REDLINE ADVISORY
Remove friction. Recover capacity. Accelerate revenue.

Redline Advisory

Privacy Policy for Clients

Contents

1. About this Privacy Policy
2. Who Redline is
3. When this Privacy Policy applies
4. Redline as controller and processor
5. Personal data we collect
6. How we obtain personal data
7. How and why we use personal data
8. Contract Friction Scorecard
9. Enquiries, discovery and business development
10. Marketing and your choices
11. Client engagements
12. Meetings, transcription and recordings
13. Artificial intelligence and automation
14. Benchmarking, statistics and case studies
15. Sharing personal data and service providers
16. International transfers and overseas access
17. How long we keep personal data
18. Security and access controls
19. Website analytics and cookies
20. Your data protection rights
21. Complaints
22. Changes to this Privacy Policy
23. Contacting Redline
Schedule 1 - Data Processing Activities
Schedule 2 - Retention Framework
Document control and revision history

REDLINE ADVISORY
Remove friction. Recover capacity. Accelerate revenue.

1. About this Privacy Policy

Redline Advisory Limited ("Redline", "we", "us" or "our") is committed to handling personal data lawfully, fairly, transparently and securely. This Privacy Policy explains what personal data we collect, where we obtain it, why we use it, the lawful bases on which we rely, how long we keep it, who we may share it with and the rights available to individuals under UK data protection law.

Redline is a business-to-business contract operations consultancy. Much of the information we work with concerns organisations, contracting processes, templates, workflows, systems and commercial operations rather than individuals. Business information can nevertheless be personal data where it identifies or relates to a person, such as a named business contact, an individual work email address, comments in a contract draft or the views of a stakeholder interviewed during an engagement.

This Policy principally explains processing for which Redline determines the purposes and means and therefore acts as controller. It also explains, at a high level, circumstances in which Redline may process personal data on behalf of a client as processor. Where Redline acts solely as processor, the relevant client is responsible for its own privacy information and Redline's processing is governed by the client agreement and applicable data processing terms.

2. Who Redline is

The controller for the processing described in this Policy is Redline Advisory Limited, company number 17457878, whose registered office is at Suite A, 82 James Carter Road, Mildenhall, IP28 7DE.

Privacy enquiries, requests to exercise data protection rights and concerns about our use of personal data can be sent to privacy@redlineadvisory.co.uk. Redline has not appointed a Data Protection Officer because it does not currently consider that it is required to do so.

3. When this Privacy Policy applies

This Policy applies where Redline processes personal data in connection with its own business activities, including people who:

- visit the Redline website or complete the Contract Friction Scorecard;
- contact us, book or attend discovery calls, or communicate with us about potential services;
- are identified as relevant business contacts through targeted business development;
- work for, represent or otherwise interact with a Redline client in connection with an engagement;
- act as suppliers, advisers, insurers or other professional contacts; or
- otherwise have personal data processed by Redline for legal, compliance, finance, security or business-administration purposes.

This Policy does not replace a client's own privacy notice where Redline processes personal data solely on that client's behalf. It should also be read together with any short privacy information provided at the point of collection, including the notice presented with the Contract Friction Scorecard.

4. Redline as controller and processor

Redline's data protection role depends on the particular processing activity. Redline is a controller when it decides why personal data is required and the essential purposes for which it will be used. This includes Redline's website and Scorecard, enquiries, targeted B2B prospecting, CRM and sales pipeline, marketing preferences, client relationship management, invoicing, legal and compliance records and Redline's own business administration.

During some client engagements, Redline may process personal data contained in client documents, systems or workflows solely to provide services requested by the client. To the extent Redline processes that personal data on the client's documented instructions, the client will generally act as controller and Redline as processor.

Redline may exercise professional or technical judgement about how to perform an engagement without necessarily determining the client's underlying purposes for personal data. Equally, not every activity undertaken during an Audit or implementation is automatically processor activity. Redline remains controller for its own engagement administration,

relationship records, legal/compliance records and other processing carried out for Redline's own legitimate purposes. Where required, the relevant contract and Data Processing Schedule set out the parties' responsibilities.

