



Privacy Notice

This Privacy Notice explains how striveX Ltd ("we", "us" or "our") collects, uses, stores, shares and protects personal data.

We process personal data in accordance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 and other applicable data protection legislation.

1. Who We Are

For the purposes of applicable data protection legislation, the data controller is:
striveX Ltd

Address: striveX Ltd, Beacon House, Ibstone Road, Stokenchurch, High Wycombe, Buckinghamshire, HP14 3FE

Email: info@strivex.co.uk

Telephone: 01628 965760

ICO registration number: ZA468196

Data protection contact: Charlotte Bell

If you have questions about this Privacy Notice or how we process personal data, please contact us using the details above.

2. Whose Personal Data We Process

In providing our services and operating our business, we may process personal data relating to:

- clients and prospective clients;
- directors;
- shareholders;
- partners;
- trustees;
- beneficiaries;



Persons with Significant Control;
employees and workers;
contractors;
customers and suppliers of our clients;
professional advisers;
representatives and authorised contacts; and
other individuals whose information is relevant to the services we provide.

Where a client provides personal data relating to another person, the client should ensure that it is entitled to provide that information to us and, where appropriate, that the individual has been informed about the processing of their personal data.

3. Personal Data We Collect

The personal data we process depends upon the nature of our relationship with you and the services being provided.

It may include:

Identity and Contact Data

name;
date of birth;
residential or business address;
email address;
telephone number;
National Insurance number;
Unique Taxpayer Reference
passport information;
driving licence information; and
other identification information.

Financial and Tax Data

bank account details;
accounting records;
income and expenditure;
assets and liabilities;



tax information;
investment information;
pension information;
payroll and employment information; and
financial transactions.

Business and Corporate Data

company and business information;
directorships;
shareholdings;
partnership interests;
beneficial ownership;
Persons with Significant Control;
company registration information; and
business transactions.

Verification and Compliance Data

identity-verification information;
anti-money laundering information;
beneficial-ownership information;
sanctions-screening results;
politically exposed person information;
source-of-funds information;
source-of-wealth information; and
information required for legal or regulatory compliance.

Technical and Usage Data

Where applicable, we may collect:
IP addresses;
device and browser information;
login information;
client-portal activity;
website usage information;
electronic acceptance records; and
security and audit logs.

Special Category and Other Sensitive Data

In some circumstances, information supplied to us in connection with professional services may include special category personal data or other sensitive information.

We will process such information only where there is an appropriate lawful basis and, where required, an additional condition permitting the processing.

Where criminal-offence data is processed, we will do so only where permitted by applicable law.

4. How We Collect Personal Data

We may obtain personal data directly from you;
from your employees, officers, representatives or advisers;
from HM Revenue & Customs;
from Companies House;
from banks and financial institutions;
from identity and electronic-verification providers;
from government bodies and regulators;
from professional advisers;
from publicly available sources;
from accounting, payroll and other software platforms;
through our website, client portal and communications systems; and
from other sources where necessary to provide our services or comply with our obligations.

5. How We Use Personal Data

We may process personal data for the following purposes.

Providing Professional Services Including:

preparing accounts and financial statements;
tax compliance and advisory services;
VAT services;
payroll services;
bookkeeping;



company secretarial services;
business and financial advisory services; and
other services agreed with our clients.

Legal, Regulatory and Professional Compliance Including:

anti-money laundering checks;
identity verification;
sanctions and politically exposed person screening;
Companies House requirements;
tax and company-law obligations;
professional-body requirements;
responding to regulators and competent authorities; and
establishing, exercising or defending legal rights.

Managing Our Relationship With Clients Including:

communicating with clients;
managing engagements;
administering services;
issuing invoices and collecting fees;
maintaining client records;
dealing with queries and complaints; and
managing the termination or transfer of engagements.

Operating and Improving Our Business Including:

quality assurance;
staff training;
internal administration;
risk management;
information security;
fraud prevention;
service development;
improving business processes and technology; and
monitoring the performance and effectiveness of our systems and services.

6. Lawful Bases for Processing

Depending upon the circumstances, we may rely upon one or more of the following lawful bases under UK GDPR.

Contract

Where processing is necessary to enter into or perform a contract with an individual.

Legal Obligation

Where processing is necessary for us to comply with a legal obligation.

Legitimate Interests

Where processing is necessary for our legitimate interests or those of a third party and those interests are not overridden by the individual's rights and interests.

Our legitimate interests may include:

- operating and administering our business;
- delivering and improving professional services;
- protecting our business and systems;
- managing risk;
- recovering amounts owed to us; and
- establishing, exercising or defending legal rights.

Consent

We may rely upon consent where appropriate and where another lawful basis does not apply. Where processing is based upon consent, consent may be withdrawn at any time. Withdrawal does not affect the lawfulness of processing carried out before consent was withdrawn.

Special Category and Criminal-Offence Data

Where we process special category personal data or criminal-offence data, we will ensure that an appropriate legal condition applies in addition to any other requirements imposed by applicable law.

7. Anti-Money Laundering and Identity Verification

We are subject to legal and regulatory obligations concerning anti-money laundering, counter-terrorist financing, sanctions and related matters.

We may therefore process personal data for purposes including:

- verifying identity;
- identifying and verifying beneficial owners;
- sanctions screening;
- politically exposed person screening;
- assessing risk;
- establishing source of funds or source of wealth where appropriate; and
- ongoing monitoring.

We may use third-party electronic verification and screening providers for these purposes.

We may also be required by law to retain information after our professional relationship has ended and, in certain circumstances, to make disclosures to competent authorities.

