LAWYERLY®

The 2026 Legal Playbook for Tech & AI Businesses

Build fast. Build right. Build to last.
Created for tech leaders who build successful companies.

Tech Industry

LAWYERLY®

Playbook **content**

Introduction

Legal work rarely sits at the top of a tech founder's priority list, and for understandable reasons. There is always something else demanding attention: the product, the next customer, the next hire, the next demo, the next raise. In the moment, tidying up the legal side later can feel like the more practical option.

Most legal gaps stem from quick decisions made to keep the business moving. They do not look serious when they first appear. It is only later, when the company comes under proper scrutiny, that those gaps become visible and the consequences start to matter. By then, they can complicate funding rounds, weaken negotiating positions in commercial deals, and unsettle buyers at the moment the business needs to project confidence.

Most of this is avoidable. This playbook shares the legal gaps our tech solicitors see most often in practice, and the steps that help prevent them. It is designed to help founders understand what to prioritise, what to fix early, and how to build their company in a way that supports growth, funding and exit.

/01
Why tech & AI founders need to think about legal earlier

A tech company creates legal risk at the same time as it creates value. The risk sits in everyday decisions: who writes the code, who owns the intellectual property, what data is used, which tools the team relies on, what the product promises customers and which markets the company sells into.

Those decisions may feel practical in the moment, but later they may be reviewed by investors, customers, buyers or regulators who are looking at them through a very different lens. The earlier those decisions are handled properly, the more control the company keeps when someone else starts asking questions.

AI companies have an additional layer to manage. Training data, copyright, privacy, bias, transparency, model outputs and user safety all raise questions that need to be handled early, especially where customers outside the United Kingdom use the product. The rules are still developing, which means founders need to keep this area under active review.

Please note:

The European Union (EU) AI Act is being introduced in stages. Some rules are already in force. Prohibited AI practices and AI literacy obligations have applied since **2 February 2025**, while general-purpose AI obligations have applied since **2 August 2025**.

Broader responsibilities are still developing, with EU lawmakers provisionally agreeing to delay enforcement of some high-risk rules until **December 2027**. Maximum penalties under the Act can reach **€35 million** or **7% of global turnover**.

For UK AI businesses with EU customers, users or outputs, this is not something to ignore until later. The question is not only whether the company is based in the EU, but whether the system is being placed on the EU market, used in the EU or relied on by EU customers.

LAWYERLY®

/02
The legal gaps that create the biggest problems

2.1 The company does not clearly own its intellectual property

For most tech businesses, the value sits in the product: the code, data, brand, know-how, systems and customer relationships that make the company commercially valuable. That is why investors and buyers look at intellectual property ownership early.

A common mistake is assuming that because someone built something for the company, the company automatically owns it. That is not always the case.

If a founder wrote code before the company was incorporated, the intellectual property may still sit with the founder personally unless it has been assigned to the company. If a contractor, agency, developer, designer, data scientist, machine learning engineer or advisor helped build the product, the company needs a proper written assignment.

A clean setup should include:

- **Founder IP assignments.** Anything created before incorporation should be transferred into the company properly.
- **Contractor and consultant agreements.** Every contractor should sign before work starts. The agreement should cover confidentiality, IP assignment, moral rights waivers and further assurance obligations.
- **Employee contracts with IP clauses.** Employment contracts should make clear that work created in the role belongs to the company.
- **Open-source controls.** Founders should know which open-source licences sit inside the product, particularly copyleft licences like the GNU General Public License (GPL) and Affero General Public License (AGPL).
- **An IP register.** Keep a practical record of software, trade marks, patents, domains, datasets, AI models, licences, third-party tools and other significant technical assets.

Ask this question:

The founders who handle this well can answer one important question: **does the company own what it is selling?** The answer should be easy to prove.

2.2 The cap table and funding documents create problems

The Seed Enterprise Investment Scheme (SEIS), Enterprise Investment Scheme (EIS) and Enterprise Management Incentive (EMI) are some of the most useful tools available to UK startups. They can help founders raise investment, attract talent and reward employees in a tax-efficient way.

Problems usually start with the wrong paperwork: the wrong investment document, the wrong share class, investor rights that do not work for SEIS or EIS, a United States-style Simple Agreement for Future Equity (SAFE) that has not been adapted for the UK, or EMI options granted without the right approvals, records and His Majesty's Revenue and Customs (HMRC) valuation process.

The cap table matters just as much. Early decisions that feel small can create friction later: too many small angel investors with full pre-emption rights, advisor equity with no written agreement or vesting, advance subscription agreements or convertibles that are not properly tracked, or option pools that have not been approved.

