FourWinds
fourwinds.ie

COMPLIANCE PACK

A sample business

122 of 154 requirements met across 2 laws and ISO 27001.

SAMPLE · EVERY NAME AND NUMBER IS MADE UP

Taken 13 Nov 2026, 10:00 Dublin time From the records in Eurus

Requirements · Met: 122 · Not met: 13 · Needs attention: 15 · Not checked yet: 4

Evidence run out or due within 30 days: 1 · Evidence to collect: 2 · High risks: 1 · Deadlines running: 2

The ledger ran 4,952 checks in the last 90 days: 4,122 passed, 732 failed. With a real business's pack, each result also comes in a CSV with its sha256.

01

Readiness by law

What's in place for each law, against the point it's measured to.

GDPR

Every duty applies now

28 of 30 in place 93%

EU AI Act

AI literacy has applied since 2 February 2025

1 of 1 in place 100%

ISO 27001

Certification needs every control in place

93 of 123 in place 76%

SAMPLE

02

Legal duties

The duties recorded for the business one by one, each with its state, its owner and what shows it: a check in the ledger, evidence on file, or nothing yet. The figures on the first page count every requirement of each law, these among them.

AI literacy of staff (EU AI Act Art. 4)
Met, shown by a document. Current evidence: AI literacy session, all staff.

Plain information and an easy way to use rights (GDPR Art. 12(1))
Met, shown by a document. Current evidence: Privacy notice on the website and in the app; Retention schedule and privacy notice entries; Data protection policy, version 1.

Answer access requests within one month (GDPR Art. 15)
Met, shown by a document. Current evidence: Data subject request procedure; Data protection policy, version 1.

Written contract with each processor (GDPR Art. 28(3))
Met, verified. 1 passing check and current evidence: Data processing agreement with Brightdesk (sample); Supplier security policy, version 1; A processing contract with every processor.

Security appropriate to the risk (GDPR Art. 32)
Not met. 6 failed checks are still open.

Breach notification within 72 hours (GDPR Art. 33)
Met, verified. 607 passing checks and current evidence: Incident response policy, version 1.

Delete data once it is no longer needed (GDPR Art. 5(1)(e))
Met, shown by a document. Current evidence: Retention schedule and privacy notice entries; Records retention policy, version 1; A retention rule for each processing activity.

No owner is named yet for any of these 7. An owner is the person who answers for a duty and keeps what shows it up to date.

DORA: does not apply to the business (20 duties set aside)
DORA is for financial entities: this software company sells to them but is not one; their contracts carry DORA's terms (Article 30).

NIS2: does not apply to the business (14 duties set aside)
A small enterprise (40 staff, under €10m): NIS2 does not reach a managed service provider of its size unless an authority names it.

03

Standards the business follows

Recorded and tracked the same way; voluntary or contractual, not a legal duty.

Access control (ISO 27001 A.5.15)
Not met. 4 failed checks are still open.

Access rights (ISO 27001 A.5.18)
Not met. 2 failed checks are still open.

Information security in supplier relationships (ISO 27001 A.5.19)
Not met, verified. Not met in the records: the security answers from Tallybook (sample) raised concerns.

SAMPLE

Information security incident management planning and preparation (ISO 27001 A.5.24)
Met, shown by a document. Current evidence: Incident response policy, version 1.

Response to information security incidents (ISO 27001 A.5.26)
Met, verified. 61 passing checks and current evidence: Incident response policy, version 1.

Information backup (ISO 27001 A.8.13)
Met, verified. 54 passing checks and current evidence: Backup restore test; Business continuity and disaster recovery policy, version 1; Restore test run on 14 Oct 2026: Mailbox and file restore; Failover test run on 24 Sept 2026: Portal failover to the second region; Restore test run on 14 Sept 2026: Website redeployed to the standby host.

Logging (ISO 27001 A.8.15)
Met, verified. 317 passing checks and current evidence: Logging and monitoring procedure.

Secure authentication (ISO 27001 A.8.5)
Not met. 17 failed checks are still open.

Management of technical vulnerabilities (ISO 27001 A.8.8)
Not met. 64 failed checks are still open.

No owner is named yet for any of these 9. An owner is the person who answers for a duty and keeps what shows it up to date.

04

Evidence

Where each item is kept, unless its line says otherwise: the shared drive.

Data processing agreements with sub-processors: runs out on 25 Nov 2026
Confirmed by Ronan Kelly (sample). For GDPR Art. 28(3) · ISO 27001 A.5.19.

Monthly vulnerability scan: in date until 15 Dec 2026
Confirmed by Darragh Walsh (sample). Where it is kept: in Eurus, under Registers, Vulnerabilities, with its SHA-256. For ISO 27001 A.8.8.

