VERSION 2.7 · IN FORCE FROM 6 NOVEMBER 2026

Privacy notice

What we hold about you, why we hold it, the lawful basis, how long we keep it, who else sees it, and what you can ask us to do about it.

In short

- Kalotect Ltd, trading as Kalotect, decides how the information in this notice is used and answers for it. Write to hello@kalotect.com about anything in it.
- We hold what we need to answer a brief, do the work our clients ask for, keep the record of that work, bill for it, and run a secure website and portal. Each section below says what we hold, why, on what lawful basis, for how long and who else sees it.
- We do not count visits to our website yet. When we do, it will be without anything on your device that identifies you, and one click in the footer of any page will stop it. There are no advertising cookies and no cross-site tracking.
- We often record and transcribe meetings so that nothing said is lost: with a client, only once the client has agreed, in the portal, when signing or at the start of a meeting; until then, any notes of their meetings are kept for us only, and are never planned into work or shared with them. The client can withdraw their agreement in the portal at any time. We tell everyone at the start, and anyone can ask us not to.
- When you sign an agreement in the portal, we keep your signature and initials as you made them, with the IP address and browser your request came from and the time, in our record of your signature and in a certified copy that cannot be changed. The signing's entry in the client's Ledger holds a fingerprint of that record, not your IP address. We keep them as evidence of what was agreed for six years after the end of the financial year in which the client's relationship with us ends, and longer only while a claim made by then is resolved.
- We do the work with people and AI together, mainly Anthropic's Claude, used only on Anthropic's commercial terms or on a consumer plan whose training setting we have checked and recorded as off, within hard budgets and limits, with people deciding. No decision with a legal or similarly significant effect on you is made by a machine alone.
- We contact businesses that may need our services. We email only limited companies and limited liability partnerships, write to or call everyone else, and stop as soon as you ask. An objection goes on a suppression list we never override.
- If you ask us to check a website, we read only what any visitor's browser receives, show version details only to someone who has shown the site is theirs, and delete the request thirty days after you last acted on it or we sent you its report, keeping only the record of anything you order.
- We do not sell personal data. The providers we use handle it on our instructions, except Anthropic when we use Claude on a consumer plan, and where one is outside the UK we rely on the safeguards the law requires.
- You can ask for a copy of your information, for a correction, for deletion or for a limit on what we do with it, and you can object. If you complain to us we acknowledge it within thirty days, and you can also complain to the Information Commissioner's Office.

1. Who we are

Kalotect Ltd, trading as Kalotect, is a design and technology studio for small and medium businesses. It is a company registered in England and Wales with company number 17517329, and its registered office is at Lambourne House, London Road, Riverhead, Sevenoaks TN13 2DE. In this notice it is "we", "us" or "our".

We are the controller of the personal data this notice describes, which means we decide why and how it is used and we are responsible for it. Write to us at hello@kalotect.com, or by post to our registered office, with any question or request about it.

We are not required to appoint a data protection officer and have not done so. Our director, Michelle Wynne, is accountable for how we handle personal data. Our head of delivery, Joe Kaul, looks after it day to day and answers what you send us.

> In plain English: One address covers everything in this notice: hello@kalotect.com.

2. When we act for our clients instead

Much of our work for clients involves personal data that belongs to them: the visitors to the sites we build for them, their customers' bookings and orders, the people on their mailing lists. For that data the client is the controller and we are their processor. We use it only on their written instructions, under the data processing schedule in our agreement with them, and never for our own purposes.

If your information reaches us that way, the client's own privacy notice explains what happens to it, and requests about it should go to the client first. We help them answer.

This notice covers what we decide for ourselves: our own website, the briefs people start on it, our clients and the people who use the portal for them, the meetings we hold, the businesses we contact, our suppliers, and people who apply to work with us.

3. The lawful bases we rely on

The law requires a lawful basis for every use of personal data. We rely on these four under the UK GDPR, and each section below says which applies to what:

- Contract (Article 6(1)(b)): we need the information to make or carry out a contract with you, or to take a step you have asked for before one, such as preparing a proposal.
- Legal obligation (Article 6(1)(c)): the law requires it, for example keeping accounting and tax records.
- Legitimate interests (Article 6(1)(f)): we need it for a purpose of ours, which we name each time, and we have weighed that purpose against your interests and rights. Each section says briefly why we think the balance falls as it does. You can object to anything we do on this basis, as "Your right to object" explains.
- Consent (Article 6(1)(a)): you have agreed. You can withdraw consent at any time, as easily as you gave it, and withdrawing does not affect what we did before.

The law gives some information extra protection, such as information about health, religion or ethnic origin, called special category data. We do not set out to collect it, and we need it for one purpose only in this notice: making adjustments for people who apply to work with us, as that section explains. If it comes up in a meeting we record, we deal with it as "Meetings we record" explains.

4. Visiting our website

When you visit kalotect.com, our hosting provider logs your request. At the date of this version we do not count visits, and no analytics script runs in your browser. When we switch counting on, it will work as described here and in our cookie policy, and the opt-out in the footer of every page will be in place before the first visit is counted.

- What we collect. Our hosting provider logs each request: your IP address, the page asked for, the time, and the browser and device type your browser reports. Once counting is on, and unless you have opted out, we will also record for each page you view the address of the page, the address you came from, your

browser, operating system and type of device, your screen size, your browser's language and time zone settings, and the time; and one short report of how quickly the page loaded, with the page address, the timings, your browser and operating system, whether your device is a mobile one, the size of the window, the type of network connection and how the page was opened. Nothing that recognises you on a later visit will be kept on your device.

