

Privacy Policy

TIMELINE

Privacy Policy

Contents

Introduction	2
Who we are	2
Our contact details	2
What this notice covers	2
Who this notice applies to	3
Our role and your relationship with us	4
What personal data we collect	5
Where we get your personal data from	8
How we use your personal data and our lawful bases	8
Recording and monitoring communications	10
Marketing	11
Artificial intelligence	11
Automated decision-making and profiling	12
Who we share your personal data with	12
International transfers	13
Cookies and similar technologies	13
How we keep your personal data secure	13
How long we keep your personal data	13
Your rights	14
Changes to this notice	15

Introduction

This notice explains how we use and protect your personal data, and the rights you have. Personal data is any information that identifies you directly or indirectly. We process it in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) and ICO guidance. Together we call these "Data Protection Laws".

Who we are

"Timeline", "we", "us" and "our" means Timeline Holdings Limited (company no. 13266210; ICO no. ZB274330) and its subsidiaries, including:

- **Timelineapp Tech Limited** (company no. 11405676; ICO no. ZA447269): provides Timeline Planning. Not regulated by the Financial Conduct Authority.
- **Timeline Portfolios Limited** (company no. 11557205; ICO no. ZA572675): provides Timeline Investing and Platform services. Authorised and regulated by the Financial Conduct Authority (FRN 840807).

These services are described in "What this notice covers" below. All three companies are registered with the Information Commissioner's Office. You can verify this at ico.org.uk. The company responsible for your personal data (the "controller") depends on the service you use (see "Our role and your relationship with us").

Our contact details

If you have any questions about this notice or our processing, or wish to exercise your rights, please contact:

Data Protection Officer

Timeline, 70 Gracechurch Street, London, EC3V 0HR, United Kingdom

Phone: 020 4572 9919

Email: support@timeline.co

Need this notice in another format? If you would like this notice in large print or another format, contact us and we will be happy to help.

What this notice covers

This single group notice covers personal data we process across our services. These are:

- **Our websites:** all sites and services operated under our timeline.co and adviser3point0.co domains (including subdomains), and any other domains we operate that link to this notice.
- **Timeline Planning:** our planning software, tools and apps used by advice firms. This includes fact find, risk profiling, cashflow modelling, portfolio analytics, IHT Planner, Digital Letters of Authority and reporting.
- **Pennee:** our AI assistant, part of Timeline Planning, which works across our ecosystem to help advice firms with tasks such as preparing meetings, drafting reports and building financial plans (see 'Artificial intelligence').

- **Timeline Meeting Notes:** our standalone app that records, transcribes and summarises meetings (see 'Artificial intelligence').
- **Timeline Investing:** our Model Portfolio Service and multi-asset fund range.
- **The Timeline Platform:** account administration, digital onboarding (including KYC and AML checks), order handling and custody (delivered through our partner Seccl), transfers, secure messaging and the client portal.
- **Our events and communities:** including Adviser 3.0, webinars, podcasts and newsletters.
- **Our business operations:** marketing, supplier management and recruitment.

Who this notice applies to

This notice applies to everyone we may process personal data about. Throughout this notice we refer to the following groups:

- **Advisers and firm staff:** financial advisers, paraplanners, administrators, directors and other staff. This covers advice firms and other businesses that use, trial or enquire about our services.
- **Clients:** anyone who invests through our investment or platform services. This can be **directly**, where you have an account or agreement with us (for example on the Timeline Platform). Or it can be **indirectly**, where you have no agreement with us and your relationship is through your adviser. See "Our role and your relationship with us" for what this means for your data.
- **Technology users:** anyone with login access to our technology. This includes adviser firm staff, clients and other permitted users.
- **Connected people:** individuals connected to a client or firm. This includes dependants, beneficiaries, trustees, settlors, attorneys, directors and shareholders, whose details appear in a financial plan, application or account.
- **Website visitors and marketing contacts:** anyone who visits our websites, submits a form, contacts us about our services, subscribes to our newsletters, or receives our marketing. This applies whether or not they ever become a customer.
- **Event, webinar and podcast participants:** attendees, registrants, speakers, partners and sponsors at our events, including Adviser 3.0.
- **Suppliers and business contacts:** staff at our suppliers, professional advisers, custodians, fund managers and other business partners.
- **Job applicants and enquirers:** anyone who contacts us about working with us or applies for a role. This notice covers you until you join us, when our separate employee privacy notice applies.