5. Personal data we collect

Category	Examples
Identity and business contact data	Name, job title, employer, work email, work telephone number where provided, LinkedIn profile and other professional contact details.
Scorecard data	First and last name, work email, company, job title, 18 structured responses, six dimension scores, overall score, classification, lowest-scoring dimensions, submission ID/timestamp and optional marketing preference.
Website and technical information	High-level website usage information generated by Framer Analytics and technical/security information necessarily processed by website and service infrastructure.
Prospect and CRM information	Company, sector, size, website, source, relevant contact details, outreach history, Scorecard participation, discovery notes, pipeline stage and marketing/suppression status.
Booking and meeting information	Name, email, job title, company, appointment date/time, meeting details, business requirements, contracting pain points, systems, volumes, objectives, budget/timing where discussed, transcripts, summaries and actions.
Client engagement information	Stakeholder details and personal data incidentally contained in contract versions, tracked changes, selected correspondence, approval information, CRM/CLM extracts, workflow/system records and deliverables.
Contract and finance data	Signatures, contractual correspondence, invoices, payment and transaction information and records required for bookkeeping, tax or dispute management.
Marketing preference data	Opt-in/withdrawal information, objections and suppression records.
Supplier/professional contact data	Names, roles, work contact details and correspondence with suppliers, advisers, insurers and other professional contacts.

Redline does not intentionally collect special category personal data or criminal-offence data through the Scorecard or ordinary business development. Such information may occasionally appear incidentally in client material. Where that occurs, Redline limits processing to what is necessary, applies appropriate safeguards and, where acting as processor, follows the client's documented instructions.

Redline's services are directed to businesses and are not directed to children. We do not knowingly seek to collect children's personal data through our website, Scorecard or business-development activities.

6. How we obtain personal data

We collect personal data directly when a person completes the Scorecard, contacts us, emails us, submits a website enquiry, books or attends a meeting, provides information during a discovery or stakeholder interview, signs or administers an agreement, or otherwise communicates with Redline.

We may also obtain business contact information from an individual's employer or colleagues and from public or professional sources such as company websites, LinkedIn, Companies House, search engines, referrals, events and networking. We also use Apollo.io as a business contact-data service to identify relevant corporate prospects and work contact information.

Relevant prospect and relationship information may be recorded in HubSpot, which Redline uses as its principal CRM.

In a client engagement, information may be supplied by the client or made available within the client's controlled environment. Depending on the engagement, this may include contract templates and versions, selected negotiation examples, approval matrices, policies, standard operating procedures, workflow information, selected CRM/CLM metrics or exports, process data and stakeholder information. We seek representative and proportionate information rather than unnecessary bulk datasets.

7. How and why we use personal data

Redline must have a lawful basis whenever it processes personal data as controller. Depending on the activity, we may rely on:

- consent under Article 6(1)(a) UK GDPR, for example where an individual actively opts in to optional marketing;
- contract or steps requested before entering into a contract under Article 6(1)(b), where that basis applies to the individual concerned;
- compliance with a legal obligation under Article 6(1)(c); or
- legitimate interests under Article 6(1)(f), where the processing is necessary for a legitimate business purpose and those interests are not overridden by the individual's rights and interests.

Where we rely on legitimate interests, those interests may include operating and securing Redline; administering the Scorecard; responding to enquiries; understanding prospective client requirements; developing relevant B2B relationships; managing the sales pipeline; delivering and improving professional services; maintaining appropriate engagement and financial records; preventing unwanted marketing through suppression records; and establishing, exercising or defending legal rights.

Schedule 1 summarises Redline's principal processing activities, purposes, lawful bases and roles.

8. Contract Friction Scorecard

The Contract Friction Scorecard is an online assessment designed to help a business understand where friction may exist within its contracting processes. It asks 18 structured questions and collects the respondent's first name, last name, work email address, company and job title. The Scorecard is not designed to collect special category personal data.

The Scorecard automatically calculates six dimension scores, an overall Contract Friction score, a classification and the lowest-scoring dimensions. The result is displayed to the respondent. This automated calculation does not make a decision about an individual that produces legal or similarly significant effects.

