GHOST
COMPLIANCE
STUDIO

FREE SAMPLE DOCUMENT

Vendor Readiness Pack

— Sample —

A preview of your complete enterprise-ready compliance documentation

ghostcompliance.studio

Prepared exclusively for you by GhostCompliance Studio · Confidential Preview
GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification.
Always consult a qualified legal professional for regulated matters.

WHAT'S IN YOUR FULL PACK

Six Documents. One Complete Pack.

When you order a Vendor Readiness Pack, you receive six customised, enterprise-grade documents drafted to your company's specifics — ready for procurement portals, enterprise RFPs, and due-diligence questionnaires.

01 **Data Protection & Privacy Policy**
GDPR-aligned. Covers lawful bases, data subjects' rights, retention schedules, sub-processor disclosure, and DPO contact information.

02 **Security Questionnaire Response Template**
ISO 27001-aligned answers to the 40 most common vendor security questions. Ready to paste into any enterprise portal.

03 **Supplier Code of Conduct**
Covers ethics, anti-bribery, environmental responsibility, and labour standards. Required by most Fortune 500 procurement teams.

04 **NDA Template (Bilateral)**
Mutual non-disclosure agreement. Solicitor-reviewed template with jurisdiction selection and standard carve-outs.

05 **Company Profile Template**
Structured company overview for procurement submissions: corporate info, financials summary, insurance, certifications.

06 **Cover Letter — Vendor Onboarding**
Professional introductory letter for new enterprise vendor submissions, adaptable for each client relationship.

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.

Data Protection & Privacy Policy

Document Ref: DPP-001
Version: 1.0 | Effective Date: [Date] | Next Review: [Date + 1 year]
Owner: Data Protection Officer | Classification: Public

& SAMPLE — FOR ILLUSTRATION ONLY. NOT A FINAL DOCUMENT.

1. Introduction & Scope

1.1 [Company Name] ("the Company", "we", "us") is committed to protecting the privacy and security of personal data in accordance with Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR") and any applicable national implementing legislation.

1.2 This Policy applies to all personal data processed by the Company in the course of its business operations, including data relating to employees, contractors, clients, prospects, and other individuals whose data the Company collects or processes ("Data Subjects").

1.3 For the purposes of GDPR, the Company acts as a Data Controller in respect of personal data it collects directly, and as a Data Processor where it processes personal data on behalf of its clients. References to obligations under Articles 13, 14, and 30 of the GDPR apply accordingly.

1.4 This Policy must be read in conjunction with the Company's Data Retention Schedule (Ref: DRS-001), Record of Processing Activities (Ref: ROPA-001), and Data Breach Response Procedure (Ref: DBRP-001).

1.5 Questions regarding this Policy should be directed to the Company's Data Protection Officer (DPO) at: dpo@[companydomain]. Individuals seeking to exercise their rights under Articles 15–22 of the GDPR should submit a written request to the same address.

SAMPLE

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.

1.6 The Company designates a Data Protection Officer pursuant to Article 37 of the GDPR. The DPO is responsible for monitoring compliance with this Policy, advising on Data Protection Impact Assessments (DPIAs), and serving as the primary contact for supervisory authorities.

1.7 All staff members and contractors with access to personal data are required to complete mandatory data protection training within 30 days of joining the Company and annually thereafter. Records of training completion are maintained by the People Operations function.

2. Data We Collect and Process

2.0 The Company collects and processes personal data in the categories and for the purposes set out below. Each processing activity is conducted on a lawful basis as identified pursuant to Article 6 GDPR (and, where applicable, Article 9 GDPR for special category data).

2.1 Client & Prospect Data: Business contact names, email addresses, telephone numbers, company details, and correspondence records. Lawful basis: Article 6(1)(b) — performance of a contract; Article 6(1)(f) — legitimate interests (business development). Retention: 7 years post-contract end.

2.2 Employee & Contractor Data: Name, address, national insurance number, bank details, employment history, performance records, absence records, and occupational health data. Lawful bases: Article 6(1)(b) — employment contract; Article 6(1)(c) — legal obligation; Article 9(2)(b) — employment law obligations (special category). Retention: 6 years post-employment.

