

AA Compliance Compass Ltd Privacy & Data Protection Policy

1. Introduction

AA Compliance Compass Ltd ("AA Compliance Compass", "we", "us" or "our") is committed to protecting the privacy, confidentiality, integrity and security of the personal and business information entrusted to us.

This Privacy & Data Protection Policy explains how we collect, use, store, protect, share and dispose of information obtained through our website, enquiries and the professional services we provide.

Our services may require us to handle both **personal data** relating to identifiable individuals and **business or commercially confidential information** belonging to clients, suppliers, contractors and other organisations.

We process personal data in accordance with applicable UK data protection legislation, including:

- **UK General Data Protection Regulation (UK GDPR);**
- **Data Protection Act 2018;**
- **Data (Use and Access) Act 2025**, including amendments made to the UK's data protection framework; and
- **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)**, where applicable to electronic communications, direct marketing, cookies and similar technologies.

The Data (Use and Access) Act 2025 came into law on 19 June 2025 and has made changes to the UK data protection framework. ([ICO](#))

2. Who We Are

AA Compliance Compass Ltd provides business consultancy, compliance and management-system support services, which may include:

Business consultancy and strategy; ISO management system support; internal auditing and management reviews; policies and procedures; HR documentation and business processes; financial, bookkeeping, cashflow and business planning support; FORS and Operator's Licence support; Constructionline, Achilles and other accreditation support; grant and funding applications; and associated consultancy services.

For personal information that we determine the purpose and means of processing, **AA Compliance Compass Ltd acts as the Data Controller.**

Where we process personal information solely on behalf of a client and under their instructions, we may act as a **Data Processor.**

3. Information We May Collect

Depending upon your relationship with us and the services you request, we may collect and process information including:

Personal information: name, job title, telephone number, email address, postal address, correspondence and other contact information.

Business information: company name, registered and trading addresses, company registration details, VAT information, organisational structures, policies, procedures, management systems, audit information, accreditation information and operational records.

Financial information: invoices, transaction information, bookkeeping records, cashflow information, budgets and other financial information where required to provide contracted services.

Employment and HR information: employee information, employment documentation, training and competency records, absence information and other HR documentation where we have been engaged to provide relevant services.

Compliance information: audit evidence, risk assessments, policies, procedures, registers, management review information, ISO documentation, FORS and transport compliance records, Constructionline/Achilles information and other evidence supplied for consultancy purposes.

Website and technical information: IP address, browser information, device information, website usage information and cookies or similar technologies where applicable.

We will only request information that is reasonably necessary for the purpose for which it is being collected.

4. Special Category Personal Data

Certain consultancy assignments may result in us receiving information classified as **special category personal data** under the UK GDPR.

This can include information concerning health, racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetic or biometric information, political opinions, sex life or sexual orientation.

Where such information is processed, we will ensure that an appropriate lawful basis and, where required, an appropriate condition under **Article 9 UK GDPR and the Data Protection Act 2018** applies.

We will apply additional safeguards to information of this nature.

5. How We Obtain Information

Information may be obtained:

- directly from you by telephone, email or other communications;
- during consultations, meetings or audits;
- through contracts and engagement documentation;
- from employees or authorised representatives of client organisations;
- from suppliers, subcontractors and professional advisers;
- through documentation provided to us for consultancy, auditing or compliance purposes;
- from publicly available sources, including Companies House and company websites, where lawful and appropriate; and
- through website technologies and analytics, where applicable.

Where personal information is obtained from another source, we will comply with the applicable UK GDPR transparency requirements. The ICO states that privacy information will generally need to be provided within a reasonable period and no later than one month where personal data is obtained from another source, subject to applicable exceptions. ([ICO](#))

6. How We Use Information

We may process information to:

Provide quotations and respond to enquiries; enter into and manage contracts; provide consultancy and professional services; conduct audits, reviews and gap analyses; develop management systems, policies and procedures; provide business planning and financial support; assist with accreditations and applications; maintain client and supplier relationships; manage invoices and accounts; meet legal, regulatory, contractual and professional obligations; maintain appropriate business records; prevent fraud and protect our business; improve our website and services; and communicate information about our services where permitted by law.

We will not use personal information for purposes incompatible with the purpose for which it was originally collected unless permitted by law.

7. Our Lawful Bases for Processing

Under the UK GDPR, we must have a lawful basis for processing personal information.

Depending on the circumstances, we may rely upon:

Contract – where processing is necessary to enter into or perform a contract with you.

Legal obligation – where processing is necessary to comply with a legal or regulatory requirement.

Legitimate interests – where processing is necessary for our legitimate business interests or those of a third party, provided those interests are not overridden by your rights and freedoms.

Consent – where you have freely given specific and informed consent to a particular use of your information.

Vital interests or public task – where applicable in the limited circumstances provided for under the UK GDPR.