Redline records Scorecard submissions to administer the assessment, understand engagement, analyse common areas of contract friction, provide appropriate follow-up about the result, invite relevant respondents to a discovery conversation and manage qualified opportunities. A respondent does not need to consent to general marketing in order for Redline to communicate appropriately about the Scorecard they chose to complete.

Scorecard submissions are currently received through Google Apps Script and stored in a restricted Google Sheet controlled by Redline. Multi-factor authentication is enabled on the relevant account. Qualified or relevant submissions may be entered manually into HubSpot. Redline may migrate this process into its Microsoft 365 environment and automate appropriate CRM integration in future; this Policy will be reviewed where that materially changes the processing.

9. Enquiries, discovery and business development

When someone contacts Redline, submits a website enquiry, books a call or takes part in a discovery conversation, we use the information provided to respond, understand the organisation's needs, assess whether our services may be relevant, prepare or discuss a proposal and manage the prospective relationship.

Website enquiries currently collect name, email address and message. Discovery calls booked through Microsoft Bookings collect first and surname, email address, job title, company and the selected appointment date/time.

Redline also carries out targeted business-to-business prospecting across relevant sectors. We may identify relevant decision-makers and business contacts through public professional sources, referrals, networking and business contact-data services such as Apollo.io, and record appropriate information in HubSpot.

Where we use a named business contact's personal data for direct marketing, UK data protection law continues to apply even though the person is acting in a business capacity. We rely on an appropriate lawful basis, make this Privacy Policy readily available and respect objections to direct marketing. Outreach identifies Redline and provides a practical means to opt out. Where a person objects, we may retain the minimum information necessary on a suppression or do-not-contact record so that the objection can be honoured.

10. Marketing and your choices

The Scorecard includes a separate, optional marketing choice. Where an individual actively opts in, Redline may use their details to send occasional contract-operations insights, guidance, articles and resources, event or webinar information, benchmark reports and information about Redline services. The marketing choice is not required to complete the Scorecard or receive appropriate communications about the Scorecard submission itself.

Where Redline relies on consent for optional marketing, consent can be withdrawn at any time. Where Redline relies on legitimate interests for permitted B2B direct marketing, the individual has an absolute right to object to the use of their personal data for direct marketing. Marketing status and suppression information may be maintained in HubSpot.

Your right to object to direct marketing: you can ask us at any time to stop using your personal data for direct marketing by contacting privacy@redlineadvisory.co.uk or using any opt-out method provided in the communication.

11. Client engagements

11.1 Contract Friction Audits

A Contract Friction Audit may involve contract templates and selected versions, negotiation examples, approval matrices, policies and SOPs, workflow information, selected CRM/CLM metrics or exports, process data and stakeholder interviews. Redline seeks representative samples rather than bulk datasets and does not require executed contracts as a default input.

Audit material is normally handled within Redline's controlled Microsoft 365 environment. We seek to minimise personal data and focus on the contracting process, systems, controls and commercial operations. Where client material contains personal data, for example names in tracked changes, negotiation correspondence or approval information, access and use are limited to what is reasonably necessary for the engagement.

11.2 Implementation and optimisation

Implementation and optimisation may involve Redline configuring workflows, conditional logic, approval routes, contract generation, automation and reporting using tools including SharePoint, Power Automate, Power BI, Microsoft Forms and Microsoft Lists.

For implementation work, Redline preferentially works within a client-controlled environment where practical. Where Redline processes client personal data solely on the client's instructions, Redline acts as processor and the client's Data Processing Schedule governs that processing. Client-system access should use named individual accounts where supported, be limited to the relevant functions and be removed when no longer required.

Redline normally uses dummy or synthetic data while developing and testing workflows. Production personal data is used only where reasonably necessary for launch, operation or controlled troubleshooting. Unnecessary exports, duplicates and temporary working copies are deleted when no longer required.

12. Meetings, transcription and recordings

Microsoft Teams is Redline's default meeting platform, although clients and other parties may invite Redline to meetings using their preferred platforms.

Discovery, stakeholder and delivery meetings may be transcribed where this assists accurate note-taking, analysis, actions or preparation of deliverables. Redline may use recording functionality where there is a genuine business need. Attendees will receive appropriate notice when transcription or recording is used.