Our role and your relationship with us

Our data protection role varies based on our services:

Relationship	Our role	What this means for you
You are an adviser or work at an advice firm using, trialling or enquiring about our services	Controller (for our relationship with you, onboarding, billing, support, training and marketing)	Contact us directly about your data.
You visit our websites, attend our events, receive our marketing or contact us directly	Controller	We decide how and why your data is used. Contact us directly.
Your advice firm uses Timeline Planning (including the fact find, cashflow modelling and Pennee) and enters your information as their client	Processor for your advice firm (the controller)	Your advice firm decides how your data is used. Direct any requests to your adviser first. We will support them.
You invest in our Model Portfolio Service or multi-asset funds through your adviser or a third-party platform, or directly with us.	Controller for the data we receive to run the portfolios and provide our services, and to meet our legal obligations (e.g. AML checks and FCA record-keeping)	Your adviser or platform remains your main contact. If you invest indirectly, we may only hold limited information about you. If you have an agreement with us, contact us directly.
You hold investments directly on the Timeline Platform	Controller for our digital platform service and legal obligations (e.g. AML checks and record keeping). For order handling and custody, Seccl acts as a separate controller and decides how it uses your data for those activities.	Seccl handles custody, execution and related reporting. Its privacy notice applies alongside ours. Contact your adviser first, or us directly.
You are a connected person (e.g. a dependant, beneficiary, trustee or attorney) named in a plan, application or account	Same role as for the client concerned (processor or controller as above)	Where we are the controller, we will tell you we hold your data within one month of receiving it, or when we first contact you, unless an exemption applies. Where your advice firm is the controller, it is responsible for telling you. Contact us or the advice firm.

A controller decides what happens to your data. A processor follows the controller's instructions. Where we act as processor, our contract with your advice firm sets out these instructions. Even where we act as processor, we remain the controller of account, login, security and usage data. We use that data to run and secure our technology, to provide support, and to improve and develop our products and services. We decide how it is used for those purposes. Their privacy notice applies alongside ours.

What personal data we collect

What we collect depends on who you are and which services you use. The groups below can overlap, for example an adviser is also a technology user.

Advisers and firm staff

- **Identity:** name, job title, role and work contact details, and your firm's details, including FCA registration information
- **AML and screening:** information gathered during onboarding and due diligence on you and your firm, including identity checks on directors and beneficial owners, copies of identity documents such as passports, and electronic checks which may include credit reference agency, politically exposed person ("PEP"), sanctions and adverse media screening
- **Financial:** billing and payment details
- **Service data:** how you use our services, including support queries, training records, feedback, survey responses, and testimonials and case studies you take part in.
- **Communication records:** (see "Anyone who communicates with us")
- Where you use Timeline Meeting Notes:
 - **Calendar:** event details including event title, time, participant emails, where connected to Google or Outlook
 - **Meeting recordings:** audio recording, meeting title, participant names, and AI-generated transcript, summary, action items, financial facts and vulnerability flags (see "Artificial intelligence")

Website visitors, marketing contacts and event, webinar and podcast participants

- **Identity:** name, job title, firm name, work contact details and location
- **Marketing:** preferences and communication history such as email opens, click-throughs and unsubscribes
- **Event:** event and webinar registration and attendance details, including dietary or access requirements where you provide them, and photographs, video and audio recorded at our events or for our podcasts, where you appear or take part
- **Online activity:** how you interact with our websites and online advertising, collected via cookies and similar technologies (see "Cookies")
- **Communication records:** (see "Anyone who communicates with us")

Clients - indirect (no agreement with us)

