The Practical Guide to EU Compliance 2026

What every website owner must know about GDPR, NIS2, DORA & the EAA — in plain language.

EUComply · eucomplypro.com

Introduction: Why Compliance Matters Now (and Why It's Not as Scary as You Think)

If you run a website that serves customers in the European Union, you have probably heard a lot of alarming words in the last few years: GDPR, NIS2, DORA, EAA, cookies, consent, data processing agreements, accessibility statements. It sounds like a pile of legal homework you never asked for — and much of the advice online is either terrifying or written by lawyers for other lawyers.

Here is the honest truth, up front:

Compliance in 2026 is mostly about a few practical things you can actually do. Most of it is not about hiring a lawyer. Most of it is about: Most of it is not about hiring a lawyer. Most of it is about:

- Making sure your website is secure (HTTPS, no obvious gaps)
- Being clear about what data you collect and why
- Having a privacy policy and cookie consent
- Being able to say "yes, we are accessible to people with disabilities"
- Having a few key documents ready if someone asks
- Knowing who your vendors are and what they do with data

This guide walks you through each of the four big frameworks — GDPR, NIS2, DORA and the EAA — in plain language. For each one we answer: *What is it? Do I have to worry? What exactly do I need to do? What does it cost?*

Who This Book Is For

- Small and medium business owners with a website
- Freelancers and solo operators who collect any customer data
- Marketing people who run their company's site and want to avoid mistakes
- Non-EU businesses that sell to EU customers and need to know the rules

If you run a WordPress site, a Shopify store, a Webflow page or a plain HTML site, the practical guidance here applies to you. The principles are the same regardless of the platform you build on.

How to Use This Book

The four frameworks overlap. Rather than reading four separate rulebooks, read this as one process:

- **Chapter 2 — GDPR covers the foundation: data, consent, privacy.** covers the foundation: data, consent, privacy.
- **Chapter 3 — NIS2 covers security obligations for a wider range of businesses.** covers security obligations for a wider range of businesses.
- **Chapter 4 — DORA covers resilience specifically for the financial sector, but with principles that apply more broadly.** covers resilience specifically for the financial sector, but with principles that apply more broadly.

- **Chapter 5 — EAA covers accessibility for everyone's websites.** covers accessibility for everyone's websites.

Then **Chapters 6–8 give you practical tools: how to scan your own site for gaps, how to build a simple compliance roadmap, and which templates to have ready.** give you practical tools: how to scan your own site for gaps, how to build a simple compliance roadmap, and which templates to have ready.

A Note on What This Book Is Not

This guide does **not replace professional legal advice. Regulations change, and the obligations can depend on your specific size, sector and circumstances. What this book gives you is the practical baseline — the 80% that most small businesses need — so that if you do talk to a lawyer, you are asking smart questions, not terrified ones.** replace professional legal advice. Regulations change, and the obligations can depend on your specific size, sector and circumstances. What this book gives you is the practical baseline — the 80% that most small businesses need — so that if you do talk to a lawyer, you are asking smart questions, not terrified ones.

The One Sentence to Remember

> **Compliance is not about being perfect. It is about being able to show you are trying, in a documented and repeatable way.**

That sentence will make everything else in this book easier to hold onto. In the next chapter we start with the rule that touches almost every website in Europe: the GDPR.

GDPR: What Every Website Actually Needs

The General Data Protection Regulation (GDPR) has been in effect since May 2018. By now, everyone has heard of it. But confusion remains about what a small business actually needs to do.

Does GDPR Apply to You?

GDPR applies if you:

- **Are based in the EU — any business, any size, any website** — any business, any size, any website
- **Are outside the EU but sell to or monitor EU residents — yes, it applies to you too** — yes, it applies to you too

The common myth that "GDPR only applies to companies with 250+ employees" is wrong. That threshold only affects *record-keeping requirements (Article 30), not whether GDPR applies at all.* (Article 30), not whether GDPR applies at all.

The 5 Things Your Website Must Have

1. A Privacy Policy

This is the most basic requirement. Your privacy policy must tell visitors:

- What data you collect (name, email, IP address, cookies, etc.)
- Why you collect it (order processing, analytics, marketing)
- How long you keep it
- Who you share it with (payment processors, hosting, analytics tools)
- What rights the visitor has (access, deletion, portability)
- How to contact you

Practical tip: Do not copy-paste a generic privacy policy template. It is obvious to regulators and does not protect you. Customize it to your actual data practices. If you only collect email addresses for a newsletter, say that. If you use Google Analytics, say that. Do not copy-paste a generic privacy policy template. It is obvious to regulators and does not protect you. Customize it to your actual data practices. If you only collect email addresses for a newsletter, say that. If you use Google Analytics, say that.