- Why. To deliver the site and keep it secure, to find and fix faults, and to learn which pages answer the questions people arrive with and how fast they load for you.
- Lawful basis. Legitimate interests: running a secure, working website and improving it. We think the balance favours this because the logs are kept briefly and only for security and faults, the counts will identify no one, and you will be able to opt out. The law allows us to count visits for statistics without asking first, provided we tell you and give you a simple way to object that costs nothing: one click in the footer of any page, which will stop both the counts and the performance reports.
- How long. Request logs are kept by our hosting provider for no more than thirty days. Visit counts will be kept for no more than twelve months, then deleted or reduced to totals that identify no one.
- Who receives it. Vercel, which hosts the site; and, once counting is on, PostHog, on its EU service. Your browser will send the counts only to our own address, which passes them to PostHog. Before counting starts we will set PostHog to discard the network address a count arrives from, and our server passes the performance reports on under a code that changes every day, never with your address.

> In plain English: We do not use advertising cookies, social media pixels or cross-site tracking. Session recordings and marketing tags never run unless you have said yes to them.

5. Starting a brief

The brief on our start page asks about your business, what is not working, who it is for, your timing and budget, and how to reach you. It saves after every answer, so nothing is lost if you close the page.

- What we collect. Your answers, which can include your business name, what it does, its town or postcode and website, who built your current site, who else decides, and anything else you choose to tell us; your name, email address and, if you give it, a phone number; how you found us; and your confirmation on the last screen that we may contact you about the brief. A cookie on your device holds a random token that links you to your draft, and nothing else.
- People you name. If your brief names someone else, such as a colleague who shares decisions or the freelancer who built your site, we hold their name and role as you gave them, use them only to answer the brief, and contact them only if you ask us to.
- Why. To answer you with a fixed price and a plan, to let you come back and finish, and to work out which of our services fits. If you stop part-way before you have answered "How do we reach you?", you can give us an email address for a link to pick the brief up, and we send it at once. Otherwise, once you have answered that question, we send one link about two hours after you stop. A week after you stop we send one note of what you told us and what we would suggest, but only to an address you gave in answer to that question, never to one you gave only for the link. We send them whether or not you reached the last screen. We send no more than one email about a brief to an address a day, so if the address you give for the link has already had one from us that day, we do not send the link, then or later. Each link works once. It opens a page with a button: pressing it takes you back to the brief, sets the cookie that links that device to your draft, and uses the link up, so nobody can open your answers with a copy of the email. If you open a link that has been used, its page lets you ask for a new one, which we send to the address the brief already has, within the same limit. To stop them, reply to any of these emails or write to hello@kalotect.com, and we send nothing more about the brief.

- Lawful basis. Contract, because preparing a proposal is a step you have asked us to take before one; and legitimate interests, in answering a business that has asked us for a price and helping it finish what it started. We think the balance favours this because we write no more than twice unless you ask us for a link, never more than once a day, only about the brief, and stop when you ask. We do not rely on consent for any of this: the confirmation on the last screen tells you how we will use your details, and it is not consent to marketing. We do not add you to any marketing list because you started a brief.
- Whether you have to give it. Your name and email address are needed to send the brief, because without them we cannot reply. The phone number and the free-text extras are optional; a brief with less in it gets a less exact answer.
- How long. An unfinished brief is deleted thirty days after you last worked on it, together with our copies of the emails we sent you about it, and the cookie lasts no longer. A completed brief that leads to work becomes part of the client's record. If you do not become a client, we delete the completed brief, and our copies of the emails about it, thirty days after our last reply to you about it.
- Who receives it. Our hosting, database, backup and email providers; and Anthropic, whose Claude models help us sort the brief by type of business when our own rules cannot, and help draft the proposal, which a person then checks, edits and sends.

> In plain English: If the budget you choose is below our lowest price, the brief says so straight away and suggests where else to look. That is a rule applied to your own answer, not a judgement about you, and you can write to us if you would like a person to look at it.

6. Checking a website

Anyone can ask us, on kalotect.com/security-check, to check a website: we read what any visitor's browser receives from it, and say what we found and how to put it right. This section covers the person who asks, and the person who runs the site, if that is someone else.

- What we collect. The address of the site, your name, your email address and, if you give it, your company; the time you ticked to say you own the site or may have it checked; whether you ticked to hear from us about website security and our services, with a fingerprint of the exact words of that box; and the version of this notice you were shown. From the site we keep what our check found, as codes and facts, never its pages: the address its home page settled on, the day its certificate runs out, the security settings it sends, and the version numbers and the names of the plugins and themes it shows to visitors. To stop the form being misused, we count requests by your connection's address, your email address and the site, keeping only a code made from each with a key of ours, never the address itself.
- How we check it. Nothing is checked until you confirm your email address from the link we send, and that email carries nothing you typed. We then read only what any visitor's browser receives from the site: its home page and the headers it sends, its certificate, its robots.txt file, the WordPress index and feed if the home page points to them and robots.txt allows them, and its SPF and DMARC records, which we look up through the name servers our hosting provider gives our servers, as we look up any other address. We say who we are when we read it, and our page kalotect.com/security-check/about says what we read and what we never do. We do not log in, and we do not look for anything hidden.
- Version details. We show version details, such as the PHP or WordPress version a site reports, only to someone who has shown the site is theirs: from an email address at the site's own domain, with a record we give them in its DNS, with a file we give them on the site, or through the paid assessment. We read that record or that file only when they ask us to look for it.
- Why. To do the check you asked for and show you its result, with how to put right what it found, and to keep the form from being used to check sites in bulk. The findings are shown on our website, on the device where you confirm the check, never in an email.