2.3 Supplier Data: Contact details of supplier representatives, payment information, and due-diligence records. Lawful basis: Article 6(1)(b) — performance of a contract; Article 6(1)(c) — legal obligations (anti-money laundering). Retention: 7 years.

2.4 Website & Digital Data: IP addresses, cookie identifiers, browsing behaviour, and analytics data collected via the Company's website. Lawful basis: Article 6(1)(a) — consent (where applicable); Article 6(1)(f) — legitimate interests (security, analytics). Retention: 13 months from collection.

SAMPLE

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.

2.5 The Company does not sell, rent, or trade personal data to third parties for marketing purposes. Where personal data is shared with processors (e.g. cloud infrastructure providers, payroll processors), appropriate Data Processing Agreements compliant with Article 28 GDPR are in place.

2.6 Transfers of personal data outside the UK/EEA are subject to appropriate safeguards in accordance with Chapter V of the GDPR, including the use of Standard Contractual Clauses (SCCs) approved by the European Commission (Decision 2021/914), adequacy decisions, or other recognised transfer mechanisms.

2.7 The Company implements technical and organisational security measures appropriate to the risk, including: (a) encryption of personal data at rest (AES-256) and in transit (TLS 1.2+); (b) role-based access controls; (c) regular penetration testing and vulnerability scanning; (d) documented incident response procedures.

2.8 Data Subjects have the right, subject to applicable conditions and limitations, to: access their personal data (Art. 15); rectification (Art. 16); erasure ("right to be forgotten") (Art. 17); restriction of processing (Art. 18); data portability (Art. 20); object to processing (Art. 21); and not be subject to solely automated decision-making with significant effects (Art. 22).

SAMPLE

Policy continues in the full document…

The complete Data Protection Policy (14 sections, 28 pages) is included in every Vendor Readiness Pack, fully customised to your company, industry sector, and applicable jurisdiction.

Security Questionnaire Response Template

& SAMPLE — FOR ILLUSTRATION ONLY. NOT A FINAL DOCUMENT.

The following represents a selection of questions from a typical enterprise vendor security questionnaire, together with model responses aligned to ISO/IEC 27001:2022. In your full pack, all 40 questions are answered and all placeholders are replaced with your company's specific details.

Q1. Do you have a written Information Security Policy?

Yes. [Company Name] maintains a formal Information Security Policy (Ref: ISP-001), reviewed annually by the CISO and approved by the Board. The policy is aligned with ISO/IEC 27001:2022 and covers all aspects of information asset management, access control, incident response, and third-party risk.

Q2. Is your organisation certified to ISO 27001 or a comparable standard?

Yes / In progress. [Company Name] holds ISO/IEC 27001:2022 certification issued by [Accredited Certification Body], valid until [Date]. Scope: [describe scope]. Our latest surveillance audit report is available on request under NDA.

Q3. How do you manage access to systems containing client data?

Access is governed by a Role-Based Access Control (RBAC) policy. Access rights are granted on a least-privilege basis, reviewed quarterly, and revoked immediately upon employee departure. Multi-factor authentication (MFA) is mandatory for all privileged accounts and remote access. Privileged access is managed via a PAM solution.

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.

Q4. What encryption standards do you apply to data at rest and in transit?

Data at rest is encrypted using AES-256. All data in transit is protected by TLS 1.2 or higher; TLS 1.0/1.1 is disabled. Encryption keys are managed via a dedicated Key Management System (KMS) with separation of duties between key custodians.

Q5. How do you handle and report security incidents?

Incidents are managed in accordance with our Incident Response Plan (Ref: IRP-001). The plan defines four severity tiers with escalation procedures. Clients are notified within 24 hours of a confirmed breach affecting their data. Regulatory notifications (e.g. to the ICO/DPA) are made within 72 hours per GDPR Art. 33. Post-incident reviews are documented.

Q6. Do you carry out regular penetration testing and vulnerability assessments?

Yes. External penetration testing is conducted annually by a CREST/CHECK-accredited third party. Automated vulnerability scanning (CVSS score "e 7.0 treated as critical) is run weekly. Critical findings must be remediated within 72 hours; high findings within 14 days. Summary executive reports are available on request.

