# Before you sign

Questions for any software supplier

# Before you sign: questions for any software supplier

Fourteen security questions drawn from the government's Software Security Code of Practice, and the questions on ownership, data, continuity and AI that a contract should answer before it is signed rather than after.

Written for whoever signs for new software or a renewal: operations directors, finance leads, procurement officers and trustees.

## Why ask at all

These questions apply to every supplier, including us: we publish this brief and also sell software, so every question here should be put to us too.

**22%**

of UK businesses considered cyber security to a large extent when buying new software. For charities the figure was 17%.

DSIT and Home Office, Cyber security breaches survey 2025/2026 (Official Statistics), 30 April 2026, Figure 3.2

**15%**

of UK businesses said they reviewed the cyber security risks posed by their immediate suppliers. For charities the figure was 9%.

DSIT and Home Office, Cyber security breaches survey 2025/2026 (Official Statistics), 30 April 2026, section 3.10

The survey covered 2,112 businesses and 1,085 registered charities, weighted to be representative; sole traders, public sector bodies and businesses with no IT capacity or online presence are outside it. Margins of error for businesses reach 2.6 points.

## Security: fourteen questions from the Code

The Software Security Code of Practice sets 14 principles in four themes, and the government says customers may use it in negotiations and contracts. The Code still says a certification scheme is being developed, so there is no Code certificate to ask for. The NCSC tells customers to request the vendor's Assurance Principles and Claims document instead: the vendor's own account of how it meets the Code.

| Theme of the Code | Ask the supplier |
|---|---|
| 1. Secure design and development (principles 1.1 to 1.4) | Which secure development framework do you follow? Can you list the third-party components, and how do you assess their risks? How is each update tested before release? Are the most secure settings on by default? |
| 2. Build environment security (2.1 and 2.2) | How is the environment where the software is built protected from unauthorised access? Are changes to it controlled and logged? |

| Theme of the Code | Ask the supplier |
|---|---|
| 3. Secure deployment and maintenance (3.1 to 3.5) | How is the software delivered securely? Where is your vulnerability disclosure process published? How do you find and rank vulnerabilities in components? Whom do you report them to? How quickly do security updates reach customers? |
| 4. Communication with customers (4.1 to 4.3) | What support and maintenance does the contract include? Will you give at least a year's notice before support ends? How will you tell customers about an incident that could significantly affect them? |

A reseller that does not write the software is expected to cover only themes 3 and 4, so put the first two to whoever wrote it.

## Ownership and data

The common assumption is that paying for bespoke software means owning it. Under the Copyright, Designs and Patents Act 1988 a computer program is a literary work, first owned by its author, or by the employer where an employee wrote it in the course of employment, and an assignment has no effect unless it is in writing and signed by or for the person assigning it. A silent contract leaves legal ownership where it started. Ask who holds the hosting account and the domain name, too.

Where the supplier handles personal data for you as your processor, UK GDPR Article 28 lists terms the contract must contain. Under Article 33 the processor must tell you of a breach without undue delay, so the contract should say how fast. The Information Commissioner's Office is reviewing its guidance on these contracts after the Data (Use and Access) Act 2025.

- [ ] The contract, signed for the supplier, assigns to you the copyright in code written for you, or states the licence you hold instead.
  Copyright, Designs and Patents Act 1988, sections 3, 11 and 90(3)
- [ ] The contract says how your data is returned or securely deleted at its end, including on transfer to another supplier.
  NCSC, Supplier assurance questions; NCSC, 10 Steps: Supply chain security
- [ ] The processor terms cover each Article 28(3) point: documented instructions, confidentiality, security, sub-processors, help with rights requests, breaches and impact assessments, deletion or return, and audits.
  UK GDPR Article 28(3); ICO, What needs to be included in the contract?
- [ ] No sub-processor is used without your written authorisation, and under a general authorisation you are told of any addition or replacement, with a chance to object.
  UK GDPR Article 28(2); ICO, What needs to be included in the contract?