The appropriate lawful basis will depend upon the purpose and circumstances of the processing.

8. Business and Commercially Confidential Information

Not all information relating to a business constitutes "personal data" under the UK GDPR. However, AA Compliance Compass recognises that clients may provide us with highly confidential or commercially sensitive business information.

This may include financial records, pricing, contracts, business plans, intellectual property, management systems, audit findings, operational processes, tender information, supplier information, employee-related records and strategic information.

We will protect such information through appropriate **confidentiality, contractual, information-security and access-control measures**, regardless of whether the information falls within the statutory definition of personal data.

We will only use client business information for the purpose for which it has been supplied or as otherwise agreed with the client.

9. Sharing Your Information

We do not sell personal information.

We may share information where reasonably necessary with trusted service providers, professional advisers, IT or cloud service providers, accountants, subcontractors or other parties involved in providing our services.

Information may also be disclosed where required by law, regulation, court order or a competent regulatory or enforcement authority.

Where another organisation processes personal data on our behalf, appropriate contractual and data-protection arrangements will be used where required.

10. International Data Transfers

Some technology or cloud service providers may process information outside the United Kingdom.

Where personal information is transferred internationally, we will take reasonable steps to ensure that an appropriate lawful transfer mechanism and safeguards are in place as required by UK data protection legislation.

11. Data Security

We take reasonable and proportionate technical and organisational measures to protect information against:

Unauthorised access; accidental loss; alteration; disclosure; destruction; misuse; and unlawful processing.

Measures may include password protection, access controls, secure devices, secure cloud storage, appropriate backup arrangements, confidentiality controls and restrictions on access according to business need.

Our approach reflects the **data protection by design and by default** principles.

12. How Long We Keep Information

We will retain personal and business information only for as long as reasonably necessary for the purpose for which it was collected, including satisfying legal, accounting, contractual, insurance and regulatory requirements.

Retention periods may therefore vary according to the nature of the information and the services provided. See retention policy AACC 115.

When information is no longer required, it will be securely deleted, destroyed or anonymised where appropriate.

13. Your Data Protection Rights

Depending upon the circumstances and lawful basis used, UK data protection legislation may give you rights including:

the right to be informed about how your information is used; access to personal information held about you; correction of inaccurate or incomplete information; erasure of information in certain circumstances; restriction of processing; objection to certain processing; data portability where applicable; and rights relating to certain automated decision-making.

Where processing relies upon consent, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing undertaken before consent was withdrawn.

The ICO requires organisations to explain these rights as part of the privacy information provided to individuals. ([ICO](#))

14. Direct Marketing

We may contact existing or prospective clients regarding our services where permitted by applicable data protection and electronic marketing legislation.

Where consent is required, we will obtain it before sending the relevant marketing communication.

You may ask us to stop sending marketing communications at any time.

Electronic marketing activities will be undertaken with regard to the requirements of **PECR and UK data protection legislation**. ([ICO](#))

15. Cookies

Our website may use cookies and similar technologies to operate correctly, maintain security, remember preferences and, where applicable, understand how visitors use our website.

Where cookies or similar technologies are not strictly necessary and consent is legally required, they should not be activated until the visitor has provided the appropriate consent.

The ICO states that organisations must provide clear information about cookies and obtain consent where required; strictly necessary cookies may be exempt from the consent requirement. ([ICO](#))

A separate **Cookie Policy** may provide further details about the cookies used by this website.

16. Data Breaches

AA Compliance Compass maintains procedures for identifying, assessing, containing and managing suspected personal data breaches.

Where a breach meets the applicable statutory threshold, we will notify the **Information Commissioner's Office (ICO)** and affected individuals where required by UK data protection legislation.

17. Third-Party Websites

Our website may contain links to third-party websites.

AA Compliance Compass Ltd is not responsible for the privacy practices or content of external websites. Visitors should review the privacy notices of those organisations before providing personal information.

18. Changes to This Policy

We may update this Privacy & Data Protection Policy to reflect changes to our services, business practices or applicable legislation.

The latest version will be published on our website and the "Last Updated" date amended accordingly.

19. Contacting Us

If you have questions about this policy, wish to exercise your data protection rights or have concerns regarding how your personal information has been handled, please contact:

AA Compliance Compass Ltd

Data Protection Contact: Managing Director

Website: compliance-compass.co.uk

Email: anne.ashman@compliance-compass.co.uk

20. Complaints to the Information Commissioner's Office

If you are dissatisfied with how we have handled your personal information, you have the right to raise a complaint with the **Information Commissioner's Office (ICO)**, the UK's independent data protection regulator.

[Information Commissioner's Office](#)

We would appreciate the opportunity to address your concerns directly before you contact the ICO, although this does not affect your right to make a complaint.

ICO Number: ZC205898