Q7. How do you manage third-party and supply chain risk?

All critical suppliers undergo documented due diligence prior to onboarding, including assessment of security posture, financial stability, and regulatory compliance. Data Processing Agreements (DPAs) are executed with all processors. Supplier security posture is reviewed at contract renewal. A register of approved sub-processors is maintained.

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.

Q8. What is your Business Continuity and Disaster Recovery capability?

A Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are maintained and tested annually via a tabletop exercise. Recovery Time Objective (RTO): [X hours]. Recovery Point Objective (RPO): [Y hours]. Off-site backups are encrypted and verified monthly. Critical system failover is supported by [describe infrastructure].

Q9. How do you ensure staff are trained on information security?

All staff complete mandatory information security awareness training at induction and annually thereafter. Training covers phishing recognition, data handling, password hygiene, and incident reporting. Completion is tracked centrally; non-compliance escalates to line management. Targeted role-based training is provided to technical and privileged-access staff.

Q10. Do you have a documented data retention and disposal policy?

Yes. Our Data Retention Schedule (Ref: DRS-001) defines retention periods for all data categories in line with legal and regulatory requirements. Secure disposal procedures (NIST 800-88 / GDPR Art. 17) are followed for all media. Certificates of destruction are obtained from certified disposal vendors and retained for 3 years.

40 questions in the full template…

Your full Security Questionnaire Response Template covers 40 ISO 27001-aligned questions across all major control domains, with answers tailored to your infrastructure, certifications, and processes.

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.

YOUR JOURNEY TO VENDOR-READINESS

What Happens When You Order

From order to enterprise-ready in 48 hours. Here's exactly how it works.

1

Complete our onboarding form

"H 15 minutes

You fill in a structured intake questionnaire covering your company details, industry sector, key certifications, data flows, and any specific requirements from your enterprise clients. No calls required.

2

We customise all documents to your company

Within 24h of your submission

Our compliance specialists use your intake data to personalise every document — your company name, registration number, registered address, DPO details, operational specifics, and applicable regulatory jurisdiction. Every placeholder is replaced.

3

You receive your complete pack

Within 48h of ordering

All six documents are delivered by email in PDF and Word/DOCX format. Word versions allow you to make minor future edits. PDFs are print-ready for portal submissions.

4

You're vendor-ready for enterprise buyers and tenders

Immediately on receipt

Upload your documents to procurement portals, attach to RFP responses, share with enterprise legal teams — confident that your compliance documentation is professional, complete, and tailored.

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.

TRANSPARENT PRICING

Choose Your Pack

One-time fee. No subscription. No hidden costs. All packs include expert customisation and 48h delivery.

Vendor Readiness Pack

€750

from, excl. VAT

- Data Protection & Privacy Policy
- Security Questionnaire Response (40 Q&A)
- Supplier Code of Conduct
- NDA Template (Bilateral)
- Company Profile Template
- Vendor Onboarding Cover Letter
- 48h delivery · PDF + DOCX

MOST POPULAR

Tender Documentation Pack

€1,500

from, excl. VAT

- Everything in Vendor Readiness Pack
- Technical Capability Statement
- Financial Stability Declaration
- Quality Management Policy
- Equal Opportunities Statement
- ESG / Sustainability Policy
- Tender submission letter template

Enterprise Buyer Pack

€2,500

from, excl. VAT

- Everything in Tender Documentation Pack
- Full Due Diligence Report (10–15 pages)
- Vendor Risk Assessment Response
- Third-Party Audit Preparation Checklist
- Board-level Governance Statement
- Annual Review & Update (1 year)
- Priority 24h delivery

Order your pack at ghostcompliance.studio

Questions? Email us: hello@ghostcompliance.studio

All prices are exclusive of VAT. Prices shown are "from" and may vary based on complexity and jurisdiction. Payment processed securely via Stripe.

GhostCompliance Studio documentation packs are professional templates customized to your company. They do not constitute legal advice or guarantee certification. Always consult a qualified legal professional for regulated matters.