Privacy & Secure Client Communications

Last updated: **28 June 2026**

This page sets out (A) our Privacy Policy and (B) our Client Secure Portal Policy.

Contents

A. Privacy Policy

1. Introduction.

Durelli Advisory Ltd ("the Company", "we", "us") is committed to protecting the privacy and personal data of visitors to its website and clients who engage with its services.

The Company is incorporated in England and Wales and processes personal data in accordance with applicable data protection laws, including the UK General Data Protection Regulation ("UK GDPR") and, where applicable, the EU General Data Protection Regulation ("GDPR").

The Company acts as a **data controller** in respect of personal data processed in connection with our website and advisory services.

The Company is registered with the UK Information Commissioner's Office (ICO) under the Data Protection (Charges and Information) Regulations 2018. **ICO Registration reference:** ZC073336.

2. Contact details

Post:

Data Protection Officer
Durelli Advisory Ltd
167-169 Great Portland Street,
5th Floor,
London, W1W 5PF, GB

Email:

info@durelliadvisory.com

3. How we collect personal data

We collect personal data in the following ways:

· when you contact us via our website or email;
· when you book an appointment using an online booking platform;
· when you engage us for advisory services;
· when you communicate with us during the course of a professional relationship;
· automatically, through limited technical data generated by website use.

4. What information we collect, use, and why

Depending on the context, we may collect and process the following categories of personal data:

(a) Contact and communication data

· name;

· email address;

· information you voluntarily provide in correspondence or enquiries.

(b) Appointment and booking data

· name and surname;

· email address;

· appointment details.

Booking is facilitated through third-party platforms (such as Google Calendar), which collect this information directly from you.

(c) Client and advisory engagement data

· contact details;

· information relevant to the provision of advisory services;

· documents, correspondence, and (where relevant) identification documents shared in connection with an engagement.

(d) Identity verification data

Where appropriate, before accepting instructions or continuing to act for a client, we may require prospective or existing clients to complete an identity verification process. The identity verification process may involve the processing of:

· identity documents;
· photographs;
· facial recognition and biometric comparison data;
· liveness detection data;
· video recordings created during the verification process;
· verification reports generated by our identity verification provider.

We use a specialist third-party identity verification provider acting as our data processor to carry out this process on our behalf.

Identity verification records form part of the client's matter file and are retained in accordance with the Company's internal document retention policies.

We only request identity verification where appropriate having regard to the nature of the engagement, our legitimate interests, our professional obligations or applicable legal requirements.

Further information regarding our identity verification provider may be provided upon request.

(e) Operation of client or customer accounts

· Names and contact details
· Account information, including registration details

(f) Payment-related data

· limited payment information necessary to process fees, handled by third-party payment service providers.

The Company does not store or process full payment card details on its own systems.

(g) To comply with legal requirements:

· Name
· Contact information
· Identification documents
· Any other personal information required to comply with legal obligations

(h) Dealing with queries, complaints or claims:

· Names and contact details
· Addresses
· Payment details
· Account information
· Financial transaction information

(i) Technical data

· IP address;
· browser type;
· basic usage data collected for security and functionality purposes.

We use personal data for the following purposes:

· to respond to enquiries and communications;
· to schedule and manage consultations and meetings;
· to provide advisory and consultancy services;
· to administer client relationships and internal records;
· to process payments and invoices;
· to comply with legal, regulatory, and professional obligations;
· to ensure website security and functionality.

5. Lawful bases and data protection rights

Under UK data protection law, we must have a "lawful basis" for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO's website.

Which lawful basis we rely on may affect your data protection rights which are set out in brief below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:

· Your right of access - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. Read more about the right of access.

· Your right to rectification - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. Read more about the right to rectification.

· Your right to erasure - You have the right to ask us to delete your personal information. Read more about the right to erasure.

· Your right to restriction of processing - You have the right to ask us to limit how we can use your personal information. Read more about the right to restriction of processing.

· Your right to object to processing - You have the right to object to the processing of your personal data. Read more about the right to object to processing.

· Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. Read more about the right to data portability.
· Your right to withdraw consent – When we use consent as our lawful basis you have the right to withdraw your consent at any time. Read more about the right to withdraw consent.
If you make a request, we must respond to you without undue delay and in any event within one month.

To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

6. Our lawful bases for the collection and use of your data
Our lawful bases for collecting or using personal information for the operation of client or customer accounts are:
· **Consent** - where you have provided it (for example, when submitting an enquiry). All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time;
· **Contractual necessity** - we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object;
· **Legitimate interests** - where processing is necessary for the operation of our advisory practice and does not override your rights;
· **Legal obligation** - where processing is required by law or regulation.
The lawful basis relied upon will depend on the specific context in which personal data is processed.

7. How long we keep personal data

We retain personal data only for as long as necessary for the purposes for which it was collected, taking into account:

· the nature of the data;

· the context of the relationship;

· legal, regulatory, and professional obligations.

Retention periods vary depending on the category of data and the purpose of processing.

8. Who we share personal data with

We may share personal data, where necessary, with:

· technology and communications service providers (including Google Workspace and Google Calendar);

· secure document storage and file-sharing platforms;

· identity verification service providers;

· payment service providers;

· professional advisers;

· regulatory or public authorities where legally required.