ISMS scope, context and interested parties: in date until 7 Jan 2027
Confirmed by Aoife Brennan (sample). For ISO 27001 4.1, 4.2, 4.3, 4.4.

Joiners and leavers access review: in date until 17 Jan 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.5.18, A.8.5.

Leadership commitment and security roles: in date until 17 Jan 2027
Confirmed by Gráinne O'Neill (sample). For ISO 27001 5.1, 5.3, A.5.2, A.5.3, A.5.4.

Resources and communication plan for the security programme: in date until 22 Jan 2027
Confirmed by Gráinne O'Neill (sample). For ISO 27001 7.1, 7.4.

Threat intelligence digest, October: in date until 22 Jan 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.5.7.

Document control procedure and register: in date until 27 Jan 2027
Confirmed by Aoife Brennan (sample). For ISO 27001 7.5.1, 7.5.2, 7.5.3, A.5.37.

Contacts with authorities and security groups: in date until 26 Feb 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.5.5, A.5.6.

Screening and disciplinary procedure: in date until 8 Mar 2027
Confirmed by Gráinne O'Neill (sample). For ISO 27001 A.6.1, A.6.4.

SAMPLE

Change management records: in date until 15 Mar 2027
Confirmed by Ronan Kelly (sample). For ISO 27001 A.8.32, 8.1.

Special category data: the condition for sick leave records: in date until 23 Mar 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 9.

Backup restore test: in date until 5 Apr 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.8.13, A.5.30.

CRM data accuracy review: in date until 20 Apr 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 5(1)(d).

Records of processing: in date until 27 Apr 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 30(1), Art. 5(1)(b), Art. 5(1)(c), Art. 6(1).

Capacity and performance review: in date until 6 May 2027
Confirmed by Ronan Kelly (sample). For ISO 27001 A.8.6, A.8.20, A.8.21.

Legal and contractual requirements register: in date until 17 May 2027
Confirmed by Aoife Brennan (sample). For ISO 27001 A.5.31, A.5.32, A.5.36.

Privacy notice on the website and in the app: in date until 17 May 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 12(1), Art. 13, Art. 14.

Security objectives for the year: in date until 16 Jun 2027
Confirmed by Gráinne O'Neill (sample). For ISO 27001 6.2, 6.3, 9.1.

Risk assessment and treatment plan: in date until 16 Jul 2027
Confirmed by Aoife Brennan (sample). For ISO 27001 6.1.1, 6.1.2, 6.1.3, 8.2, 8.3.

Consent and marketing opt-out records: in date until 5 Aug 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 7, Art. 21(3).

Information asset inventory and classification: in date until 20 Aug 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.5.9, A.5.12, A.5.13.

Penetration test report, summer: in date until 21 Aug 2027
Confirmed by Ronan Kelly (sample). For ISO 27001 A.8.8, A.8.29.

Data subject request procedure: in date until 27 Aug 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 15, Art. 16, Art. 18, Art. 20, Art. 21(1).

Security awareness training, all staff: in date until 2 Sept 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.6.3, 7.2, 7.3.

Engineering standards: architecture, environments and test data: in date until 4 Sept 2027
Confirmed by Ronan Kelly (sample). For ISO 27001 A.5.8, A.8.11, A.8.26, A.8.27, A.8.31, A.8.33.

Retention schedule and privacy notice entries: in date until 4 Sept 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 5(1)(e), Art. 12(1).

AI literacy session, all staff: in date until 8 Sept 2027
Confirmed by Aoife Brennan (sample). For EU AI Act Art. 4.

Logging and monitoring procedure: in date until 20 Sept 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.8.15, A.8.16, A.8.17.

Endpoint and network configuration standard: in date until 24 Sept 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.8.18, A.8.19, A.8.22, A.8.23.

Information security policy: in date until 24 Sept 2027
Confirmed by Gráinne O'Neill (sample). For ISO 27001 A.5.15 · GDPR Art. 32.

Breach log and notification procedure: in date until 8 Oct 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 33(5), Art. 34.

SAMPLE

Device return and disposal records: in date until 16 Oct 2027
Confirmed by Darragh Walsh (sample). For ISO 27001 A.5.11, A.7.9, A.7.10, A.7.14.

DPIA for the analytics feature: in date until 20 Oct 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 35, Art. 25.

Transfer impact assessment for US sub-processors: in date until 23 Oct 2027
Confirmed by Aoife Brennan (sample). For GDPR Art. 44.

Internal audit report, Q3: in date until 27 Oct 2027
Confirmed by Aoife Brennan (sample). For ISO 27001 9.2.1, 9.2.2, A.5.35.

Management review minutes, October: in date until 30 Oct 2027
Confirmed by Gráinne O'Neill (sample). For ISO 27001 9.3.1, 9.3.2, 9.3.3.

Nonconformity and corrective action log: in date until 3 Nov 2027
Confirmed by Aoife Brennan (sample). For ISO 27001 10.1, 10.2.