None of this feels urgent in the early stages. By Series A, though, investors expect a clean, fully diluted cap table that ties back to the company's records. If it does not, it raises questions about how carefully the rest of the business is being run.

The risk is not only technical. SEIS can give angel investors valuable tax relief, including 50% income tax relief on qualifying investments. EIS can offer 30% income tax relief on qualifying investments. If investors believe that relief is at risk, they may slow down, renegotiate or walk away.

A messy cap table, unclear investment documents or avoidable tax-relief risk can make the current round, and every round that follows, harder.

Before raising, get advice on:

- **Advance assurance.** Where SEIS or EIS are part of the funding strategy, deal with this before issuing shares.
- **Share class design.** Keep the structure clean and avoid rights that could undermine tax relief.
- **ASAs and SAFEs.** UK advance subscription agreements need careful drafting. US-style SAFEs are often unsuitable without changes.
- **Use of funds.** Investment funds should be spent on qualifying activities.
- **Investor rights.** Be careful with redemption rights, preferential rights and any arrangement that could look like value extraction.
- **EMI options.** Set EMI up properly. Get the valuation. Grant options clearly. Keep records.

The practical lesson is to treat investment paperwork less like admin and more like the company's investment story. Good funding documents make the next raise easier.

LAWYERLY®

/03
Data, AI & compliance

Data protection, AI governance, cyber security and consumer compliance are often pushed into the future. For tech and AI businesses, they become relevant as soon as the company starts collecting, analysing or using data.

From that point, privacy becomes part of the product, the customer relationship and the risk picture investors will look at.

For AI businesses, the compliance picture is wider because data, model behaviour, customer promises and product risk are closely connected. This affects how the product is built, what the public should know, what contracts should cover and what evidence investors or buyers will expect during due diligence.

At an early stage, the privacy and compliance foundation should cover the basics:

- **A privacy notice people can actually understand.** It should cover what data is collected, why, how it is used, who it is shared with and what rights people have.
- **Cookie notice and consent setup**, especially where the business uses analytics, tracking, remarketing or product behaviour tools.
- **A record of processing activities,** giving the business a practical map of the personal data it processes.
- **Data processing agreements** with processors, sub-processors and customers where needed.
- **Data protection impact assessments (DPIAs) for higher-risk processing,** particularly AI, automated decision-making, sensitive data, children's data and large-scale monitoring.
- **An AI register** covering which tools are used, what data they process, what risk they create and who is responsible, classified by risk tier.
- **A breach response process,** so the team knows what to do if customer data is exposed.

Please note:

The Data Use and Access Act 2025 is being introduced in stages, but most of its key data protection provisions are already in force. The first provisions came into force on **19 and 20 August 2025**, followed by further data protection changes on **5 February 2026**. Some complaints procedure requirements are due to commence on **19 June 2026**.

For founders, the practical point is simple: privacy documents and internal processes should not be treated as static. They need to keep pace with how the product uses data and how the law is changing.

LAWYERLY®

/04
Stage 1: Pre-incorporation & pre-seed

4.1 Set the company up properly before speed creates a mess

This is the stage where founders make decisions that follow the company for years. At pre-incorporation and pre-seed stage, legal work should not feel heavy or over-engineered. The priority is to create clarity around the basics before the business has meaningful revenue.

The key questions are simple:

- Who owns what?
- Who is responsible for what?
- How does equity work?
- What happens if someone leaves?
- Can the company raise investment cleanly?
- Can the company prove it owns the product?

If these questions are answered early, the business has a much stronger foundation.

4.2 Know what mistakes to look out for

Mistakes usually happen at this stage because things feel informal. The team is small, everyone trusts each other, and the priority is growth. That makes sense, but informal decisions can create problems later.

Founders often:

- Split shares equally without thinking about what happens if one founder leaves.
- Start building before checking whether a current or previous employment contract claims ownership over side projects.
- Use friends, freelancers or overseas contractors without written agreements.
- Incorporate with basic model articles and never revisit them.
- Speak to angel investors before checking SEIS or EIS.
- Register a company name before checking trade mark risk.
- Use consumer AI tools with confidential business information.
- Keep major decisions in WhatsApp messages instead of proper company records.

None of these feel serious at the time, but they can quickly become difficult to explain when the company is raising, selling, hiring or signing customers.

4.3 What to put in place

- **Founder agreement.** A founder agreement should cover roles, equity, decision-making, vesting, leaver provisions, IP, confidentiality, restrictive covenants and deadlock. It protects the company if priorities shift or a founder leaves earlier than expected.
- **Reverse vesting.** A founder who leaves after three months should not walk away with a large permanent stake in the company. A four-year vesting schedule with a one-year cliff is common. The exact structure should be tailored, but the principle is the same: equity stays connected to contribution.