2. Cookie Consent (Consent Banner)

If your website uses cookies for anything other than "strictly necessary" functions (like session management), you need a consent banner that:

- Blocks non-essential cookies **before consent is given** consent is given
- Lets users accept or reject specific categories
- Records the consent (for your own documentation)
- Is as easy to reject as to accept (the "cookie wall" approach is illegal)

What changed in 2026: The ePrivacy Regulation continues to tighten. Pre-ticked boxes have been illegal since 2018. The current standard is that rejecting must be as easy as accepting — no more hidden "Reject" buttons in tiny grey text. The ePrivacy Regulation continues to tighten. Pre-ticked boxes have been illegal since 2018. The current standard is that rejecting must be as easy as accepting — no more hidden "Reject" buttons in tiny grey text.

3. Contact Information

You must provide a way for data subjects to reach you about their data. This can be an email address, a contact form, or a physical address. For EU-based businesses, it is common to include your VAT number and company registration.

4. Data Processing Records (if 250+ employees or high-risk processing)

If you have more than 250 employees, or if you process special categories of data (health, biometrics, political opinions, etc.), you must maintain a Record of Processing Activities (ROPA). This is a document listing every data processing activity in your organization.

5. Data Processing Agreement with Vendors

If you use third-party services that process data on your behalf — email marketing, hosting, analytics, payment processing — you need a Data Processing Agreement (DPA) with each vendor. Many vendors (Shopify, Google, Mailchimp) offer standard DPAs that you can accept in their dashboard.

Common GDPR Pitfalls for Small Businesses

Pitfall | Why It's a Problem | How to Fix

No privacy policy | Basic violation, starting fines | Write one (see Chapter 8 for templates)

No cookie consent | Very common, actively enforced | Add a consent banner

Data stored forever | Violates storage limitation | Delete old customer data annually

Using Google Fonts without hosting locally | German courts have fined for this | Self-host fonts or use system fonts

Contact form without HTTPS | Data in transit is unprotected | Check your site has HTTPS

Email list without consent records | Cannot prove opt-in | Use a double opt-in system

GDPR Fine Levels

GDPR fines are structured in two tiers:

- **Lower tier: Up to €10 million or 2% of annual global turnover** Up to €10 million or 2% of annual global turnover
- **Upper tier: Up to €20 million or 4% of annual global turnover** Up to €20 million or 4% of annual global turnover

In practice, fines for small businesses are rarely at these maximum levels. The first step from a data protection authority is almost always a warning and a demand to fix the issue. But fines do happen, and the cost of non-compliance (including lost business from customers who check) often exceeds the cost of

getting compliant.

What You Can Do Right Now (5 Minutes)

- Go to your website. Is there a privacy policy link in the footer? If not, make a note to add one.
- Check if your site has HTTPS (look for the padlock in the address bar). If not, fix this immediately — it is free with Cloudflare or Let's Encrypt.
- Open your browser's developer tools and check for cookies. If you see tracking cookies but no consent banner, that is a violation.
- Look at your email list. Can you prove when and how each person signed up?

Next chapter: NIS2 — the security regulation that expands the scope of who must have documented security measures. NIS2 — the security regulation that expands the scope of who must have documented security measures.

NIS2: Security for a Wider Range of Businesses

The Network and Information Security 2 Directive (NIS2) came into effect in October 2024, with EU member states required to implement it into national law by October 2024. By 2026, it is fully operational across the EU. It expands the scope of cybersecurity regulation far beyond the original NIS Directive.

What NIS2 Actually Says

NIS2 requires businesses in specific sectors to implement **appropriate and proportionate technical, operational and organizational measures to manage cybersecurity risks. It also requires incident reporting.** to manage cybersecurity risks. It also requires incident reporting.

The key difference from GDPR: where GDPR protects *data, NIS2 protects the* , NIS2 protects the *systems that process it.* that process it.

Does NIS2 Apply to You?