AI literacy training, all staff: still to collect
Nobody in the business has confirmed it yet. For EU AI Act Art. 4.

Data processing agreement with Brightdesk (sample): in date
Confirmed by Aoife Brennan (sample). For GDPR Art. 28(3).

Data protection officer assessment: in date
Confirmed by Aoife Brennan (sample). For GDPR Art. 37.

Office security walkthrough: still to collect
Nobody in the business has confirmed it yet. For ISO 27001 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.7, A.7.8, A.7.11, A.7.12, A.7.13.

Security answers: Tallybook (sample): in date
Nobody in the business has confirmed it yet. Where it is kept: Sent by the supplier through a one-use link.

Staff contracts with confidentiality terms: in date
Confirmed by Gráinne O'Neill (sample). For ISO 27001 A.6.2, A.6.6.

05

Risks

Likelihood times impact, each 1 to 5: 15 and over is high.

Someone gets in with a stolen staff password (score 15, high)
Open: the plan is to reduce it. Owner: Darragh Walsh (sample). Review on 13 Dec 2026.

A known hole in a library the product uses (score 12, medium)
Open: the plan is to reduce it. Owner: Ronan Kelly (sample). Review on 13 Dec 2026.

The platform is down for a day (score 8, medium)
Being reduced. Owner: Ronan Kelly (sample). Review on 11 Feb 2027.

One engineer alone knows the billing integration (score 6, low)
Accepted. Owner: Gráinne O'Neill (sample). Review on 12 Jan 2027.

A supplier holds customers' data with no processing agreement (score 6, low)
Being reduced. Owner: Aoife Brennan (sample). Review on 11 Feb 2027.

Customer data pasted into an AI tool the business has not approved (score 6, low)
Being reduced. Owner: Aoife Brennan (sample). Review on 13 Mar 2027.

SAMPLE

06

AI in use

Each AI system or tool, its class under the AI Act, and what is missing.

Wordbridge Translate (sample): minimal risk
Translating support replies and help articles for customers in France and Germany. · users trained · approved by Aoife Brennan (sample)

GitHub Copilot: minimal risk
Suggesting code to the engineers. · users trained · approved by Gráinne O'Neill (sample)

Microsoft 365 Copilot: minimal risk
Drafting emails and documents, and summarising meetings. · users trained · approved by Gráinne O'Neill (sample)

Support assistant in Brightdesk (sample): limited risk (people must be told it is AI)
Suggesting first replies to support messages, and answering simple questions in the help centre chat. · users trained · approved by Gráinne O'Neill (sample)

07

Incidents

Each incident and every deadline it started, with when each was met.

A customer export left in a shared folder anyone in the company could open: personal data breach, high, open
First sign 12 Nov 2026, 14:00. Aware then; the clocks run from awareness. The business was the controller.
- Notify the supervisory authority (in Ireland, the Data Protection Commission), unless the breach is unlikely to put people at risk (GDPR Art. 33(1)): due 15 Nov 2026, 14:00

A customer's invoice emailed to another customer: personal data breach, medium, closed
First sign 1 Nov 2026, 09:20. Aware then; the clocks run from awareness. The business was the controller.
Outcome: Reported to the Data Protection Commission 41 hours after it was found; the customer was told; invoices are now sent only to the address on the customer's own record.
- Notify the supervisory authority (in Ireland, the Data Protection Commission), unless the breach is unlikely to put people at risk (GDPR Art. 33(1)): met 3 Nov 2026, 02:20, ref. DPC breach notification BN-1104 (sample)

08

Requests

Requests the law gives a reply time: data subject requests, protected disclosures and remote or flexible working requests.

Data protection right (erasure, rectification, objection or portability): received 22 Oct 2026, open, due 22 Nov 2026
A former customer asks for their data to be erased.

Access to personal data: received 24 Aug 2026, answered 5 Sept 2026
A customer's former employee asks for a copy of their account data. Outcome: Sent a copy of their account records and the support messages, by secure link.

SAMPLE

Data protection right (erasure, rectification, objection or portability): received 16 Sept 2026, answered 20 Sept 2026

A trial user asks for their account to be deleted. Outcome: Account and its data deleted; the trial invoice is kept for six years, as Revenue requires.

Access to personal data: received 7 Oct 2026, answered 18 Oct 2026

A customer asks what the analytics feature records about their staff. Outcome: Explained what is recorded and for how long, with the DPIA summary.

Data protection right (erasure, rectification, objection or portability): received 29 Oct 2026, answered 30 Oct 2026

A newsletter subscriber asks to be taken off every list. Outcome: Taken off every list in HubSpot; marked so they are not added again.

What this is: the business's own compliance records as they stood when the pack was taken. It is not legal advice and not a certification.

SAMPLE