Raw transcripts or recordings are not retained indefinitely. Where an accurate summary, action record or relevant deliverable has been created, the raw transcript or recording will normally be deleted within 120 days of the relevant meeting or engagement stage unless there is a genuine operational, contractual or legal reason to retain it for longer. Material summaries or decisions may form part of the relevant engagement record.

13. Artificial intelligence and automation

Redline uses Microsoft Copilot within its Microsoft 365 business environment to support appropriate business activities such as drafting, analysis, summarisation and development of recommendations. Redline may also use automation within Microsoft 365, including Power Automate, to support contract generation, workflow, reporting and administrative processes.

AI is a support tool and does not replace professional judgement. Material AI-assisted analysis or recommendations supplied to a client are subject to appropriate human review before use.

Redline does not use personal or consumer AI services as repositories for identifiable client personal data or client-confidential information. Where generic drafting or research tools are used outside the approved business environment, information must first be genuinely anonymised or sufficiently redacted so that individuals and confidential client information are not identifiable.

Where Redline acts as processor, any use of an AI provider involving client personal data must also be consistent with the client's documented instructions, Redline's Data Processing Schedule and applicable sub-processor arrangements.

Redline does not use AI to make solely automated decisions about individuals that produce legal or similarly significant effects.

14. Benchmarking, statistics and case studies

Redline may analyse Scorecard information and service experience to understand recurring contract-friction themes and develop benchmarks, statistics, research and market insights. Identifiable information remains personal data while it is analysed in identifiable form and is processed under the lawful basis applicable to that activity.

Information is treated as anonymous only once Redline has taken reasonable steps to ensure that individuals cannot be identified or reasonably re-identified. Public benchmarking will not identify individual respondents or clients unless there is a separate, express agreement to do so.

Redline uses a conservative minimum cohort of 50 organisations or respondents before publishing a segmented public benchmark and applies additional judgement where combinations of sector, organisation size, geography, role or other characteristics could still create a meaningful re-identification risk.

Genuinely anonymous aggregate information may be retained and reused because it is no longer personal data. Any named client case study, testimonial, client-list reference or use of a client's logo or identity for promotional purposes requires separate agreement and is not inferred from participation in the Scorecard or a client engagement.

15. Sharing personal data and service providers

Redline does not sell personal data and does not provide Scorecard respondent contact details to third parties for those third parties' own marketing.

We may disclose personal data where reasonably necessary to operate the business, deliver services, comply with law or protect legal rights. Depending on the activity, recipients may include:

- Microsoft, for Redline's business email, collaboration, document management, meetings, bookings, automation, reporting, forms, lists and approved AI functionality within Microsoft 365;
- Framer, for the Redline website and built-in website analytics;
- HubSpot, for CRM, sales pipeline, relationship management and marketing/suppression records;
- Google, for the current restricted Scorecard intake and storage arrangement using Google Apps Script and Google Sheets;
- Apollo.io, for business contact-data and prospecting support;
- BoldSign, for electronic signatures;
- Tide and other banking or financial service providers used for invoicing and receipt of payments;
- professional advisers, insurers, accountants, IT/security providers and other suppliers where reasonably required; and
- regulators, courts, law enforcement bodies or public authorities where disclosure is required or permitted by law.

Not every provider receives every category of personal data. Where a provider processes personal data on Redline's behalf, Redline uses appropriate contractual arrangements and proportionate due diligence.

15.1 Client-data sub-processors

The suppliers Redline uses for its own business operations are not automatically sub-processors of client personal data. Where Redline acts as a processor for a client, a supplier is treated as a sub-processor only where that supplier is engaged by Redline to process Client Personal Data on Redline's behalf in delivering the processor services.

Redline's standard Data Processing Schedule identifies the approved sub-processor arrangements applicable to Client Personal Data. Microsoft is the principal approved sub-processor in Redline's standard operating model. Any additional sub-processor use is governed by the applicable client agreement and Data Processing Schedule.