NIS2 splits organizations into two categories:

Essential entities (strictest requirements): - Energy, transport, water, health, digital infrastructure - No size threshold — any size qualifies (strictest requirements): - Energy, transport, water, health, digital infrastructure - No size threshold — any size qualifies

Important entities (slightly lighter requirements): - Postal services, waste management, manufacturing of critical products - Digital providers (marketplaces, search engines, social networks) - (slightly lighter requirements): - Postal services, waste management, manufacturing of critical products - Digital providers (marketplaces, search engines, social networks) - **Any medium-sized enterprise (50+ employees or €10M+ turnover) in these sectors** (50+ employees or €10M+ turnover) in these sectors

The big change from NIS2's predecessor: many more businesses are now in scope. If you run a digital marketplace, an e-commerce platform, or a managed hosting service, you are likely affected.

What You Need to Do

1. Risk Assessment

You must document a cybersecurity risk assessment covering:

- Threats to your systems and data
- Vulnerabilities in your infrastructure
- Impact of potential incidents
- Mitigation measures

2. Security Measures

You must implement security measures appropriate to your risk level. These include:

- **Access control: Who can access what? Use strong passwords and two-factor authentication.** Who can access what? Use strong passwords and two-factor authentication.

- **Network security: Firewalls, HTTPS, regular updates.** Firewalls, HTTPS, regular updates.
- **Incident detection: You need a way to know when something is wrong.** You need a way to know when something is wrong.
- **Business continuity: What happens if your website goes down? Do you have a backup?** What happens if your website goes down? Do you have a backup?
- **Supply chain security: Your vendors' security affects yours. Review their practices.** Your vendors' security affects yours. Review their practices.

3. Incident Reporting

If you have a significant cybersecurity incident, you must report it:

- **Initial notification: Within 24 hours (essential) or 72 hours (important)** Within 24 hours (essential) or 72 hours (important)
- **Final report: Within 1 month** Within 1 month

A "significant incident" is one that disrupts your services or affects data integrity.

4. Supply Chain Security

NIS2 specifically requires you to assess the cybersecurity of your supply chain. If you use a third-party payment processor, hosting provider, or SaaS tool, you should know their security posture and have a contractual agreement covering it.

How NIS2 Overlaps with GDPR

Aspect | GDPR | NIS2

What it protects | Personal data | Systems and networks

Breach notification | 72 hours | 24-72 hours

Risk assessment | Recommended | Required

Supply chain | DPA required | Security assessment required

Fines | Up to €20M or 4% | Up to €10M or 2% (important) / higher (essential)

Practical NIS2 Checklist

- [ ] You have a documented cybersecurity risk assessment
- [ ] Access controls are in place (2FA, role-based access, password policies)
- [ ] HTTPS is active on all pages
- [ ] You have a backup and recovery plan (tested)
- [ ] You know how to report an incident within the required timeframe
- [ ] Your vendors' security is documented

Key Takeaway

NIS2 is about showing you take security seriously. You do not need a military-grade security setup — but you do need documentation that you have thought about the risks, taken reasonable measures, and have a plan for when things go wrong. The key word in the directive is **proportionate. A small online shop does not need the same security as a national energy grid, but it needs** . A small online shop does not need the same security as a national energy grid, but it needs *some security.* security.

Next chapter: DORA — the Digital Operational Resilience Act for the financial sector, with principles that apply to anyone who handles digital transactions. DORA — the Digital Operational Resilience Act for the financial sector, with principles that apply to anyone who handles digital transactions.

DORA: Digital Resilience for Financial Services

The Digital Operational Resilience Act (DORA) came into full effect in January 2025. It is the strictest of the four frameworks — but it applies to a narrower group.

What DORA Says

DORA requires financial institutions to ensure they can withstand, respond to, and recover from all types of ICT (Information and Communication Technology) disruptions. It covers:

- **ICT risk management: Internal policies for managing technology risk** Internal policies for managing technology risk
- **Incident reporting: Classifying and reporting ICT-related incidents** Classifying and reporting ICT-related incidents
- **Resilience testing: Regular testing of systems** Regular testing of systems
- **Third-party risk: Managing the risk from ICT service providers** Managing the risk from ICT service providers
- **Information sharing: Voluntary intelligence sharing about threats** Voluntary intelligence sharing about threats

Does DORA Apply to You?

DORA applies to **financial entities:**:

- Banks, investment firms, payment institutions
- Insurance companies, reinsurance firms
- Credit rating agencies, crowdfunding platforms
- Crypto-asset service providers

If you run a website that processes payments, you are **not automatically a financial entity under DORA unless that is your primary business. However, the principles of DORA are a useful benchmark for any business that handles financial transactions.** automatically a financial entity under DORA unless that is your primary business. However, the principles of DORA are a useful benchmark for any business that handles financial transactions.