- **Planning:** information entered into our software by your adviser or by you. This includes identity and contact details, goals and objectives, dependants and family circumstances,

employment, income, assets, expenditure, risk profile responses, estate and IHT planning details, and any health or vulnerability information recorded (see "Special category and criminal offence data")

- **Account and transaction:** where you invest in our Model Portfolio Service or multi-asset funds, information your adviser or platform passes to us to operate the portfolios or funds. This includes your name, account number or other identifier, model portfolio selection, holdings and valuations.
- **Timeline Meeting Notes:** Where your adviser uses this product your email address may be included in a calendar event if invited to a meeting, and the meeting recording and its AI-generated outputs may include your name and information discussed (see 'Artificial intelligence'). Your adviser is responsible for telling you before a meeting is recorded.

Clients - direct (an account or agreement with us)

- **Identity:** such as your name, date of birth, address, contact details, marital status, gender, nationality, and national insurance or other identity numbers, and our agreement with you
- **Financial:** such as your employment, income, assets and personal wealth, bank account details, tax status and tax identification numbers
- **Account and transaction:** such as your account number or other identifier, holdings, expected and total investment amounts, orders, valuations, transfers, statements and fees
- **AML and screening:** such as verification results, identification documents, source of funds and source of wealth information, PEP and sanctions screening outcomes, and our risk assessments
- **Special category:** health or vulnerability information shared with us, or identified by us, so we can support you appropriately (see 'Special category and criminal offence data')
- **Communication records:** (see "Anyone who communicates with us")
- Where you use the Client Portal: portal usage, secure messages and document access
- Where your adviser uses our planning tools: the planning information described under "Clients - indirect" above
- Where your adviser uses Timeline Meeting Notes: see 'Clients - indirect' above.

Anyone who communicates with us

- **Communications records:** such as emails, correspondence, chat transcripts, call and video recordings, and notes and transcripts of our conversations (see "Recording and monitoring communications")

Technology users (all products)

- **Account and login:** credentials, user IDs, authentication data, and role and permission settings
- **Security:** device, browser and connection information, and security and audit logs
- **Usage:** features used, actions taken, documents accessed and messages sent, which we use to run, secure, support and improve our technology, including Pennee

Connected people

- Details of dependants, beneficiaries, trustees, settlors, attorneys, directors, shareholders and beneficial owners, where they appear in a plan, application, trust or corporate account. This typically includes identity, relationship and, where relevant, financial details. If you provide us with information about someone else, please make sure they are aware of this notice.

Suppliers and business contacts

- **Identity:** such as work contact details, correspondence and contract information for staff at our suppliers, partners and other organisations we deal with
- **Financial:** such as bank account, billing and payment information, and tax and/or VAT registration details.

Job applicants and enquirers

- **Identity:** contact details when you enquire about working with us, including speculative applications.
- **Communication records:** (see "Anyone who communicates with us")
- **Recruitment:** such as CVs, application forms, interview notes and assessments, references, right-to-work checks and other pre-employment checks. Pre-employment checks are carried out once we have offered you a role and the level of checks depends on it. They may include credit checks, criminal record checks, and verification against the FCA register, directorship and other public records.
- If your application is successful, we transfer your information to your employment record and our separate employee privacy notice applies from that point.

Special category and criminal offence data

Where advice firms use our planning tools, sensitive data such as health and vulnerability details may be recorded. Your advice firm decides what is collected as controller, and we process it on their instructions as a processor.

As a controller in our own right, we process special category data only in limited situations:

- Health or vulnerability information you choose to share with us so we can support you appropriately. Disclosing this is voluntary. We record it under the same substantial public interest condition set out below, so that we can keep supporting you consistently.
- Vulnerability information we identify, or that your adviser or a platform tells us about. This may include through AI analysis of meeting recordings in Timeline Meeting Notes. We record this so we can support you in line with FCA expectations. We rely on the substantial public interest condition in Schedule 1 to the Data Protection Act 2018 for the exercise of our regulated functions, because recording and acting on vulnerability is part of meeting our obligations to you under FCA rules. Where someone is at risk of harm, we rely instead on the condition covering the safeguarding of individuals at risk. We keep an appropriate policy document explaining how we comply, which you can ask us for. We do not rely on your consent for this, so withdrawing consent will not remove a vulnerability record we are required to keep.
- Accessibility or dietary needs you share for our events, processed with your consent.