- Lawful basis. Legitimate interests: answering a request you made, and keeping the check for the people it is for. We think the balance favours this because we read only what any visitor's browser receives, keep it only as long as the request, and count requests only to stop misuse.
- If you run a site someone else asked us to check. We hold its address and what it showed to visitors for as long as we keep that request, and show its version details to nobody who has not shown the site is theirs. We rely on legitimate interests in answering the person who asked. We think the balance favours this because we read only what any visitor's browser receives, we limit how often any site is checked, our check says who it is when it reads, and we stop checking a site for good when its owner asks. Telling every site's owner each time would take an effort out of proportion to that, so this notice and our page kalotect.com/security-check/about are how we tell you. Write to hello@kalotect.com and we stop checking your site for good.
- Emails. If you ticked the box, we send you at most three emails in all about website security and our services after the check, on the basis of your consent, which you can withdraw in one click from any of them. If you did not tick it, we send you only the email to confirm the check, and those about anything you order.
- Whether you have to give it. The site's address, your name and your email address are needed: without them we cannot check the site or send you the link. Your company is optional.
- How long. If you do not confirm, we delete the request after two days. Otherwise we delete the request and its result thirty days after the last time you confirmed it, showed us the site is yours, ordered or paid for an assessment or asked for its re-check, or we emailed you its report. Our copies of the emails we sent you about it go with it, unless another request of yours is still kept. A count against misuse covers a month at most, and is deleted after that, the next time we start a new count.
- Who receives it. Our hosting, database, backup and email providers.

7. Buying a website assessment

If our check saw a WordPress site, you can buy an assessment of it: with administrator access you give us, we read what is installed on the site and check it against a database of known vulnerabilities. Our website assessment terms at kalotect.com/terms/website-assessment are the contract.

- During our launch. While card payments are not open, an assessment costs nothing: we take no payment, Stripe receives nothing about your order, and what this section says about paying, refunds, Stripe and the record of the sale applies only to an order you pay for. We keep the record of a free order (your two ticks, the day you ordered and the version of our terms) for as long as the record of a sale, as our record of the access you authorised, on the basis of legitimate interests: being able to show what you asked us to do; one we close, because you did not give us access, we could not send its report or you asked us to cancel it, is deleted whole thirty days after we close it. Until our vulnerability database is connected, we send nothing to WPScan, and the report says it could not check plugins, themes and WordPress itself against known advisories. A free order's report has no plain-English summary, and we send no reminder of its re-check.
- What we collect. Your two ticks on our order page, with their times: that you may give us administrator access to the site and buy the assessment for it, and that you ask us to start as soon as you have paid; whether you ticked to refuse follow-up emails about the assessment; the price, any VAT and the version of our terms; from Stripe, the payment's references, the amount and that it was paid, never your card details; any PHP or WordPress version you tell us; and, from the site, the versions of WordPress, its plugins and its themes, whether each is switched on, three of its settings (its address, and whether pingbacks and comments are open by default) and the counts of its pages, posts and administrators. We also read the content of up to five of its pages to count what they hold, such as forms and media, and keep only those counts, never the words. We never ask for or keep the names or email addresses of the

site's users.

- Giving us access. You give us access with an Application Password for a temporary administrator user you make for us. We use it for less than a minute, while our access page checks it, and only at the address your free check read: to check that it works, and to read what is installed, three of its settings, the counts of its pages, posts and administrators, and the content of up to five of its pages. We never write it, or the user's name, to our database, our logs or our backups. Delete the user, or its password, when we have sent the report.
- The report. We email you the report as a PDF, usually within the hour of your giving us access. We keep a copy of that email without the findings, which are only in the attachment, whose name alone we keep, and without the link to your re-check. We may later add a short plain-English summary, drafted by an AI model and signed by a person in the studio, as "How we use AI, and decisions about you" says, and we email you the report again when we do. One re-check, with access given again, is included for thirty days after the report is sent.
- Why. To carry out the assessment you ordered, send you its report, refund you when our terms say we do, and keep the record of the sale.
- Lawful basis. Contract, for the assessment and the emails it needs: your receipt, the report, the summary if one is added, and a refund. Legal obligation, for the record of the sale, which the law requires us to keep in our accounts.
- Emails about the assessment. As our customer, you may also get an email reminding you of your re-check, unless you ticked the box on our order page to refuse such emails, and it has a one-click unsubscribe. Lawful basis: legitimate interests, in telling our customers about the re-check they bought. We think the balance favours this because it is about what you bought, you can refuse it when you order and in one click from the email, and no address gets more than three follow-up emails from us about website checks and assessments in all. To send it by email, we rely on the rule that lets a business email its own customers about its similar services, with the chance to refuse each time.
- Whether you have to give it. The two ticks and the access are needed: without them we cannot sell or carry out the assessment. A version you tell us is optional.
- How long. We clear the findings, the list of what is installed and the report from our records thirty days after we send the report or after we refund you, and after that we cannot send the report again. If we cannot send you the report within thirty days of your payment, we refund you in full. We keep the record of the sale (the amount, any VAT, the day you paid, your two ticks, the version of our terms and Stripe's references) for seven years from the day you paid, because the law requires us to keep accounts, and then delete it. An order you do not pay for is deleted whole thirty days after its payment page closes. Stripe keeps its own record of the payment.
- Who receives it. Our hosting, database, backup and email providers; Stripe, which takes the payment; Anthropic, which receives for the summary only the findings' references, kinds, states and severities, their CVE numbers and the versions that fix them, never the site's address, your name or your email address; and WPScan, the database of known vulnerabilities we check against, which receives only the version of WordPress and the names of the plugins and themes installed, which are not personal data.