Practical Principles for Non-Financial Businesses

Even if DORA does not directly apply to you, its principles represent the new standard for digital resilience:

1. Know Your Critical Systems

What systems would bring your business to a halt if they went down? For most businesses: website, payment processing, email, customer database. Document what these are and what happens if each one fails.

2. Test Your Recovery

DORA requires regular testing. For smaller businesses, this means:

- Test your backup restore process at least once a year
- Simulate a website outage (what do you do? how long to recover?)
- Test your incident response plan

3. Know Your Third-Party Risk

DORA requires financial institutions to map their ICT third-party dependencies and assess concentration risk. For any business, you should:

- List every third-party tool you depend on
- Know what happens if each one becomes unavailable
- Have a backup option for critical services

Practical Checklist

- [ ] Your critical systems are documented
- [ ] You have tested your backups (actually restored from them)
- [ ] You know your dependency on third-party providers
- [ ] You have a plan for a 24-hour outage of your website

Key Takeaway

DORA is the strictest framework, but its principles of resilience — knowing your systems, testing your recovery, managing third-party risk — are good practice for any business. If you are not a financial institution, you can adopt the principles at a proportional level without the full regulatory burden.

Next chapter: The European Accessibility Act — the 2025 deadline that affects nearly every website serving EU customers. The European Accessibility Act — the 2025 deadline that affects nearly every website serving EU customers.

EAA: Accessibility Is the Law

The European Accessibility Act (EAA) is the newest of the four frameworks, and the one that catches the most website owners by surprise. It took effect in June 2025, with a phased enforcement period.

What the EAA Says

The EAA requires that **digital products and services be accessible to people with disabilities. This includes:** be accessible to people with disabilities. This includes:

- Websites and e-commerce platforms
- Mobile apps
- E-books and digital documents
- Banking services and ATMs
- E-ticketing and e-commerce
- Telecommunications services

The technical standard is **EN 301 549, which largely aligns with the Web Content Accessibility Guidelines (WCAG) 2.2 Level AA.**, which largely aligns with the Web Content Accessibility Guidelines (WCAG) 2.2 Level AA.

Does the EAA Apply to You?

Yes, if you sell products or services to EU consumers through a digital channel. There is no size exemption — a one-person shop with a WooCommerce site is just as subject to the EAA as a multinational retailer.

The only exemptions are: - Micro-enterprises providing **only non-digital services (e.g., a local bakery that does not take online orders) - Public sector bodies (they are covered by a separate directive, but the requirements are similar)** non-digital services (e.g., a local bakery that does not take online orders) - Public sector bodies (they are covered by a separate directive, but the requirements are similar)

What You Need to Do

1. Publish an Accessibility Statement

Your website must have an accessibility statement that:

- States your commitment to accessibility
- Lists which parts of your site are accessible and which are not
- Provides a way for users to report accessibility issues
- References the applicable standard (EN 301 549 / WCAG 2.2)
- Includes a contact method

2. Meet WCAG 2.2 Level AA

This is the technical requirement. The main areas:

Perceivable: - All images have alt text (descriptions for screen readers) - Videos have captions - Content is readable and understandable - All images have alt text (descriptions for screen readers) - Videos have captions - Content is readable and understandable

Operable: - Everything can be done with a keyboard (no mouse-only interactions) - Navigation is consistent - Users have enough time to read and use content - No flashing content that could cause seizures - Everything can be done with a keyboard (no mouse-only interactions) - Navigation is consistent - Users have enough time to read and use content - No flashing content that could cause seizures

Understandable: - Text is readable and predictable - Forms have clear labels and error messages - The language of the page is declared - Text is readable and predictable - Forms have clear labels and error messages - The language of the page is declared

Robust: - Content works with current and future assistive technologies - Valid HTML, proper semantic structure - Content works with current and future assistive technologies - Valid HTML, proper semantic structure

3. Fix Common Issues

The most common accessibility barriers on small business websites:

Issue | How to Fix

Missing alt text | Add descriptive alt text to all images

Low contrast text | Use a contrast checker (free online tools)

No heading hierarchy | Use h1-h6 properly, not just for font size

Forms without labels | Every input needs a visible `<label>`

No skip-to-content link | Add one at the top of the page

PDFs not accessible | Provide HTML versions or accessible PDFs

Keyboard traps | Test that Tab works through all interactive elements

Practical Checklist

- [ ] Accessibility statement is published on your website
- [ ] Alt text is present on all images
- [ ] Contrast ratio meets WCAG AA standards (4.5:1 for normal text)
- [ ] Website is fully navigable by keyboard
- [ ] Forms have proper labels and error messages
- [ ] Heading structure is logical (h1 → h2 → h3)
- [ ] You have a contact method for accessibility issues

What It Costs

Accessibility fixes range from free (adding alt text, fixing contrast in CSS) to investment-level (redesigning a complex checkout flow). Most small businesses can reach a reasonable level of compliance

with a few hours of work and free tools.