- **Founder IP assignments.** If founders created code, designs, brand assets, product concepts, technical architecture, datasets, prompts, models or business materials before incorporation, that IP should be assigned to the company. Do not leave it until the first funding round.
- **Clean company structure.** For most UK tech startups, a private company limited by shares is the right starting point. More complex structures should only be used where there is a clear reason, such as a genuine US investment plan, regulated activity, IP structuring or international expansion.
- **Trade mark clearance.** Check the company name, product name and core brand before investing in design, domain, launch and marketing. A name that looks available at Companies House is not necessarily safe to use as a brand.
- **SEIS and EIS planning.** If angel investment is part of the plan, structure the company and the fundraising properly from the start. This is not something to clean up after shares have already been issued.
- **Basic privacy setup.** Put the basics in place early: a privacy notice, a cookie notice, Information Commissioner's Office registration where required and a simple data map. At this stage, the business needs to know what data it collects and why.
- **AI acceptable use policy.** Even a short internal policy is useful. It should explain which AI tools can be used, what data must not be entered, when human review is required and who approves higher-risk use cases.

Ask this question:

Can the company can prove that it owns the product, the equity is clean and the business is ready to raise? If any of those answers is unclear, fix that before momentum makes it harder.

/05
Stage 2: Seed stage

5.1 Build the legal stack that supports hiring, customers and investment

Seed stage is where the company starts becoming more than an idea. The business may now have employees, contractors, customers, investors, a live product, product data, marketing activity, third-party vendors and revenue.

Legal needs to shift at this point from founder setup to operational protection. The focus moves to giving the business the documents, processes and controls it needs to hire properly, sell confidently, protect the product and raise investment without creating problems.

5.2 Know what mistakes to look out for

When the company grows faster than its paperwork, legal mistakes follow. The team starts selling, hiring and building before the legal foundations have caught up.

Founders often:

- Continue to use informal customer terms.
- Hire people without proper employment contracts.
- Rely on contractors who look a lot like employees.
- Grant equity without setting up EMI properly.
- Copy another company's privacy policy.
- Sign enterprise customer terms without reviewing liability, data and IP clauses.
- Use AI in the product without explaining how outputs should be treated.
- Fail to keep board minutes, shareholder approvals or a clean cap table.
- Collect more data than they need because "it might be useful later".

5.3 What to put in place

- **Employment contracts.** Employment contracts should cover pay, benefits, confidentiality, IP, restrictive covenants, notice, probation, policies and equipment. For a tech company, the IP and confidentiality clauses legally protect the value being created.
- **Contractor agreements.** Use proper agreements with freelancers, developers, designers, data consultants, machine learning engineers, agencies and advisors before work starts. The agreement should cover deliverables, payment, confidentiality, IP ownership, data protection, security, termination and handover.
- **EMI option scheme.** For eligible companies and employees, EMI is usually the most attractive UK share option structure. Set it up properly: get the valuation, approve the scheme, make grants clearly and keep proper records. Do not treat option grants as informal promises.
- **Standard customer contract.** For SaaS and tech companies, this usually means terms of service or a master services agreement, order form, acceptable use terms, support terms, payment terms, IP provisions, liability limits, data protection terms and termination rights. It should be easy enough for sales to use, but strong enough to protect the business.
- **Data processing agreement and privacy documents.** Where the business processes personal data for customers, a proper data processing agreement is needed. The company should also have a privacy notice, cookie notice, record of processing activities, sub-processor list, breach process and data protection impact assessment template.
- **Security schedule.** Enterprise customers will ask about encryption, access controls, multi-factor authentication, hosting, backups, breach notification, sub-processors and incident response. A standard security schedule helps sales move faster because the business is not rebuilding answers for every deal.
- **Open-source policy and software bill of materials.** Know what is in the codebase. An open-source policy and software bill of materials can prevent issues with restrictive licences, customer warranties and future mergers and acquisitions diligence.
- **AI product terms.** If the product includes AI, the position should be clear. What does the AI do? What does it not do? Can outputs be inaccurate? Is human review required? Is customer data used for training? Can the model provider access the data? Who is responsible for how outputs are used? Ambiguity here creates risk.
- **Board and shareholder records.** Keep resolutions, consents, share issuances, option grants and major decisions organised. Clean records make funding and diligence easier later.

Ask this question:

Can your company keep moving forward without legal risk being created at every step? The test at this stage is whether the company can hire, sell and raise without creating avoidable legal risk every time the business takes a step forward.