8. Clients and the people who use the portal

When a business becomes our client, we give the people it names an account in the client portal at portal.kalotect.com. This section covers the client itself, where the client is a sole trader or a partnership, and every person who uses the portal for a client. If your employer invited you, we received your name, work email address and role from them, and we tell you this when we invite you, with a link to this notice.

- What we collect. Your name, work email address and role; what you tell us when you first sign in, such as the name you prefer, your job title and a mobile number; the passkeys you register, of which we hold only

the public part, so your fingerprint, face or device PIN never leaves your device; a record of each sign-in, with the time, your IP address and your browser; your notification choices; and what you do in the portal: approvals, answers to our questions, comments, tickets, change requests, the files you add and the documents you sign.

- Signing. When you sign an agreement in the portal, we keep the record that "Signing an agreement in the portal" describes.
- Billing. The business's name and address, its invoices and payments, and the status of its Direct Debit mandate. Stripe collects card and bank details on its own pages; we never see or store a full card or account number.
- Why. To provide the services in the client's agreement and the portal they run through; to act on approvals and answers, which are binding instructions; to keep the client's Ledger; to bill and collect payment; to send the emails the service needs, such as sign-in links, approvals waiting, trial reminders and invoices; and to keep accounts secure.
- Lawful basis. Contract, where you are our client yourself. Legitimate interests, where you use the portal for a client business: we need to know who approves and decides for the business we work for, and to keep a reliable record of it; we think the balance favours this because the client chose you to act for it, you act in your work role, and we hold only what that needs. Legal obligation, for accounting and tax records. Legitimate interests, for keeping accounts secure and for keeping the Ledger as evidence of what was asked, agreed and done, which protects the client and its people as much as us.
- Whether you have to give it. Your name and work email address are needed for an account; without them we cannot give you access or record your approvals.
- How long. An account lasts as long as the client's agreement with us, and we remove a person's access as soon as the client asks. Sign-in records are kept for twelve months. When the agreement ends, the client can export its data for 90 days, and we then delete it, except the Ledger, the signed agreement and the billing records. We keep those for six years after the end of the financial year in which the relationship ended, because tax law requires the accounting records and because they are the evidence either side would need for a claim, and then delete them, except that if a claim has been made by then, we keep what it needs until it is resolved.
- Who receives it. Our hosting, database, backup, file storage and email providers; Stripe, for payments; Starling, our bank, for money received; Anthropic, whose Claude models and Claude Code sessions do work for the client under a person's control; GitHub and Vercel, where we work on the client's code and deploy previews; our accountant; and the client business itself, whose admins can see what its people have done in the portal.

The Ledger. We record every action we take for a client in its Ledger: what was done, by whom, why and with what evidence. Entries name the people involved, including the client's people when they approve or answer something, and ours. When a person is invited to the portal, accepts, or has their role changed or their access removed, the entry also records their work email address; when they change the address they sign in with, the entries record the new address, and the old one once the change is made; and when they sign a device out of the portal, the entry names it in a few words, such as "Safari on iPhone". Everyone the client gives access to the portal can read these entries. When one of our people works in a client's portal for them, which is possible only for a stated reason and for an hour at most, the Ledger records who, why and until when. While we keep the Ledger, its entries are never edited or deleted, because the chain that links them is what proves the record has not been altered; a mistake is put right by a new entry that corrects it. When the retention period above ends, we delete the Ledger with the rest of the client's records. Entries about our own running, such as our costs, are not shown to the client.

> In plain English: The client's admins can see in the Ledger who approved or answered what, and when. That is its purpose: it is the shared record of the work.

9. Signing an agreement in the portal

When you sign an agreement with us in the portal, for yourself or for a business, we keep a record that shows who signed, that they meant to, what they signed and when. Our terms of business, under "Signing electronically", say the same from the agreement's side.