16. International transfers and overseas access

Redline is UK-based and may work with clients in the United Kingdom, European Economic Area and Middle East. Authorised Redline personnel may occasionally access Redline or client-controlled systems while travelling outside the UK. Overseas access is expected to use secure remote access rather than creating unnecessary local repositories of client files.

Some technology providers or their group companies may process or make personal data available outside the United Kingdom. Where Redline makes a restricted transfer under UK data protection law, we use an appropriate transfer mechanism, which may include UK adequacy regulations or approved contractual safeguards together with any assessment or supplementary measures required in the circumstances.

Where Redline acts as processor, international transfers are also subject to the client's documented instructions and applicable data processing terms. You may contact privacy@redlineadvisory.co.uk for further information about safeguards relevant to a particular transfer.

17. How long we keep personal data

Redline keeps personal data only for as long as reasonably necessary for the purpose for which it was collected, taking account of legal and accounting obligations, the nature of the record, security needs, client instructions and the potential need to establish or defend legal rights.

As a general framework, identifiable Scorecard submissions that do not become part of an active client relationship are normally retained for 24 months. Unsuccessful enquiries and prospect records are normally retained for 24 months from the last meaningful interaction, subject to any fresh interaction and the need to retain a minimal suppression record. Core client contractual and project records may normally be retained for up to six years after the engagement ends, while temporary working copies, bulk client data and unnecessary exports are deleted much earlier.

Where Redline acts as processor, the client agreement and Data Processing Schedule govern return or deletion of the underlying Client Personal Data. Redline does not apply its general controller retention period to an entire client dataset merely because it needs to retain its own contract, invoice, material instruction or final-deliverable records.

Schedule 2 provides Redline's current default retention framework.

18. Security and access controls

Redline applies proportionate technical and organisational measures intended to protect personal data against unauthorised access, accidental loss, alteration, disclosure or destruction.

Microsoft 365 is Redline's primary controlled business environment. Exchange/Outlook, SharePoint, OneDrive, Teams, Bookings, Copilot, Power Automate, Power BI, Microsoft Forms and Microsoft Lists may be used for appropriate Redline business and service-delivery purposes. SharePoint and OneDrive operate as the principal Redline repositories for business and client documents.

Access is limited according to business need and multi-factor authentication is used on material Redline business accounts where supported. Devices used for Redline work are protected by appropriate password, PIN or biometric controls, security updates and device encryption where supported. Redline/client information must not be stored in uncontrolled personal cloud repositories.

Any future director, employee, associate or contractor requiring system access will receive an individual account and access appropriate to their role. Access will be removed when no longer required. Security incidents are escalated promptly so that access can be revoked, the incident contained and any personal data breach risk assessed.

19. Website analytics and cookies

Redline's website is built and hosted using Framer. Redline currently uses Framer's built-in Analytics to understand high-level website usage. Redline's current configuration does not intentionally deploy Google Analytics, Google Tag Manager, advertising pixels or other advertising/conversion tracking technologies.

Redline does not currently use a cookie consent banner solely for its present Framer Analytics configuration. We keep the website technology stack under review and will reassess the position before introducing additional analytics, advertising, embedded services or other technologies that store information on, or access information from, a user's device.

Where applicable law requires consent for a cookie or similar technology, that technology will not be activated until appropriate information and a valid consent mechanism are in place. Essential technologies may be used without consent where the applicable legal conditions are satisfied.

20. Your data protection rights

UK data protection law gives individuals a number of rights in relation to their personal data. The rights available in a particular case depend on the circumstances and lawful basis, and some rights are subject to statutory conditions or exemptions.

Right	What it means
Access	Ask whether Redline processes your personal data and request a copy together with relevant information about the processing.
Rectification	Ask Redline to correct inaccurate personal data or complete incomplete information.
Erasure	Ask Redline to delete personal data where the legal conditions for erasure are met.
Restriction	Ask Redline to restrict processing in certain circumstances.
Data portability	Receive certain personal data in a structured, commonly used and machine-readable format where the right applies.
Object	Object to processing based on legitimate interests. You have an absolute right to object to processing for direct marketing.
Withdraw consent	Withdraw consent at any time where Redline relies on consent, without affecting processing carried out before withdrawal.
Automated decisions	Rights may apply to certain solely automated decisions with legal or similarly significant effects. Redline does not currently carry out this form of automated decision-making.