/06
Stage 3: Series A & growth

6.1 Build the legal structure that helps you scale

By Series A, legal stops being something the business fixes only when there is a problem. It becomes part of how the company wins larger customers, hires better people, expands into new markets and manages risk at scale.

Investors and enterprise customers do not expect perfection at this stage, but they do expect structure. Informal decisions, inconsistent contracts and undocumented risks become harder to explain than they were a year earlier.

6.2 Know what mistakes to look out for

Founders often:

- Underestimate enterprise contracting.
- Accept unlimited liability to win early customers.
- Sign customer procurement terms that override their own terms.
- Ignore international data transfers.
- Expand into the US or EU without checking tax, employment, regulatory or privacy issues.
- Assume AI product is low risk without doing a proper assessment.
- Fail to review whether online safety, financial services, consumer protection or sector-specific rules apply.
- Treat cyber security as an IT issue instead of a board-level risk.

6.3 What to put in place

- **Investor-grade articles and shareholder documents.** Series A usually needs more sophisticated documents: articles, shareholders' agreement, subscription agreement, reserved matters, investor rights, drag and tag provisions, warranties and disclosure. These documents should protect the company without giving investors day-to-day control over operational decisions.
- **Contract playbook.** As deal volume grows, the sales team needs clear guidance on which clauses are acceptable, which require approval and which should be pushed back on. It should cover liability caps, indemnities, data protection, security, payment terms, termination, AI outputs, service levels and governing law.
- **Liability position.** Decide where to cap liability, where a higher cap may be acceptable and what sits outside the cap. Be careful with unlimited liability, broad indemnities, customer-drafted AI clauses and security promises that go beyond what the product can realistically support.
- **Data protection maturity.** The business should now have a more developed privacy setup: record of processing activities, data protection impact assessments, data processing agreements, transfer documents, sub-processor records, breach logs, retention rules and internal privacy responsibilities. The more data-intensive the product, the more important this becomes.
- **AI governance.** AI governance is now part of product credibility. Maintain an AI register, model risk assessments, internal AI use rules, customer-facing AI terms, human oversight processes and documentation around training data, model providers and output risks.

- **Bias and adversarial testing.** Before deployment, AI systems that affect people should be tested for bias and robustness against adversarial inputs, with the results documented. Under the Equality Act 2010, bias in AI-driven decisions can amount to indirect discrimination, and the Information Commissioner's Office expects bias mitigation across the AI lifecycle.
- **Model documentation.** For each AI system the company develops or deploys, maintain a model card or system card describing intended use, performance characteristics, limitations and ethical considerations.
- **EU AI Act review.** If EU customers use the AI system or its outputs, check whether the EU AI Act applies. The regime is being phased in and remains an area to keep under regular review, especially for products that fall into higher-risk categories.
- **Cyber certification roadmap.** Cyber Essentials Plus or ISO 27001 becomes increasingly important when selling to enterprise, government, financial services, health tech or regulated customers. Incident response plans should also cover AI-specific scenarios such as model poisoning, prompt injection, data exfiltration via prompts and adversarial inputs.

Please note:

The Cyber Security and Resilience Bill introduced in November 2025 and progressing through Parliament, will expand the UK's cyber security regime in line with the EU's NIS2 Directive. It extends scope to managed service providers and data-centre operators, introduces **24-hour initial incident reporting** with a **72-hour full report**, and **raises maximum fines to 4% of global turnover**.

- **AI in HR decisions.** If AI is used in recruitment, performance management or disciplinary processes, those tools should be audited for discriminatory bias and meaningful human review should be in place. An AI workplace policy covering acceptable use, confidentiality, data entry restrictions and employee rights is also needed before any disciplinary action relating to employee misuse of AI.
- **Director duties and personal liability.** Founders carry more personal responsibility than they often realise once they become directors. Directors have legal duties under the Companies Act 2006, including duties to act in the company's best interests, use reasonable care, avoid conflicts and make decisions properly. If the company starts facing serious financial pressure, those duties can shift towards protecting creditors.
- **Good governance is not just admin.** Keep board minutes, document major decisions, stay on top of Companies House filings, manage right-to-work checks properly and get advice early if cash flow becomes difficult. From Series A onwards, directors and officers insurance is also worth considering.
- **Fraud and compliance controls.** The Failure to Prevent Fraud offence came into force on 1 September 2025. It applies to larger organisations that meet at least two of three thresholds: more than £36 million turnover, more than £18 million on the balance sheet, or more than 250 employees.