Separately, financial crime screening may reveal information about criminal convictions or alleged offences. This includes sanctions, PEP and adverse media checks. We undertake this screening to meet our anti-money laundering (“AML”) obligations. We rely on the conditions in Schedule 1 to the Data Protection Act 2018 for preventing or detecting unlawful acts, for regulatory requirements relating to unlawful acts and dishonesty, and for preventing fraud. We keep an appropriate policy document explaining how we comply, which you can ask us for.

Children

Our services are designed for adults and advice professionals. We may process limited information about children. This applies where they appear in a financial plan as dependants or beneficiaries, or where an account is held for them, such as a junior account. We do not market to children and we do not offer our services directly to them. We only use their data to run the plan or account concerned, and we apply the same protections set out in this notice.

Where we get your personal data from

- Directly from you when you register, contact us, sign up to events or newsletters, or use our websites and products
- From your financial adviser or advice firm, or others acting on your behalf
- From other platforms and providers, such as our custody partner, other investment platforms and product providers
- From third parties. This includes identity verification, AML and fraud prevention providers, credit reference agencies, pre-employment check providers, referees, and B2B marketing data providers such as Financial Clarity
- From publicly available sources such as the FCA register, Companies House, firm websites, social media and professional networking sites
- Generated by us such as account records, analytics, call recordings and audit trails

Do you have to provide your personal data?

Some information is needed to comply with the law, such as identity information for anti-money laundering checks, or to enter into and carry out our contract with you or your firm. If it isn't provided, we may not be able to open your account, process transactions, or provide the service. Where information is optional, such as health or vulnerability details, we will make that clear when we ask.

How we use your personal data and our lawful bases

We only process personal data where Data Protection Laws allow. This table sets out our lawful basis for processing, where we are the controller. For some services, including Timeline Planning and Timeline Meeting Notes, your advice firm is the controller and we act as their processor, on their instructions (see 'Our role and your relationship with us'). 'What personal data we collect' sets out what we hold across all our services, including as processor.

Purpose	Data used	Lawful basis
Providing our investment and platform services including managing accounts, orders, custody and	Identity, Financial,	Contract (direct agreements); legitimate interests (where you

Purpose	Data used	Lawful basis
transfers; operating the client portal and secure messaging; providing support, handling complaints and protecting our legal rights	Account and transaction	are not the contracting party, e.g. staff at a firm)
Digital onboarding, identity verification, KYC/AML, sanctions and fraud checks; tax reporting; regulatory record-keeping and reporting to the FCA, HMRC and other authorities	Identity, AML and screening	Legal obligation; plus, for any criminal offence data revealed by screening, the Schedule 1 conditions for preventing or detecting unlawful acts, for regulatory requirements relating to unlawful acts and dishonesty, and for preventing fraud
Providing and operating Timeline Planning including Pennee and the Adviser and Client Portals	Account and login, Security, Usage	Contract (direct agreements); legitimate interests (where you are not the contracting party, e.g. staff at a firm), consent (opting in to Pennee, revocable at any time)
Providing and operating Timeline Meeting Notes	Account and login, Security, Usage, Calendar, Meeting recordings	Contract (direct agreements); legitimate interests (account access, and our own handling of recordings); consent (calendar connection, revocable at any time)
Supporting you where you share, or we identify, health or vulnerability information; accessibility and dietary needs for our events	Special category	Legal obligation and legitimate interests (Article 6); explicit consent for accessibility and dietary needs, and the substantial public interest condition in Schedule 1 for the exercise of our regulated functions, or where someone is at risk of harm, the condition for safeguarding individuals at risk (Article 9)
Recording and monitoring communications for regulatory compliance, quality and service, training our staff, and gathering feedback to improve our products and services	Communication records, Service data	Legal obligation (where required by FCA rules); legitimate interests
Improving and developing our products, technology and services. This includes analytics, testing,	Usage, Security, Service data, Communications	Legitimate interests with a right to object for the profiling element