To exercise a right, contact privacy@redlineadvisory.co.uk. We may need to take reasonable steps to verify identity before disclosing or changing personal data. Redline will respond within the period required by applicable data protection law and will explain if a request cannot be complied with in full.

21. Complaints

If you have a concern about Redline's use of your personal data, please contact privacy@redlineadvisory.co.uk first so that we have an opportunity to investigate and respond.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK's data protection regulator. Further information about the ICO and how to make a complaint is available at ico.org.uk.

22. Changes to this Privacy Policy

Redline keeps this Privacy Policy under review and conducts a formal review at least annually. We may update it sooner where we introduce a material new service, supplier, system, analytics technology or use of personal data, where our business structure changes, or where legal or regulatory developments make an update appropriate.

Where a material new use of personal data requires additional transparency, we will update the relevant privacy information before or at the time that processing begins. The current version and effective date are shown in this Policy.

23. Contacting Redline

Contact point	Details
Controller	Redline Advisory Limited
Company number	17457878
Privacy email	privacy@redlineadvisory.co.uk
Registered office	Suite A, 82 James Carter Road, Mildenhall, IP28 7DE
Website	www.redlineadvisory.co.uk

REDLINE ADVISORY
Remove friction. Recover capacity. Accelerate revenue.

Schedule 1 - Data Processing Activities

This schedule summarises Redline's principal controller processing and identifies activities in which Redline may instead act as processor. The actual role depends on the facts and purposes of the particular processing.

Activity	Personal data	Purpose	Basis	LI / note	Role
Website operation/security	Technical/security information; enquiries	Operate, secure and maintain website	Art. 6(1)(f)	Secure/effective website and business operations	Controller
Framer Analytics	High-level site usage	Understand website performance	Art. 6(1)(f), to extent personal data is processed	Website/service improvement	Controller to extent personal data is processed
Scorecard administration	Identity/business contacts; 18 answers; scores/results	Administer assessment, analyse results, follow up and qualify opportunities	Art. 6(1)(f)	Operate Scorecard; understand friction; relevant B2B relationship	Controller
Scorecard benchmarking - identifiable stage	Scorecard results and business profile	Analyse patterns before anonymisation	Art. 6(1)(f)	Service improvement and evidence-based insight	Controller
Anonymous benchmarking	Genuinely anonymous/aggregate statistics	Publish and retain benchmarks/insights	Outside UK GDPR once genuinely anonymous	N/A	N/A
Enquiries and bookings	Business contacts; enquiry/booking details	Respond, arrange calls and assess potential engagement	Art. 6(1)(f); Art. 6(1)(b) where applicable	Prospective client management	Controller
B2B prospecting	Business contacts; public/professional/Apollo data; outreach history	Identify and approach relevant corporate prospects	Art. 6(1)(f), subject to applicable PECR rules	Targeted business development	Controller
CRM and pipeline	Contacts, company, interactions, Scorecard/discovery and stage	Manage prospects and opportunities	Art. 6(1)(f)	Relationship and pipeline management	Controller
Optional marketing	Name, work email, company and preference record	Send opted-in insights/resources/events/benchmark/service updates	Art. 6(1)(a)	Consent	Controller
Marketing suppression	Contact identifier and objection/opt-out	Prevent further unwanted direct marketing	Art. 6(1)(f) / compliance with rights	Respect objections and prevent re-contact	Controller
Discovery calls	Business contacts; meeting content; summaries	Understand requirements and scope services	Art. 6(1)(f); Art. 6(1)(b) where applicable	Accurate discovery and service design	Controller
Stakeholder interviews	Stakeholder contacts, views, transcript/summary	Understand current process and stakeholder experience	Underlying basis depends on role	Professional Audit methodology/service delivery	Controller or processor depending facts
Client relationship/contracting	Contacts, signatures, correspondence, SOW/proposal	Enter, administer and manage engagement	Art. 6(1)(f); 6(1)(b) where applicable; 6(1)(c) where required	B2B relationship and contract records	Controller
Audit - Redline records	Stakeholder contacts; notes; correspondence; outputs	Manage and evidence Audit delivery	Art. 6(1)(f)	Professional service delivery and records	Controller
Audit - client data on instructions	Personal data in selected contract versions, comments, correspondence, CRM/CLM material	Analyse client process solely for engagement	Client determines lawful basis; Art. 28 terms where applicable	N/A	Processor where solely instructed
Implementation / optimisation	User/workflow/approval/contract/system data	Configure, test, implement and optimise workflows/automation	Client determines lawful basis; Art. 28 terms where applicable	N/A	Likely processor for client personal data
AI-assisted processing	Relevant data for approved use	Assist analysis, summarisation, drafting or delivery	Underlying basis for relevant activity	Efficiency/quality with human review and tool controls	Follows underlying role
Finance and tax	Contacts, invoices, transaction data	Billing, banking, bookkeeping and tax	Art. 6(1)(c); Art. 6(1)(f)	Financial administration/compliance	Controller