- **Free tools: WAVE browser extension, axe DevTools, Lighthouse in Chrome** WAVE browser extension, axe DevTools, Lighthouse in Chrome
- **Audit tools: Paid services $50–$200 per scan** Paid services $50–$200 per scan
- **Professional audit: $500–$3,000 depending on site complexity** $500–$3,000 depending on site complexity

Key Takeaway

The EAA is the newest regulation and the one most small businesses are least prepared for. But it is also the most straightforward to make progress on: fix alt text, fix contrast, fix keyboard navigation, publish a statement. You do not need to be perfect on day one, but you need to be able to show progress.

Next chapter: How to scan your own website for compliance gaps — the practical tool you can use right now. How to scan your own website for compliance gaps — the practical tool you can use right now.

Chapter 6: How to Scan Your Website for Compliance Gaps

Theory is useful. But what you actually need is a way to check your own website and see what is missing. This chapter gives you a practical, repeatable process.

The 5-Minute Quick Scan

You can do this right now, without any tools beyond a browser:

1. Check for HTTPS Look at the address bar. Do you see a padlock? If not, your site is not secure. Visit https://www.ssllabs.com/ssltest/ to check your certificate quality. Look at the address bar. Do you see a padlock? If not, your site is not secure. Visit https://www.ssllabs.com/ssltest/ to check your certificate quality.

2. Check for a Privacy Policy Scroll to the footer of your website. Is there a link called "Privacy Policy" or "Privacy"? Click it. Does it contain actual information about your data practices, or is it a generic placeholder? Scroll to the footer of your website. Is there a link called "Privacy Policy" or "Privacy"? Click it. Does it contain actual information about your data practices, or is it a generic placeholder?

3. Check for Cookie Consent Open your website in an incognito/private window. Do you see a cookie banner? If not, tracking cookies are likely being set without consent. Open Developer Tools → Application → Cookies and look for any third-party cookies. Open your website in an incognito/private window. Do you see a cookie banner? If not, tracking cookies are likely being set without consent. Open Developer Tools → Application → Cookies and look for any third-party cookies.

4. Check for an Accessibility Statement Look in the footer for "Accessibility" or "Accessibility Statement." If it exists, does it include a contact method? Look in the footer for "Accessibility" or "Accessibility Statement." If it exists, does it include a contact method?

5. Check for a Contact Method Is there a clear way for someone to contact you? An email, a form, or a physical address? This is required under GDPR. Is there a clear way for someone to contact you? An email, a form, or a physical address? This is required under GDPR.

The Automated Scan (Free)

A more thorough scan checks multiple things at once:

- HTTPS configuration and security headers
- Cookie consent presence
- Privacy policy link in common locations
- Contact information availability
- Form handling (encrypted submission)
- Third-party scripts and data flows
- Accessibility basics (alt text, contrast, keyboard navigation)

The result is a summary of what is present and what is missing, with specific recommendations for each finding.

The 30-Minute Compliance Audit

When you are ready for a deeper check, go through this list:

Security: - [ ] SSL/TLS certificate is valid and properly configured - [ ] All pages redirect to HTTPS - [ ] Security headers (HSTS, X-Frame-Options, CSP) are present - [ ] Forms submit over HTTPS - [ ] SSL/TLS certificate is valid and properly configured - [ ] All pages redirect to HTTPS - [ ] Security headers (HSTS, X-Frame-Options, CSP) are present - [ ] Forms submit over HTTPS

Data & Privacy: - [ ] Privacy policy covers all data collection - [ ] Cookie consent blocks tracking before consent - [ ] Consent is recorded (date, time, what was accepted) - [ ] Data Processing Agreements exist with vendors - [ ] Privacy policy covers all data collection - [ ] Cookie consent blocks tracking before consent - [ ] Consent is recorded (date, time, what was accepted) - [ ] Data Processing Agreements exist with vendors