- What we collect. Your name, your role and the email address of the account you signed in with; your signature and your initials exactly as you made them, whether typed, drawn or uploaded as a picture; which sections you initialled, with the time your browser gave for each and the time we received it; that you ticked to confirm you have read the documents and have authority to sign; how you had signed in, by passkey or by email link, and when you last confirmed it was you; the IP address your request reached us from; the description your browser gives of itself, such as its name, version and operating system, up to its first 300 characters; the time you signed, by our server's clock; and the SHA-256 fingerprint of the exact text you signed. Before you sign, the portal shows you the IP address we will record. An agreement signed before we began recording the address itself holds a one-way hash of it instead, which can still be matched to the address.
- Where we keep it. In our database: in our record of your signature, which is kept with the agreement, and in a certified copy of the agreement, a PDF of the documents exactly as signed, with every signature and initial and a certificate of what we recorded, which we keep unchanged. The certified copy is also filed with the client's documents in the portal, and we email it to you, and to our own team, when you sign. We record the signing in the client's Ledger too: who signed and their role, how they signed in and when they last confirmed that it was them, how the signature and initials were made, with the SHA-256 fingerprint of each that was drawn or uploaded, the sections initialled, whether the separate box agreeing that we may record our meetings was ticked, the date and time, and the SHA-256 fingerprints of the text signed, of the certified copy and of our record of your signature. The signing's entry does not hold your IP address, your browser's description of itself, your email address, or your signature or initials as you made them: of our record of your signature, it holds only the record's reference and fingerprint, which would change if anything in the record changed. Those are kept in our database and in the certified copy.
- Why, and the lawful basis. To be able to prove the agreement: who made it, that they meant to, and exactly what they agreed and when. Contract, where you sign for yourself as our client. Legitimate interests, where you sign for a business: we need to be able to prove who made the agreement for it and on what terms, if either side ever questions it. We think the balance favours this because you sign in your work role, you are told before you sign what we record, and we use the record for nothing else.
- How long. We keep our record of your signature, with the IP address and your browser's description of itself in it, and the certified copy, for as long as we keep the signed agreement, as "Clients and the people who use the portal" describes: six years after the end of the financial year in which the client's relationship with us ends, and, if a claim has been made by then, until it is resolved. When that time is over, we delete them, with the client's Ledger, which holds the signing's entry and the fingerprint of our record. The platform refuses to delete a certified copy at any other time, so deleting one is a deliberate step we take when its period ends.
- Your rights over it. The certified copy cannot be changed or deleted in that time, and nor can the Ledger entry that records it, because they are the evidence of the agreement. If you ask us to delete or change either, we explain that this is why, as the law allows where information is needed to establish, exercise or defend a legal claim, and we use it for nothing else. If something in it is wrong, we record a correction in the client's Ledger beside it. You can object, as "Your right to object" explains, and we consider your objection against our need to be able to prove the agreement.
- Who receives it. Our hosting, database, backup, file storage and email providers; the client business, whose people who use the portal can see who signed and when, see your signature as you made it on the agreement in the portal, with the IP address, read the signing's entry in the client's Ledger, and read and download the certified copy, which shows the IP address; and, if the agreement is ever disputed, our

lawyers and a court.

- Whether you have to give it. To sign in the portal you need to give your name and role, make your signature, initial the key sections and tick the confirmation; without them the agreement cannot be signed there.

> In plain English: We keep your signature as we would a signed paper contract: unchanged, for as long as it may be needed as evidence of what was agreed, and for nothing else.

10. Meetings we record

We often record and transcribe our meetings with clients, and with businesses thinking of becoming clients, using a Plaud recording device and its app, so that nothing said is lost.

- How you know. With a client, we record a meeting only once the client has agreed that we may. The client can agree in the portal, by answering the one-click question we put to them there; when they sign the engagement schedule, by ticking its separate, optional box; or by telling us at the start of a meeting, which the person from our studio who asked records on the client's record. Until the client has agreed, any notes of their meetings are kept for us only, and are never planned into work or shared with them. The client can withdraw their agreement in the portal at any time. We say at the start of each meeting that we are recording, and anyone can ask us not to, in which case we take written notes instead. Anyone who joins later is told when they join. We also ask everyone not to mention health or other sensitive details about anyone who could be identified, and to ask us to pause the recording if they need to.
- What we collect. The recording; a transcript of it; a summary with the decisions and actions; the names of the people present and, where we have them, their email addresses; and the plan of work we draw from the meeting.
- Our client's people and customers. Where a meeting names or discusses people whose personal data we hold for the client, such as its customers, patients or staff, that part is the client's personal data, which we process for the client as its processor under the data processing schedule, not as this notice describes. We remove those details from the transcript and notes we keep, and until we have, that part is returned or deleted with the rest of the client's personal data.
- Sensitive details. If health or other special category details are recorded anyway, Plaud will have recorded and transcribed them. A person at the studio checks each transcript, and the notes with it, for such details and removes them from both before either is used to plan work or goes to a Claude model to be planned, and before anything of the meeting reaches the portal; and they go from Plaud when the audio is deleted.
- Why. To keep an accurate record, to plan and assign the work the meeting agreed, and to show you the summary and actions so that you can correct them.
- Lawful basis. Legitimate interests: keeping an accurate record of what was discussed and agreed, and planning the work from it. We think the balance favours this because you are told at the start and can decline, the meeting is about business, a person checks the notes before they are used, and you can see and correct the summary. Where you are our client yourself, also contract. What is said in a meeting becomes an instruction only once it is confirmed in the portal.
- How long. The audio recording is deleted from Plaud within thirty days, once the transcript has been filed and checked. The transcript, summary and actions are filed to the client's record and kept for as long as that record is kept. Notes of a meeting with a business that does not become a client are deleted twelve months after the meeting.
- Who receives it. Our hosting, database and backup providers, which keep what we record; Plaud, which records, transcribes and summarises; Zapier, which passes the transcript and summary of each new recording from Plaud to our platform; Anthropic, whose Claude models, in a Claude Code session, collect

new recordings when we ask them to and, once a person at the studio has checked a meeting's notes for sensitive details, read them with the names of our clients to suggest whose meeting it was, and draft the summary and plan; and the client, who sees the summary and actions in the portal, with the work and questions the plan makes for them, once a person at the studio has checked that the meeting is theirs and released it. A person confirms which client a meeting is filed to, and can correct it. The full transcript is for our use and is not shown in the portal, but you can ask us for a copy.

