store and process Personal Information in the United Kingdom and the European Economic Area (EEA). However, we and our service providers may transfer, store, or access Personal Information in countries outside the UK and EEA where this is necessary to provide, support, secure, or improve our website, platform, and services.

Where Personal Information is transferred outside the UK or EEA to a country that has not been recognised as providing an adequate level of protection, we will put in place appropriate safeguards as required by applicable law. These may include the UK International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses, the European Commission's Standard Contractual Clauses, adequacy regulations or adequacy decisions, transfer risk assessments, and supplementary technical and organisational measures where appropriate.

You may contact us using the details in Section 20 for further information about the safeguards we use for international transfers.

19. Changes to this Privacy Policy

KYND may change this Privacy Policy from time to time by posting a new version on our website. The new version will become effective on the date it is posted, unless stated otherwise. We encourage you to check this page from time to time to ensure that you are satisfied with any changes. Where required by law, we will provide additional notice or seek consent for material changes.

20. How to Contact Us

You may contact us by post or email if you have any questions about this Privacy Policy or the information we hold about you, to exercise any of your rights under data protection law, to exercise your opt-out rights, to withdraw consent, or to make a complaint.

KYND Limited
Unit 3-4, The Grain Store, 70 Weston Street, London SE1 3QH
Email: legal@kynd.io