Personal data is **not sold or shared for marketing purposes**.

Principal data processors

· *Google Workspace (cloud-based IT and communications services provider; technology sector; UK\/EEA\/international)*

This data processor does the following activities for us: Provides cloud-based email, calendar, document storage and collaboration tools used to manage business communications, scheduling, and internal documentation.

· *Stripe (payment processing services provider; financial technology sector; international)*
This data processor does the following activities for us: Processes payments for services provided by the Company, including handling payment card transactions and related payment information.

· *Box (Cloud-based document storage and secure file-sharing service provider (technology sector)*
This data processor does the following activities for us: Provides secure cloud-based document storage and file-sharing services used to store and exchange client documents and related business records.

· *Kaseya (Spanning Backup for Google Workspace)* (cloud-based data backup and disaster recovery services provider (technology sector; operating internationally).
This data processor does the following activities for us: Provides automated backup and recovery services for business data stored in cloud-based systems, including email and documents, for data protection and business continuity purposes.

· *Didit (Identity verification and fraud prevention services provider; technology sector; EEA/international)*
This data processor carries out identity verification, document authenticity checks, biometric comparison, liveness detection and fraud prevention services on behalf of

the Company where identity verification is required as part of the client onboarding process.

Sharing information outside the UK

Some of the Company's service providers operate internationally. As a result, personal data may be processed outside the UK by those providers.

Where applicable, such transfers are made subject to appropriate safeguards in accordance with UK GDPR, including the use of standard contractual clauses together with the UK Addendum.

Further information about applicable safeguards may be obtained by contacting us.

9. How we keep personal data secure

We implement appropriate technical and organisational measures to protect personal data, including:

· secure hosting and encrypted connections;

· restricted access controls;

· secure email, document management, and file-sharing systems.

10. Third-party websites and platforms

Our website may contain links or redirections to third-party websites or platforms (including booking systems).

We are not responsible for the privacy practices of those third parties, and you are encouraged to review their privacy notices and terms.

11. How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

You also have the right to lodge a complaint with the UK Information Commissioner's Office (ICO):
The ICO's address:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113
Website: https://www.ico.org.uk/make-a-complaint

12. Updates to this notice

This Privacy Notice may be updated from time to time to reflect changes in legal requirements or business practices. The most current version published on the website applies.

Cross-reference
For information on how client documents are shared securely, please see Section B – Client Secure Portal Policy.

B. Client Secure Portal Policy

1. Purpose of this Policy

This policy explains how the Firm provides secure access to client documents using third-party cloud-based document management and sharing platforms, and the safeguards applied to protect confidentiality, integrity, and availability of client information.

The Company does not operate a bespoke or proprietary client portal system. Instead, it uses reputable third-party secure document platforms that provide controlled, access-restricted environments appropriate to the nature of the services provided.

2. Secure Document Platform

The Company uses a secure, cloud-based document management platform operated by a third-party provider to share and store client documents.

The platform provides encrypted storage, permission-based access controls, and user account authentication to support the secure exchange of documents.

3. Access Controls

Client documents are made available only to authorised users through individual user accounts or explicitly invited external collaborators.

Access controls include, as applicable:

• unique user authentication credentials;

• password protection and account security measures;

• role-based permissions (such as view, upload, edit, or download);

• the ability to revoke access at any time.

Access is granted strictly on a need-to-know basis and limited to the specific documents or folders relevant to the client engagement.

4. External Client Access

Clients may be granted access to specific folders or documents within the secure platform.

External access may be provided by:

• invitation to collaborate using an email address; or

• secure sharing links with configurable restrictions (such as access limitations or expiry).

Clients are responsible for maintaining the confidentiality of their login credentials and for ensuring that any access granted on their side is appropriately controlled.

5. Security Measures

The Firm relies on the security features provided by the platform, which include:

• encryption of data in transit and at rest (using platform-managed encryption);

• secure data centres operated by the platform provider; and

• standard availability, integrity, and backup protections.

The Firm does not manage or control encryption keys directly and does not provide client-specific cryptographic key management.

6. Monitoring and Audit

The Firm may review basic activity information available within the platform to manage access and ensure appropriate use.

The platform is not used as a regulatory audit or forensic monitoring system, and the Firm does not represent that it provides enterprise-grade audit logging, data loss prevention, or regulatory compliance dashboards.

7. Appropriate Use and Limitations

The secure document platform is intended for the exchange and storage of professional documentation relevant to the Firm's advisory services.

It is not intended to function as:

- a banking platform;
- a regulated transaction system; or
- a client-side document management system under the client's sole control.

Clients should retain their own copies of documents for record-keeping purposes.

8. Data Protection

The use of the secure document platform forms part of the Firm's data processing activities and is subject to the Firm's Privacy Policy.

The platform provider acts as a data processor, and the Firm applies appropriate technical and organisational measures in line with applicable data protection laws, including the UK GDPR, taking into account the nature, scope, and risk profile of the services provided.

9. Changes to This Policy

The Firm may update or change the secure document platform or related procedures from time to time. Any material changes will be reflected in an updated version of this policy.

Cross-reference

This policy should be read together with the Privacy Policy above.