Most early-stage startups aren't in scope yet, but customers, investors, and procurement teams will expect basic fraud controls: approvals, supplier checks, expense policies, whistleblowing channels, training, and clear reporting lines.

- **Companies House and director admin.** Identity verification is now a legal requirement for directors and people with significant control. Existing directors and people with significant control need to verify by their due dates, while new appointments must follow the new verification process. Poor company admin creates unnecessary friction in funding, banking, diligence and governance checks, so keep Companies House records clean and know who needs to verify.
- **Employment and people policies.** As the team grows, internal policies need to keep pace. Put proper policies in place for disciplinary matters, grievances, harassment, whistleblowing, remote work, expenses, information security, data use and AI use. Growing teams should also review employment contracts, restrictive covenants and contractor arrangements regularly, especially as employment law continues to change through 2026 and 2027.

Please note:

The Employment Rights Act 2025 introduces changes around statutory sick pay, family leave, tribunal time limits and "fire and rehire". The government has also reopened the conversation around non-compete clauses, including whether they should be capped.

The test at this stage is whether the business can scale without relying on informal decisions, inconsistent contracts and undocumented risk.

/07 Stage 4: International expansion

7.1 Do not let growth create avoidable tax, data and employment risk

International expansion does not always mean opening an office in another country. It can start much earlier through remote hiring, data stored in another jurisdiction, international suppliers, overseas customers or investment from foreign investors.

Each decision may make commercial sense at the time, but together they can quietly create tax, employment, data, contractual and regulatory obligations before the company has planned for them.

7.2 Know what mistakes to look out for

Founders often:

- Hire globally without checking permanent establishment risk.
- Assume an Employer of Record solves everything.
- Let overseas employees negotiate and sign customer contracts.
- Serve EU users without checking the General Data Protection Regulation (GDPR), AI Act, consumer or sector-specific rules.
- Flip to Delaware too early.
- Ignore local employment law.
- Assume UK contracts work everywhere.
- Sell into regulated sectors without checking licensing or local rules.

7.3 What to put in place

- **International expansion memo.** Before entering a new market, work through the company structure, tax, employment, data, regulatory and contracting issues. This does not need to be overcomplicated, but the business should understand the consequences before making decisions that are difficult to reverse.
- **Permanent establishment review.** Be careful where employees negotiate, sell and sign contracts. A salesperson in another country can create more tax and compliance exposure than founders expect, especially where they have authority to agree terms or close deals on behalf of the company.
- **Employer of record review.** An employer of record can be useful, but it does not remove every risk. The company still needs to understand local employment rules, management responsibilities, IP ownership, confidentiality, data protection, tax exposure and how the relationship works in practice.
- **Local employment advice.** Employment law varies significantly by country. UK contracts and policies are not enough for overseas employees. Local advice is especially important for probation, notice periods, benefits, termination rights, restrictive covenants, working time and mandatory protections.
- **Data transfer structure.** Use the right transfer documents where personal data moves internationally. Check customer requirements around hosting, sub-processors, audit rights, security, data residency and breach notification.
- **US expansion planning.** Decide whether the business needs a US subsidiary, who signs contracts, where revenue sits, how transfer pricing works and whether state-level obligations are triggered.
- **EU compliance review.** For AI, SaaS, marketplaces, consumer apps, healthtech, fintech, edtech or platforms, EU rules may apply even where the company is based in the UK.
- **Delaware flip analysis.** A Delaware flip can make sense when US investment is genuinely driving the next stage. It should not be done casually. It can affect tax, SEIS and EIS, governance, shareholder rights and future structure.

Ask this question:

Is the company expanding with a plan, or creating a trail of one-off decisions it will need to untangle later?

LAWYERLY®

/08
Stage 5: Exit readiness

8.1 Build the company in a way a buyer can trust

Exit readiness starts long before the company starts looking for a buyer. As the business grows, its legal record should stay clean enough for someone else to understand it quickly.