> In plain English: A person at the studio checks each meeting's notes for sensitive details before they are used, and nothing of a meeting reaches the portal until a person releases it. If a summary gets something wrong, tell us and we add a correction.

11. Businesses we contact first

We look for businesses that may need our services and contact them. If you run one, or work for one, we may hold information about you that we did not get from you. This section says what, where it came from, and what you can do about it.

- Where we got it. The Companies House register; public business listings, such as Google's; your business's own website; public professional profiles, such as LinkedIn; a person who recommended you to us; and our own notes if we have spoken or met.
- What we hold. Your business's name, legal form, company number, address and website, and public facts about it from those sources, such as its industry codes and how its website is built and performs; the names and roles of its directors or of the person we want to reach; business contact details, such as a work email address, phone number, postal address or professional profile; and, if a letter we sent carries a code to a page we made for your business, whether and when that page was opened.
- Why. To judge whether our services could help your business, to contact you about them, and to decide whether to follow up. We score how closely a business matches the kind of client we are looking for in an area, and a person reviews every first approach before it is sent.
- How we contact you. We send unsolicited email only to limited companies and limited liability partnerships, and a message on LinkedIn follows the same rule. A sole trader or a partnership gets a letter, a call or a visit instead, and so does any business whose legal form we cannot confirm. We do not call a number registered with the Telephone Preference Service or the Corporate Telephone Preference Service unless you have told us we may. We contact you no more than three times, two weeks apart, and stop as soon as you reply. The page a letter links to sets no cookie.
- Lawful basis. Legitimate interests: offering our services to businesses that may need them. We have weighed that against your interests: we use only business information, contact you in your business capacity, and stop when you ask.
- When we tell you. Our first message to you links to this notice, and we tell you within a month of getting your details at the latest.
- How long. If we do not contact you within one month of finding your details, we delete them. If we contact you and you do not reply, or tell us you are not interested, we delete your details twelve months after our last contact. In both cases we keep only the entry that holds you on our suppression list, if you are on it.
- Who receives it. Our hosting, database and backup providers, which keep what we record; Stannp, which prints and posts our letters; the provider of our outreach mailbox, which sends and receives our email; and Anthropic, whose Claude models help us classify a business's legal form, judge fit and draft the first approach.

> In plain English: Ask us to stop and we stop. The next section explains how.

12. Your right to object

You can object at any time to our using your information for direct marketing, including the scoring we do to decide whom to contact. When you do, we stop, and we do not ask you why.

You can also object to anything else we do on the basis of legitimate interests, on grounds relating to your particular situation. We then stop, unless we have compelling legitimate grounds that override your interests, rights and freedoms, or we need the information to establish, exercise or defend a legal claim.

To object, reply to any message from us, use the unsubscribe link in any marketing email, or write to hello@kalotect.com. We act on an unsubscribe within the hour.

We then add your email address, website domain, company number or postcode to our suppression list, which we check before every message we send and never override. We keep that entry permanently, holding only what we need to recognise you, so that you are not contacted again.

Every follow-up email we send after a website check or a website assessment has an unsubscribe link, and carries what your email program needs to offer its own unsubscribe button. Either stops them at once. We keep your address on our list of people not to send them to, so that you never get another, and that list is kept after everything else about you is deleted. We keep it on the basis of legitimate interests: honouring your objection, which needs only your address.

> In plain English: Saying no once is enough, and it lasts unless you tell us otherwise.

13. Suppliers and freelancers

- What we collect. The names, roles and contact details of the people we deal with; the contract, invoices, payments and bank details; and, for freelancers working on client projects, the access we give them and the work they do, which is recorded in the client's Ledger as ours is.
- Why. To buy from you, pay you, manage the work and keep our accounts.
- Lawful basis. Contract, where you are the supplier yourself; legitimate interests, where you work for a supplier business; legal obligation, for accounting and tax records.
- How long. For as long as you supply us, then six years after the end of the financial year in which you last did, for tax and accounting.
- Who receives it. Our hosting, database and backup providers, which keep what we record; our bank, our accountant and our accounting software; and, where you work on a client's project, that client, through its Ledger.

14. People who apply to work with us

If you apply to work with us, as an employee or a freelancer, we hold your application and CV, our notes from any interview, and any references you agree we may take. We use them to decide whether to offer you work, which is a step you ask us to take before a contract, and in our legitimate interest in recruiting fairly and well, which we think you share because it is the process you asked to join.

If you tell us about a disability, or anything else we need to know to make the process fair, we use it only to make adjustments, because the Equality Act 2010 requires us to. That is information about your health, which the law protects more closely. We rely on our legal obligation (Article 6(1)(c)) and on the condition for obligations under employment law (Article 9(2)(b) of the UK GDPR, with paragraph 1 of Schedule 1 to the Data Protection Act 2018). We keep it apart from your application, only the people arranging the adjustment see it, and we delete it with your application.