Purpose	Data used	Lawful basis
research and understanding the firms we serve (which may involve profiling), and keeping our systems, premises and data secure		
Marketing our products, services and events; measuring engagement and firm-level segmentation (which may involve profiling)	Marketing data, Event data, Usage, Communications	Consent (where you sign up); legitimate interests where you become a customer (we tell you at onboarding and you can opt out at any time); legitimate interests, with a right to object, for the profiling element.
Recruitment including assessing applications and enquiries about working with us	Identity, Recruitment data	Legitimate interests; legal obligation; steps before entering a contract
Corporate transactions e.g. a merger, acquisition, restructuring or sale involving Timeline	Identity, Financial	Legitimate interests
Managing relationships with suppliers, partners and professional advisers	Identity, Financial	Contract; legitimate interests

Where we rely on legitimate interests, we balance our interests against your rights and freedoms. We do not use this basis where your interests override ours. You can ask us for more information about our balancing assessments.

Recording and monitoring communications

We record and monitor communications with you including telephone and video calls, secure messages within our technology, support chats and emails. We do this:

- To comply with our legal and regulatory obligations, including FCA rules requiring us to record certain communications relating to orders and transactions
- For our legitimate interests in carrying out instructions accurately, resolving queries and disputes, monitoring service quality, and training our people
- To gather feedback and understand how our products and services are used, so we can improve them
- To keep our systems and users secure and to detect fraud or misuse

We may use technology, including AI tools, to transcribe, summarise or analyse recorded communications for these purposes (see "Artificial intelligence"). Copies of recorded communications are available on request.

Webinars, podcasts and events may be recorded, including questions and contributions from participants. Where a recording is for publication, we will make this clear at the time.

Marketing

We market mainly to financial advice professionals in a business-to-business context. We may contact you about our products and services, research, newsletters, regulatory updates, podcasts, webinars and events (including Adviser 3.0). We do this where you have opted in. We also do this where we obtained your details while selling, or negotiating to sell, similar products or services to you, and you did not opt out at the time. This is known as soft opt in. When you opt in, you can choose which types of communication you receive, and you can change these preferences at any time.

We collect marketing data directly from you, and from your interactions with our communications and websites. We also collect it from third-party B2B data providers such as Financial Clarity. We measure engagement (such as email opens and event attendance) to keep communications relevant, and use aggregated insights to understand the firms we serve (see "Automated decision-making and profiling").

You can opt out at any time using the unsubscribe link in any marketing email or by contacting us at support@timeline.co. If you do, we keep your details on a suppression list so we can honour your preference. We do not sell your personal data.

Artificial intelligence

We use artificial intelligence ("AI") to enhance our services and run our business efficiently. Where AI processes personal data, it does so for the purposes and on the lawful bases set out in this notice.

Our services may use AI to suggest, summarise or automate tasks, including recording, transcribing and summarising meetings. Timeline Meeting Notes, our standalone meeting app, records meetings and processes audio recordings and transcripts using third-party AI services. This produces a transcript, summary, action items and, where relevant, financial facts and vulnerability flags. Recordings and transcripts are then available within Timeline Planning, where Pennee, our AI assistant, may also process them. Pennee's AI features are opt-in only and act on your firm's instructions. If Pennee is not switched on for an account, Pennee has no access to recordings and transcripts. These features, including Pennee, process personal data within our ecosystem and never take action without user approval.

Timeline Meeting Notes can also connect to your Google or Outlook calendar to retrieve event and participant details. Where we receive data through Google Workspace APIs, we follow the [Google API Services User Data Policy](#), including its Limited Use requirements. We only use this data to run the calendar feature.