Activity	Personal data	Purpose	Basis	LI / note	Role
Legal/compliance/incidents	Contracts, correspondence, incident and evidence records	Protect rights, comply with law, handle requests/incidents/disputes	Art. 6(1)(f); Art. 6(1)(c) where applicable	Legal rights, accountability and compliance	Controller
Suppliers/professional contacts	Name, role, work contacts and correspondence	Manage suppliers/advisers/insurers	Art. 6(1)(f); Art. 6(1)(b) where applicable	Business administration	Controller

REDLINE ADVISORY
Remove friction. Recover capacity. Accelerate revenue.

Schedule 2 - Retention Framework

The periods below are Redline's current default framework. A shorter or longer period may apply where the context, law, contract, dispute, security need or client instruction reasonably requires it. Redline avoids retaining unnecessary bulk client data merely because a related engagement record is retained.

Record / data	Default position	Rationale / treatment
Scorecard - no active client relationship	24 months from submission	Proportionate follow-up, analysis and service improvement without indefinite identifiable retention.
Unsuccessful enquiry / prospect	24 months from last meaningful interaction	Fresh meaningful re-engagement may create a new retention point; suppression information is treated separately.
Marketing consent/preferences	For the relevant marketing relationship	Consent can be withdrawn at any time; status should remain accurate.
Marketing suppression	As long as reasonably needed to honour objection	Keep only enough information to prevent unwanted re-contact.
Discovery/proposal not converted	Normally 24 months from last meaningful interaction	Longer only for a specific contractual, legal or dispute-management reason.
Raw meeting transcript / recording	Normally up to 120 days after meeting or relevant engagement stage	Delete earlier where summary/actions are sufficient; retain longer only where genuinely needed.
Core client contract/project records	Normally up to 6 years after engagement ends	Contract administration, professional record-keeping and potential legal claims, subject to record type.
Invoices/accounting/banking records	Applicable statutory/accounting period, normally at least 6 years where required	Tax and accounting compliance.
Temporary client working data, exports and duplicates	Delete/return when no longer needed	Data minimisation; do not retain merely because core engagement records are kept.
Processor data held for a client	As instructed in client agreement/Data Processing Schedule	Return/delete at end of processor services unless law requires storage.
Security/access/incident logs	According to security purpose and system need	Security, investigation and accountability.
Data subject request log	As reasonably required for accountability and legal record	Keep a proportionate record of request and outcome; avoid unnecessary copies of identity evidence.
Genuinely anonymised statistics	Indefinitely	Outside UK GDPR once reasonable re-identification is no longer possible.

Document control and revision history

Field	Details
Document owner	Redline Advisory Limited
Approved by	Redline Advisory Limited
Version	1.0
Effective date	13 September 2026
Last reviewed	13 September 2026
Next review	13 September 2027, or sooner following material change
Public facing	Yes

Revision history

Version	Date	Status	Description
1.0	13 September 2026	Final draft	Launch-ready public policy aligned to Redline's Microsoft 365 environment, Scorecard, CRM, prospecting, client delivery model and Data Processing Schedule.