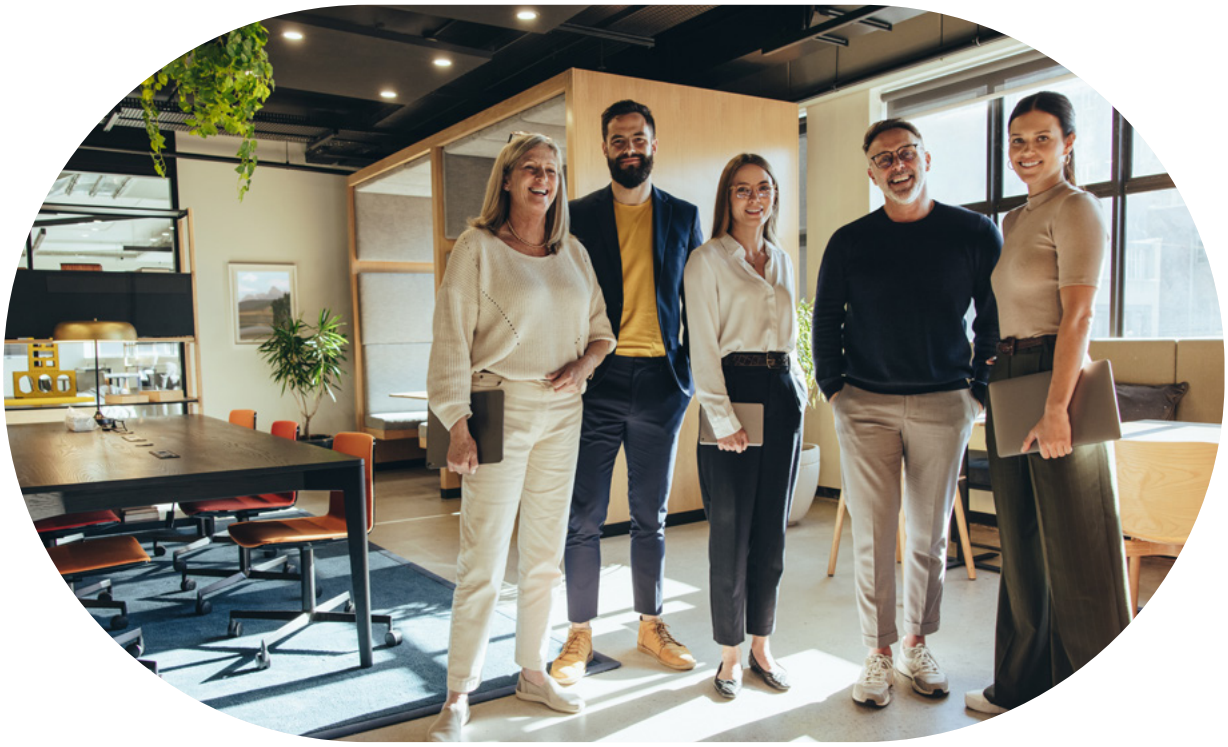
Buyers and investors want confidence in the company behind the numbers. They need to understand what the business owns, what it has promised, where the main risks sit and whether the company can continue operating smoothly after the deal is done. Legal gaps at this point can slow the process, weaken negotiation and reduce value.

8.2 Know what buyers usually look for

- **Clean IP ownership.** Founder, employee and contractor assignments should be complete. There should be no uncertainty about who owns the product, code, models, datasets, designs, documentation or brand.
- **A reliable cap table.** All shares, options, convertibles, ASAs and investor rights should be recorded. The buyer should be able to understand ownership without forensic work.
- **Customer contracts.** Buyers look for change-of-control rights, termination rights, uncapped liability, unusual indemnities, weak payment terms and customer rights that could reduce value.
- **Data protection compliance.** They will ask for privacy notices, DPAs, DPIAs, breach logs, sub-processors, transfer documents, security measures and evidence that data use matches what the company says publicly and contractually.
- **AI governance.** AI companies should expect questions about training data, model providers, output risks, customer data use, bias, explainability, human review and regulatory exposure.
- **Open-source software.** Buyers may run automated scans. AGPL, GPL or undocumented open-source use can create real issues if it has not been tracked and managed properly.
- **Employment records.** Contracts, policies, option grants, settlement agreements, contractor status and disputes should all be clear.
- **Tax and research and development (R&D) claims.** R&D claims, Pay As You Earn (PAYE), value-added tax (VAT), corporation tax, EMI and transfer pricing need to stand up to review.
- **Board minutes and filings.** Companies House filings, shareholder resolutions and board decisions should be complete and easy to follow. A clean legal record reduces risk and supports valuation.

Ask this question:

The founder question at this stage is simple: **can a buyer trust the legal story behind the business?**



/09
Closing thoughts

A good legal foundation is not the result of getting everything right in one sitting. It is the accumulation of small, well-timed decisions taken over the years a company is being built: assigning IP properly when a contractor is hired, structuring a fundraise before shares go out, documenting an EMI grant the day it is promised, updating the data processing agreement when the product changes.

The strongest tech and AI businesses we work with are not the ones with the most complicated legal setup. They are the ones that have dealt with the right things at the right stage, so growth is not slowed down by avoidable legal gaps. That mindset is what this playbook is trying to help build. Not a perfect set of documents, but a habit of taking the right legal step at the moment the company is making the underlying commercial decision.