Where advice firms use our AI features, including Pennee, the firm remains the controller of its clients' personal data. It decides what data is used, must tell participants about this and get consent where needed.

We also use AI tools to work efficiently, including to transcribe meetings we take part in, and in our marketing, to understand the firms we serve (see "Automated decision-making and profiling"). We tell participants when a transcription tool is used.

When we test new AI features, we use synthetic data. Where AI is used for product research and analytics we may use personal data, including from calls (see 'Recording and monitoring communications'). Personal data is not used to train AI models, including by any third-party AI

providers we use. We carry out due diligence and data protection impact assessments before using AI that processes personal data. We also put contractual safeguards in place with AI providers. We do not use AI to make solely automated decisions with legal or similarly significant effects on you. We will update this notice before materially changing how AI processes personal data.

Automated decision-making and profiling

We do not make decisions based solely on automated processing that produce legal or similarly significant effects on you. Some of our processes are automated, such as elements of identity verification and AML screening. However, before any decision that has a legal or similarly significant effect on you, a trained member of our staff with authority to change the outcome reviews the case and makes the decision. You can ask us to explain a decision and to review it again.

To understand the different types of firm we serve, we also build combined, firm-level profiles of our adviser customers. These draw on themes from our own contact with you, such as sales, support and relationship calls, and on public information about firms. We do not use data processed on behalf of advice firms through our products (such as Pennee meeting recordings) for this purpose. This profiling is designed to describe firms, not individuals. However, drawing themes from our calls involves processing recordings that contain personal data (see "Recording and monitoring communications"). Where a firm is a sole trader or small practice, its profile can itself be personal data. We rely on legitimate interests for this, and you can object at any time.

Who we share your personal data with

We share personal data only where needed for the purposes set out in this notice. Where a third party processes data for us, we require it by contract to meet our data protection and security standards. Our Trust Centre at trust.timeline.co lists the providers we use and the countries they operate from. Depending on the services used, we may share data with:

- **Timeline group:** between our operating companies for administration, service delivery, security, analytics and (where permitted) marketing; and with Timeline Holdings Limited only where group business operations require it, such as governance, audit, group reporting or a corporate transaction.
- **Your advice firm and those acting for you:** your financial adviser, appointed representatives, your bank, and anyone you authorise.
- **Financial market participants:** including Seccl, which provides order handling and custody for the Timeline Platform (Seccl's own privacy notice also applies); and custodians, fund managers, clearing houses, other platforms and product providers, for example when processing transfers or Letters of Authority.
- **Service providers:** providers of cloud hosting, identity verification and AML screening, background checks, credit reference agencies, payments, support and communications tools, analytics, CRM and email platforms, AI services, and IT security, subject to due diligence and contracts requiring our data protection and security standards; and, for job applicants, referees and previous employers. Our Trust Centre at timeline.co/trust names the providers in each of these categories, what they do for us, and the countries they work from.

- **Event and marketing partners:** venues, event platforms and co-hosts, where you register for or take part in our events.
- **Regulators, authorities and law enforcement:** including the FCA, ICO, HMRC, courts and fraud prevention agencies, where required or permitted by law.
- **Professional advisers and consultants:** our auditors, accountants, insurers, insurance brokers, compliance and HR consultants, and legal advisers.
- **Corporate transactions:** a buyer, seller or successor (and their advisers) in the event of an actual or proposed merger, acquisition, restructuring or sale involving Timeline, with appropriate safeguards.

International transfers

We store personal data mainly in the UK and the European Economic Area (EEA), which UK adequacy regulations cover. The main countries outside the UK and EEA that our providers process or access data from are the United States. Our Trust Centre at trust.timeline.co sets out the current list. Some service providers and contractors working for us from outside the UK and EEA process or access personal data. Where they do, we put equivalent protection in place. This may include:

- UK adequacy regulations covering the destination country
- The UK Extension to the EU–US Data Privacy Framework, for certified US recipients
- The UK International Data Transfer Agreement (IDTA), or the EU Standard Contractual Clauses together with the UK Addendum, supported by transfer risk assessments

You can contact us for more information about, or a copy of, the safeguards for a specific transfer.