8. Artificial Intelligence, Automation and Technology

We may use software, automation, artificial intelligence and machine-learning technologies to assist in operating our business and delivering professional services.

Depending upon the system and purpose, these technologies may assist with activities including:

- extracting and organising information;
- document preparation and drafting;
- reviewing or summarising information;
- workflow automation;
- research;
- administrative processes;
- quality control; and
- improving efficiency and consistency.

Where personal data is processed using such technology, we will take appropriate steps having regard to the nature, purpose and risks of the processing.

We remain responsible for ensuring that our processing of personal data complies with applicable data protection legislation.

Use of artificial intelligence or automated technology to assist our work does not remove the responsibility of appropriately qualified personnel for professional judgement and final professional outputs.

9. Automated Decision-Making

We do not ordinarily make decisions producing legal or similarly significant effects on individuals solely by automated means.

If we undertake such processing in circumstances where UK GDPR gives an individual specific rights in relation to automated decision-making, we will provide the information and safeguards required by law.

10. Who We Share Personal Data With

Where necessary and lawful, we may share personal data with third parties including:

Government, Regulatory and Professional Bodies Such as

HM Revenue & Customs;
Companies House;
the Information Commissioner's Office;
law-enforcement agencies;
courts and tribunals
our professional body or supervisory authority; and
other competent authorities.

Service Providers Such as providers of

accounting and tax software;
payroll software;
practice-management systems;

client portals;
electronic signature systems;
identity-verification and screening services;
cloud hosting and storage;
payment services;
communications systems;
cyber-security services;
automation and artificial-intelligence systems; and
other technology used in operating our business or providing services.

Where a service provider processes personal data on our behalf, we will take appropriate steps to ensure that the processing is subject to suitable contractual and data-protection safeguards.

Professional Advisers and Specialists Such as:

solicitors;
barristers;
tax specialists;
auditors;
consultants;
insurers and insurance advisers; and
other specialists engaged where necessary.

We will only disclose personal data where there is an appropriate purpose and lawful basis for doing so.

11. International Transfers

Some organisations that process personal data on our behalf may be located outside the United Kingdom or may use infrastructure located outside the United Kingdom.

Where personal data is transferred to a country or recipient not covered by applicable UK adequacy regulations, we will ensure that an appropriate transfer mechanism or safeguard is used where required by law.

This may include:

- an applicable UK adequacy regulation;
- the UK International Data Transfer Agreement;
- the UK Addendum to approved EU Standard Contractual Clauses; or
- another transfer mechanism permitted under applicable data protection legislation.

Where required, we will also consider whether additional safeguards are necessary having regard to the circumstances of the transfer.

12. Data Retention

We retain personal data only for as long as reasonably necessary for the purposes for which it was collected and to meet applicable legal, regulatory, professional, contractual and risk-management requirements.

The appropriate retention period depends upon the nature of the information and the reason it is held.

In determining retention periods, we may consider:

- statutory record-retention requirements;
- anti-money laundering requirements;
- tax and company-law requirements;
- professional-body requirements;
- limitation periods for legal claims;
- insurance and risk-management requirements; and
- the nature and sensitivity of the information.

Certain anti-money laundering records are generally required to be retained for prescribed statutory periods following the end of the relevant business relationship or transaction.

Client and engagement records may be retained for longer where reasonably necessary to comply with other legal or professional obligations or to establish, exercise or defend legal claims.

At the end of the applicable retention period, personal data will be securely deleted, destroyed or anonymised where appropriate.

13. Data Security

We maintain appropriate technical and organisational measures designed to protect personal data against:

- unauthorised or unlawful access;
- accidental loss;
- destruction;
- alteration;
- inappropriate disclosure; and
- misuse.

Measures may include access controls, authentication, encryption, secure storage, backups, monitoring, staff training and supplier-management procedures, as appropriate to the risks involved.

No information system can be guaranteed to be completely secure.

14. Your Data Protection Rights

Depending upon the circumstances, you may have the right to:

- request access to personal data we hold about you;
- request correction of inaccurate or incomplete personal data;
- request deletion of personal data;
- request restriction of processing;
- object to certain processing;
- request portability of certain personal data;
- withdraw consent where processing is based upon consent; and
- exercise rights relating to certain automated decision-making.

These rights are subject to conditions and exemptions under applicable law and will not apply in every circumstance.

We may need to verify your identity before responding to a request.

To exercise a data-protection right, contact us using the details in section 1.

15. Marketing

Where we send electronic direct marketing, we will do so in accordance with applicable data-protection and electronic-marketing legislation.

Where consent is required, we will obtain it.

You may opt out of receiving direct marketing communications at any time by using the unsubscribe method provided or contacting us.

Service and administrative communications relating to an existing engagement are not marketing communications.

16. Complaints

If you have concerns about how we process your personal data, please contact us in the first instance using the details in section 1.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK's data-protection supervisory authority.

Information about making a complaint is available from the ICO.

17. Changes to This Privacy Notice

We may update this Privacy Notice periodically to reflect changes in our business, services, technology, legal requirements or data-processing activities.

The current version will be made available through our Client Portal.

Where appropriate, we will bring material changes to your attention.



18. Contact Us

Questions concerning this Privacy Notice or our processing of personal data should be directed to:

Charlotte Bell
striveX Ltd

Email: info@strivex.co.uk

Telephone: 01628 965760

Address: striveX Ltd, Beacon House, Ibstone Road, Stokenchurch, High Wycombe, Buckinghamshire, HP14 3FE