## Continuity and AI

01 **After an incident such as ransomware, how much data could be lost, for how long could the service be down, and when did you last test a restore from backup?**

UK GDPR Article 32 lists the ability to restore personal data promptly after an incident, and regular testing of security measures. The NCSC asks what continuity plan maintains minimum service levels for you in an incident.

02 **For each AI feature, which model provider receives the data, in which country, and for how long is it kept?**

The NCSC says a customer should know where its data is, including derivatives such as logs and machine learning models.

03 **Will the data train or improve any model, yours or another provider's, and can that be refused in writing?**

The NCSC notes that some usage agreements let a provider use customer data for machine learning, and that such terms are particularly common on free tiers of business services.

Send each supplier the same questions and ask for written answers, each citing the contract clause where it appears. Score 0 where there is no answer, 1 where the answer exists only in correspondence, and 2 where it is a term of the contract. The totals are not assurance. They measure how far each supplier has put its answers into the contract.

### Sources


Department for Science, Innovation and Technology and Home Office, Cyber security breaches survey 2025/2026, Official Statistics, published 30 April 2026 (GOV.UK now lists it under the Department for Digital, Culture, Media and Sport as well as DSIT). Summary, section 1.3 (methodology), Figure 3.2, section 3.10 and Appendix A (Table A.1).

Department for Science, Innovation and Technology, Software Security Code of Practice, GOV.UK guidance, published 7 May 2025, updated 15 January 2026 (the page now also lists the Department for Digital, Culture, Media and Sport). Background, Audience and scope, Assurance and self-assessment, the 14 principles and the Glossary.

National Cyber Security Centre, Software Security Code of Practice: For software customers, accessed 19 September 2026. How customers can check suppliers comply.

Copyright, Designs and Patents Act 1988, c. 48, section 3(1), legislation.gov.uk, revised text, no outstanding effects at 19 September 2026.

Copyright, Designs and Patents Act 1988, c. 48, section 11, First ownership of copyright, legislation.gov.uk, revised text, no outstanding effects at 19 September 2026.

Copyright, Designs and Patents Act 1988, c. 48, section 90(3), Assignment and licences, legislation.gov.uk, revised text, no outstanding effects at 19 September 2026.

UK GDPR (Regulation (EU) 2016/679 as it forms part of UK law), Article 28, Processor, paragraphs 2 and 3, legislation.gov.uk, up to date with changes in force on or before 19 September 2026.

UK GDPR, Article 33, Notification of a personal data breach, paragraphs 1 and 2, legislation.gov.uk, up to date with changes in force on or before 19 September 2026 (SI 2026/386 amendments replacing references to the Commissioner are yet to be applied).

UK GDPR, Article 32, Security of processing, paragraph 1(c) and (d), legislation.gov.uk, up to date with changes in force on or before 19 September 2026.

Information Commissioner's Office, Contracts and liabilities between controllers and processors: What needs to be included in the contract?, accessed 19 September 2026. Review notice, minimum required terms and sub-processors.

National Cyber Security Centre, Supplier assurance questions, published 17 December 2020. Managing and recovering from incidents; Other contractual considerations.

National Cyber Security Centre, 10 Steps to Cyber Security: Supply chain security, published 11 May 2021. Embed security within your contracting process.

National Cyber Security Centre, Cloud security guidance, Principle 2: Asset protection and resilience, published 17 November 2018, reviewed 7 June 2023. Principle 2.1, physical location and legal jurisdiction.


### What this brief is not

This brief is not legal advice, and it certifies nothing. It reports what the cited legislation, regulators and government guidance said when last checked on 19 September 2026. Good answers, even contractual ones, are commitments to be tested, not proof of security. It is not a product comparison: we sell software ourselves, so weigh the brief accordingly.


Theo Coleman

Chief Technology Officer, BespokeWorks. July 2026