Cookies and similar technologies

Our websites use cookies and similar technologies to make them work, to understand how they are used and to support our marketing. You can manage non-essential cookies through the cookie banner on our websites and via your browser settings. Some features may not function fully if you disable them.

For details of the specific cookies we use and how long they last, see our Cookie Policy at timeline.co/legal.

How we keep your personal data secure

We take a layered approach to security across our organisation, people, processes and technology. This includes encryption in transit and at rest, access controls and authentication, monitoring, testing and staff training. Third parties processing data for us must meet contractual security and confidentiality duties. We review their controls.

How long we keep your personal data

During our relationship with you, we keep the personal data needed to provide our services. We take reasonable steps to keep it accurate and up to date. Some records must be kept for minimum periods required by law or regulation. These generally include:

- Five years for investment business records, including recordings of communications about orders and transactions (seven where required by the FCA)
- Five years from the end of our relationship for anti-money laundering and identity verification records
- Indefinitely for pension transfers, where applicable

Beyond our relationship with you and these legal minimums, we may keep data where we have a legitimate interest in doing so. We balance those interests against your rights and freedoms first. Generally, we keep data relating to our services for six years after our relationship ends. This lets us respond to queries or complaints, defend legal claims and evidence our compliance if asked. If we hold data for more than one purpose, we keep it until the longest retention period ends. We only use it for the purposes that still apply. Shorter periods apply to other categories, such as enquiries that do not proceed, marketing data and unsuccessful job applications. Website analytics data is kept as set out in our Cookie Policy. Once the relevant period ends, we securely delete or anonymise the data. You can also ask us to delete your data at any time, subject to the retention obligations above.

For further information about our retention policy, please contact us.

Your rights

Under Data Protection Laws you have the following rights:

- **A right of access:** ask us for a copy of your personal information (known as a 'subject access request').
- **A right to rectification:** ask us to rectify personal information you think is inaccurate or incomplete.
- **A right to erasure:** ask us to delete your personal information, in certain circumstances.
- **A right to restriction:** ask us to limit how we can use your personal information, in some cases.
- **A right to data portability:** ask us to transfer the personal information you gave us to you, or to another organisation, in some cases.
- **A right to object:** you can object to processing of your personal information based on our legitimate interests. You have an absolute right to object to direct marketing.
- **A right to withdraw consent:** at any time, where we rely on consent
- **A right about automated decision making:** you can ask not to be subject to fully automated decisions, including profiling, that have legal or similarly significant effects.

These rights are not absolute. For example, we cannot erase records we must keep to comply with our legal and regulatory obligations. We will explain any limitation when we respond.

You can exercise your rights free of charge by contacting us (see "Who we are"). We may need to verify your identity first. We will only charge a reasonable fee, or refuse to act, where a request is manifestly unfounded or excessive. We have one month to respond, and may extend this by up to two further months for complex or multiple requests. We will tell you within the first month if so, and explain why. If your data was entered into our technology by your advice firm, we may need to refer your request to them as controller and will tell you if so.

You also have the right to complain to the Information Commissioner's Office at any time, although we would welcome the chance to address your concerns first:

- Online: ico.org.uk/make-a-complaint
- Telephone: 0303 123 1113
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Changes to this notice

We review this notice regularly and update it when the law, our services or our technology change. You can find the latest version on our website. If a change affects you significantly, we will take reasonable steps to let you know.

Last reviewed and updated: 7 September 2026



Email support@timeline.co

Office 70 Gracechurch St
4th Floor
London
EC3V 0HR

timeline.co

Timeline investing and platform services are provided by Timeline Portfolios Limited (No. 11557205), which is authorised and regulated by the Financial Conduct Authority (FRN: 840807). Timeline planning software and tools are provided by Timelineapp Tech Limited (No. 11405676) and are not regulated by the Financial Conduct Authority. Both companies are registered in England and Wales with their registered office at 70 Gracechurch Street, London, EC3V 0HR.