If we offer you a job, we check your right to work in the UK, as the law requires. No decision about an application is made by AI.

If you are not offered work, we delete your application six months after we tell you, unless you agree that we may keep it for future roles. If you join us, we give you a separate notice for the people who work for us.

15. How we use AI, and decisions about you

We work with people and AI together. We use AI models, mainly Anthropic's Claude, including Claude Code sessions, to draft, build, check and summarise: for example to sort a brief by type of business, draft a proposal, match meeting notes to the right client and plan the work, classify a business's legal form, and write and test code, which can mean opening pull requests on a client's code and deploying previews to Vercel. We may later ask models from OpenAI or Google for a second opinion on our own work; we do not do so yet.

We use Claude, including Claude Code, only through accounts held by Kalotect Ltd or by our people, of two kinds. The first is on Anthropic's commercial terms and its data processing addendum, through its API or a Team or Enterprise plan; under those terms Anthropic does not train its models on what we send. The second is a Pro or Max plan, on Anthropic's consumer terms, which has a setting that lets Anthropic use what we send to improve its models: before any client work is sent to such an account, we check that the setting is off and record the check, and our platform refuses to send client work to a consumer account without that record. On the first kind Anthropic processes what we send on our instructions; on the second it handles it under its consumer terms and its own privacy policy. We use our other AI providers under terms and settings that likewise stop them using the personal data we send them to train their models.

Every AI task runs within a hard budget and limited permissions, and is given only the client information its task needs: a Claude Code session is given only the code repositories of the client its work is for. Anything a model produces is checked against a defined format before it touches data, files or systems, and our platform refuses to record a task's results against any client other than the one it was for. A person approves anything that carries a client's name before it is published or sent, and every change before it reaches a client's live site. AI cannot approve anything or move money.

We do not make decisions about you that have legal or similarly significant effects solely by automated means. People decide what we propose, what we charge, whom we work with and whom we employ. Three things are settled by rules or models without a person looking at each case, and none has a significant effect on you: whether we may email a business or must write to it instead, which falls to a letter whenever we are unsure; the scores that put the businesses we might contact in order; and the message a brief shows when the budget chosen is below our lowest price. If you think an automated step has treated you unfairly, write to us and a person will look at it.

Where the law or a platform requires it, we disclose AI involvement in what we publish, and we do not deliver to a client an image or video we have made, or changed with AI, until it carries signed Content Credentials: a C2PA manifest, signed by us and kept with the file, inside it or alongside it. Our AI disclosure at kalotect.com/ai-disclosure sets out the detail.

If you order a website assessment, a Claude model may draft a short plain-English summary of its findings. It is given only the findings' references, kinds, states and severities, their CVE numbers and the versions that fix them, never the site's address, your name or your email address. A person in the studio checks and signs every summary before it is added to your report, and the report says so. The findings themselves are produced by our code. Whether a check shows version details, how many checks we take, and a refund after three failed tries at access are settled by rules in our code, and none has a legal or similarly significant effect on you.

16. Who receives personal data

We share personal data only as this notice describes. We do not sell it, and we do not share it for anyone else's marketing.

These providers process it for us, on our instructions, under written terms that oblige them to protect it and stop them using it for their own purposes:

- Hosting and database: Vercel, for the website and portal, and Neon, for the database, in its London region.
- Files: our database.
- Backups: Cloudflare, which keeps our nightly backups in the European Union, sealed with our own key so that Cloudflare cannot read them; and GitHub, whose jobs take each backup and, once a month, restore one to check it, holding the data only while each job runs, in the United States.
- Email and documents: Google, for our company email, calendar and documents (Google Workspace), where what you write to us arrives; Resend, for the emails our platform sends; and the provider of our outreach mailbox.
- Payments: Stripe, for cards, Direct Debit, invoices and the payment for a website assessment.
- Analytics and errors: PostHog, on its EU service, once we count visits; and Sentry, which receives reports of errors on our servers: the error, where it happened, and the account or client it concerned.
- AI: Anthropic, for Claude and Claude Code, under its commercial terms, or, on a Pro or Max plan, under its consumer terms and its own privacy policy rather than on our instructions, as "How we use AI, and decisions about you" describes; OpenAI and Google, if we come to ask them for a second opinion, which we do not do yet; and ElevenLabs and our image and video providers, when we make narration, images or video for a client. Those last receive no personal data unless the client has approved, in the portal or in writing, a person's likeness or voice for that use with that provider, and Seedream and Kling never receive one.
- Code and deployment: GitHub and Vercel, where we work on a client's code and deploy previews.
- Meetings: Plaud, which records, transcribes and summarises, and Zapier, which passes the transcript and summary of each recording from Plaud to our platform.
- Letters: Stannp, which prints and posts them.

These receive it as controllers in their own right, under their own privacy notices:

- Stripe, for its own fraud prevention and its legal duties as a payment provider, and Starling Bank, our bank;
- Google, for YouTube, and Vimeo, when you press play on a video of theirs in the portal and not before: your IP address, what your browser says about itself, the address of our portal (never of the page you are on), and what their player stores on your device, for their own purposes as well as to play the video;
- our accountant, lawyers, insurers and other professional advisers;
- HMRC, regulators, the police or a court, where the law requires us to share it; and
- a buyer of our business or its assets, and their advisers under a duty of confidence, if we sell it, in which case this notice continues to apply to your information.