If you are not sure where the business sits against this playbook, it is worth having that conversation before momentum turns small legal gaps into bigger problems.

Checklist A:
The legal foundations every tech company should have

/01
Founder documents

These set the tone for the company.

- ○ Founder agreement
- ○ Vesting and leaver terms
- ○ Founder IP assignments
- ○ Decision-making rules
- ○ Reserved matters
- ○ Deadlock process
- ○ Confidentiality obligations
- ○ Restrictive covenants
- ○ Shareholder records
- ○ Board approval process

/02
IP protection

For tech and AI companies, IP is not a side issue. It is the business.

- ○ Founder IP assignments
- ○ Employee IP clauses
- ○ Contractor IP assignments
- ○ Trade mark clearance
- ○ Trade mark registrations
- ○ Open-source policy
- ○ Software bill of materials (SBOM)
- ○ Confidentiality controls
- ○ Patent strategy review where relevant
- ○ Domain ownership records
- ○ AI dataset and model records
- ○ Third-party licence records

/03

Investment readiness

Avoid raising on documents that create problems later.

- SEIS and EIS planning
- Advance assurance where appropriate
- Clean share classes
- Suitable advance subscription agreement (ASA) documentation
- Cap table management
- Investor consents
- Option pool planning
- EMI scheme and valuation
- Board and shareholder approvals
- Disclosure records
- Investor communication records

/04

Customer contracts

Your customer contract should help you sell, not give away the business.

- Terms of service or master services agreement (MSA)
- Order form
- Service level agreement (SLA)
- DPA
- Security schedule
- Acceptable use policy
- AI terms where relevant
- IP ownership terms
- Liability caps
- Indemnity position
- Termination rights
- Payment terms
- Change control process
- Sub-processor wording
- Support terms

/05
Data protection & privacy

Privacy is now part of product trust.

- ○ Privacy notice
- ○ Cookie notice
- ○ Cookie consent setup
- ○ Record of processing activities (RoPA)
- ○ Data protection impact assessment (DPIA) template
- ○ Data processing agreement (DPA) template
- ○ Sub-processor list
- ○ Transfer documents
- ○ Breach response process
- ○ Retention policy
- ○ Data subject request process
- ○ AI and automated decision-making review
- ○ Complaints process

/06
AI governance

AI governance does not need to be heavy at the start, but it does need to exist.

- ○ AI acceptable use policy
- ○ AI product risk assessment
- ○ AI register
- ○ Model provider review
- ○ Training data records
- ○ Output risk review
- ○ Human oversight process
- ○ Customer-facing AI terms
- ○ DPIAs where personal data is involved
- ○ EU AI Act applicability review
- ○ Audit logs for higher-risk use cases
- ○ Internal approval process for sensitive AI use

/07
Employment & people

People risk grows quickly.

- Employment contracts
- Contractor agreements
- Consultancy agreements
- Staff handbook
- Disciplinary and grievance policies
- Anti-harassment policy
- Whistleblowing policy
- Remote work policy
- Information security policy
- AI use policy
- Option agreements
- Right-to-work process
- Intermediaries legislation (IR35) review where relevant
- International hiring review

/08
Cyber security

Cyber security is now a legal, commercial and board-level issue.

- Access control rules
- Multi-factor authentication (MFA)
- Encryption standards
- Device management
- Incident response plan
- Supplier security review
- Backups and disaster recovery
- Cyber Essentials or ISO 27001 roadmap
- Breach notification process
- Security schedule for customers
- Cyber insurance review
- Employee security training

LAWYERLY®

Checklist B: The AI-specific legal checklist

AI companies need to think about more than standard software risk. The questions below should be answered before the company scales, sells into regulated sectors or raises serious investment.

/01 Training data

- ○ Where did the data come from?
- ○ Do you have rights to use it?
- ○ Does it include personal data?
- ○ Was it scraped?
- ○ Was consent needed?
- ○ Are there licence restrictions?
- ○ Can you explain the dataset if asked?
- ○ Do your public statements match reality?

/02 Model providers

- ○ Which third-party models are you using?
- ○ Do their terms allow your use case?
- ○ Can customer data be used for training?
- ○ Are outputs indemnified?
- ○ Are there prohibited uses?
- ○ Can the provider change or withdraw the model?
- ○ Are enterprise terms needed rather than consumer terms?

/03 Outputs

- ○ Can outputs be inaccurate?
- ○ Could customers rely on them in high-risk contexts?
- ○ Is human review required?
- ○ Do the terms explain the limits?
- ○ Are outputs logged where needed?
- ○ Can customers challenge or review important decisions?
- ○ Are outputs labelled where required?