This notice lists the providers we use for our own purposes. The data processing schedule in our agreement with each client lists the providers that handle that client's personal data for us, and we send either list to anyone who asks.

17. Transfers outside the UK

Our database and the servers that run our website and portal are in London, and our hosting provider's network serves pages from around the world. Some of our providers are based outside the UK, or reach data from outside it, among them Vercel, Neon, Cloudflare, Stripe, Resend, Sentry, GitHub, Google, Anthropic, OpenAI, Plaud, Zapier, ElevenLabs and our image and video providers. PostHog processes our analytics in the European Union, and our backups are kept there.

Where personal data goes outside the UK, we rely on the UK's adequacy regulations, which cover the European Economic Area and US organisations certified under the UK Extension to the EU-US Data Privacy Framework, or otherwise on the International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses in our contract with the provider. We send no personal data to a provider in a country without UK adequacy unless one of those safeguards is in place and we have assessed the risk of the transfer. Write to hello@kalotect.com for a copy of the safeguards that apply to any provider.

18. How long we keep it

Each section above says how long we keep that information. In addition:

- copies of our database in our database provider's recovery history expire as that history rolls on, within ninety days at most, and our own nightly backups are deleted within ninety days of being taken, so information we delete is gone from both within that time; if we ever restore one, we delete again anything that was deleted after it was taken;
- when a client's agreement ends, its data stays available to export for 90 days and is then deleted, except the records described under "Clients and the people who use the portal";
- where we keep a record because the law requires it, or for a possible legal claim, we use it for nothing else; and
- when a period ends, we delete the information or reduce it to totals that identify no one.

19. Keeping it safe

We protect personal data with measures suited to the risk. Among them: sign-in by passkey or by a single-use email link, with a fresh check before billing and settings; sessions stored on our side only as a one-way hash; each client's data kept apart from every other client's; the keys to accounts we connect for clients stored encrypted; our own people's access limited to what their work needs, and recorded; and a Ledger whose entries are chained, so that any alteration would show.

No system is completely secure. If a breach of security puts personal data at risk, we handle it under our breach process and tell the Information Commissioner's Office, and you, where the law requires.

20. Your rights

You have these rights over your personal data:

- to be told what we hold and to have a copy of it;
- to have it corrected if it is wrong or incomplete;
- to have it deleted;
- to have us limit what we do with it while a question about it is settled;
- to have it in a portable form, where we hold it on the basis of contract or consent;
- to object, as "Your right to object" explains;
- to withdraw consent, where we rely on it; and

- where a decision with legal or similarly significant effects on you is made solely by automated means, to be told about it, to give your view, to have a person reconsider it and to challenge it. We make no such decisions, as "How we use AI, and decisions about you" explains.

Some rights depend on the lawful basis, and some have exceptions. For example, we cannot delete records the law requires us to keep, or Ledger entries and the certified copy of a signed agreement, which we need as evidence for a legal claim, though we stop using them for anything else. "Signing an agreement in the portal" explains how long we keep the certified copy.

To use any of these rights, write to hello@kalotect.com or to our registered office. We may ask you to confirm who you are, in proportion to what you ask for. We answer within one month, free of charge. If a request is complex, or one of several, we can take up to two months more, and if we need to we tell you so within the first month.

> In plain English: Clients do not need to ask: a client's admins can read the Ledger and the client's documents in the portal at any time, and request an export of the Ledger there.

21. Complaints

If you are unhappy with how we have handled your information, please tell us first, at hello@kalotect.com or by post to our registered office, saying what went wrong and what you would like us to do. However a complaint reaches us, we treat it as one.

We acknowledge your complaint within thirty days of receiving it, look into it, keep you told what we are doing, and give you our answer without undue delay.

You also have the right to complain to the Information Commissioner's Office, the UK regulator for data protection, at ico.org.uk or on 0303 123 1113. The ICO will normally expect you to have complained to us first and to have given us the chance to put things right.

22. Cookies

Our website, the portal and our staff console set only a few cookies, and none that follows you to other sites. For example, one remembers whether you chose the light or the dark theme, one links you to a brief you started, others keep you signed in to the portal or the console, and one saves us offering you a passkey more than once. None of them needs consent, for the reasons our cookie policy gives for each. The one thing in the portal that does is a video from YouTube or Vimeo: its player loads only when you press play, and we tell you before you do that it sets cookies of its own. Once we count visits, the counting itself will use no cookie, but if you opt out we remember that in a cookie, so that we keep honouring it.

If we ever ask your consent for anything else, such as session recordings, nothing runs until you have said yes, and saying no is as easy as saying yes. Our cookie policy at kalotect.com/cookies is the full list: every cookie and similar item, what it does, how long it lasts and how to turn it off.

23. Children

Our website and services are for businesses and the people who run and work in them. They are not directed at children, and we do not knowingly collect personal data about children, other than where it appears in material a client gives us, which we handle as that client's processor. If you think a child has given us their information, tell us and we will delete it.

24. Changes to this notice

The version of this notice and the date it took effect are shown at the top. When we change it, we publish the new version here with its date and keep the earlier versions, which we send to anyone who asks.

If a change affects how we use information we already hold, we tell clients in the portal and by email before it takes effect. We do not start using your information for a new purpose without telling you first.