/04
Customer data

- Is customer data used to train models?
- Is it retained?
- Is it shared with third-party providers?
- Can customers opt out?
- Is this clear in the contract and privacy notice?
- Is customer data being used in a way the customer would reasonably expect?

/05
Automated decisions

- Does the AI make or support decisions about people?
- Is there human oversight?
- Can people challenge decisions?
- Has a DPIA been completed?
- Do users understand when AI is involved?
- Could the decision affect someone's job, money, health, access to services or legal position?

/06
EU use, if applicable

- Could EU customers use the system?
- Could outputs be used in the EU?
- Could the system fall into a higher-risk category?
- Is an EU AI Act assessment needed?
- Are customers asking for EU AI Act warranties or documentation?

/07
Internal use

- Are employees putting confidential data into consumer AI tools?
- Are prompts and outputs stored?
- Are client documents being uploaded?
- Is there an approved AI tool list?
- Are employees trained on what not to share?
- Is there a process for approving new AI tools?

LAWYERLY®

Checklist C:
A practical legal roadmap for founders

/01
Pre-seed

Focus on ownership and investability.

- ○ Founder agreement
- ○ Founder IP assignments
- ○ Private limited company (Ltd) structure
- ○ Appropriate articles
- ○ Trade mark checks
- ○ SEIS and EIS planning
- ○ Privacy notice
- ○ Cookie setup
- ○ Contractor agreement
- ○ AI acceptable use policy
- ○ Clean cap table
- ○ Basic board records

The priority at this stage is to avoid creating problems that will block funding later.

/02
Seed

Focus on hiring, customers and product risk.

- ○ Employment contracts
- ○ EMI scheme
- ○ Customer terms
- ○ MSA, DPA and SLA
- ○ Security schedule
- ○ Open-source software (OSS) policy
- ○ SBOM
- ○ DPIA template
- ○ RoPA
- ○ Breach response plan
- ○ Investor documents
- ○ Board records
- ○ AI product terms
- ○ Sub-processor list

At this stage, the business needs legal documents that help it operate properly.

/03
Series A

Focus on governance, scale and enterprise readiness.

- Investor-grade articles
- Shareholders' agreement
- Contract playbook
- Data protection maturity
- AI governance framework
- EU AI Act assessment
- Cyber Essentials Plus or ISO roadmap
- International expansion review
- Directors and officers insurance
- Regulatory horizon scanning
- Employment policy suite
- Supplier due diligence

At this stage, legal structure becomes part of how the company wins bigger opportunities.

/04
Series B and beyond

Focus on resilience and institutional discipline.

- In-house or fractional legal support
- Formal risk register
- Board-level compliance reviews
- Vendor due diligence
- Advanced security controls
- Regulatory licensing where needed
- Employment law audits
- Tax and transfer pricing review
- International data transfer review
- Customer contract standardisation
- Fraud prevention procedures
- AI assurance documentation

At this stage, the company needs repeatable processes, not founder memory.

/05
Pre-exit

Focus on diligence.

- Vendor due diligence
- IP cleanup
- OSS remediation
- Cap table cleanup
- Contract review
- Employment classification review
- Data room
- Tax review
- AI governance evidence
- Cyber security evidence
- Warranty and indemnity (W&I) insurance planning
- Change-of-control review
- Customer consent plan

At this stage, the question is not only whether the business is valuable. It is whether the buyer can trust what they are buying.

LAWYERLY®

Watchlist:
Red flags investors & buyers notice quickly

Investors do not expect perfection. They do expect founders to know where the risks are. These are the issues that tend to raise concern:

- No founder IP assignments
- No contractor IP assignments
- No founder vesting
- Messy cap table
- Unclear SEIS or EIS position
- US SAFE used without UK tax advice
- No EMI valuation
- No customer contract template
- Unlimited liability in customer contracts
- No DPA
- No privacy notice
- No DPIAs for higher-risk processing
- No AI policy
- No record of AI tools used
- No open-source policy
- AGPL or GPL code used without review
- No board minutes
- Late Companies House filings
- Unclear employment status for contractors
- No right-to-work process
- No cyber incident plan
- No trade mark clearance
- Customer contracts with change-of-control termination rights
- No data room
- No clear sub-processor list
- No AI output disclaimer
- No security schedule
- No breach response process
- No bias testing of AI systems
- No model cards or system cards for AI products
- Incident response plan does not cover AI-specific scenarios
- No Article 28 data processing agreement with foundation model providers

Get ahead of it:

A founder who can show a plan to fix gaps is in a much stronger position than one who discovers them for the first time during diligence.