Accessibility: - [ ] Alt text on all meaningful images - [ ] Color contrast meets WCAG AA (4.5:1) - [ ] Website works with keyboard only (Tab through all interactive elements) - [ ] Heading hierarchy is logical - [ ] Forms have visible labels - [ ] Alt text on all meaningful images - [ ] Color contrast meets WCAG AA (4.5:1) - [ ] Website works with keyboard only (Tab through all interactive elements) - [ ] Heading hierarchy is logical - [ ] Forms have visible labels

Legal: - [ ] Contact information is published - [ ] Accessibility statement is published - [ ] Terms of service (if applicable) are published - [ ] Cookie policy is published - [ ] Contact information is published - [ ] Accessibility statement is published - [ ] Terms of service (if applicable) are published - [ ] Cookie policy is published

How Often to Scan

- **Quick scan: Every month (takes 5 minutes)** Every month (takes 5 minutes)
- **Automated scan: Every quarter** Every quarter
- **Full audit: Every 6-12 months, or when you redesign your site** Every 6-12 months, or when you redesign your site

Tools Mentioned

Tool | What It Does | Cost

EUComply (free) | Automated compliance scan | Free

WAVE browser extension | Accessibility check | Free

axe DevTools | Accessibility audit | Free / Pro

Lighthouse (Chrome) | Performance + accessibility | Free

SSL Labs | HTTPS certificate check | Free

Wave | Accessibility evaluation | Free

Key Takeaway

You do not need to be an expert to check your own compliance. The automated tools do the heavy lifting. What matters is that you run the checks regularly and fix what they find.

Next chapter: Building a compliance roadmap — how to prioritize and schedule the work. Building a compliance roadmap — how to prioritize and schedule the work.

Chapter 7: Building Your Compliance Roadmap

You have scanned your site. You have a list of issues. Now you need a plan. This chapter gives you a phased approach that works for any small or medium business.

The Three-Phase Approach

Phase 1: Immediate (Week 1)

Fix the things that expose you to the highest risk. These are the violations that regulators most commonly pursue, and they are also the easiest to fix:

Task | Time | Cost

Enable HTTPS (if not already active) | 30 min | Free

Add a privacy policy | 1-2 hours | Free or $10-50 template

Add a cookie consent banner | 1 hour | Free (Cookiebot, Osano)

Add alt text to key images | 30 min | Free

Publish contact information | 15 min | Free

Add an accessibility statement | 30 min | Free

Goal: All critical compliance gaps closed within 7 days. All critical compliance gaps closed within 7 days.

Phase 2: Foundation (Month 1)

Build the documentation and processes that protect you long-term:

Task | Time | Cost

Complete a cybersecurity risk assessment | 2-4 hours | Free

Write or customize a Data Processing Agreement | 1 hour | Free template

Sign DPAs with all vendors | 1 hour per vendor | Free

Set up incident reporting procedure | 1-2 hours | Free

Create a data retention schedule | 1 hour | Free

Add skip-to-content link on all pages | 30 min | Free

Fix keyboard navigation issues | 1-2 hours | Free

Goal: Full documentation and vendor compliance within 30 days. Full documentation and vendor compliance within 30 days.

Phase 3: Maintenance (Ongoing)

Task | Frequency | Time

Run a compliance scan | Monthly | 5 min

Review and update privacy policy | Annually | 1 hour

Test backup restore | Annually | 2 hours

Review vendor agreements | Annually | 1 hour

Full accessibility audit | Annually | 2-4 hours

Update accessibility statement | When changes occur | 30 min

Annual Compliance Budget

For a small business (1-10 employees), the annual cost of maintaining compliance:

Item | Cost

Free compliance scanner (EUComply) | $0

Cookie consent tool (free tier) | $0

Accessibility statement | $0

Privacy policy (one-time) | $0-50

Cybersecurity assessment (self-audit) | $0

Professional legal review (optional) | $500-2,000

Total (with legal review) | **$500-2,050/year**

Total (DIY) | **$0-50/year**

When to Call a Lawyer

You can handle most compliance yourself. Call a lawyer when:

- You process large volumes of sensitive data (health, biometrics)
- You have had a data breach
- You are negotiating contracts that reference compliance obligations
- You are preparing for a regulatory inspection
- You operate in multiple EU countries with different interpretations

Key Takeaway

Phase 1 takes a weekend. Phase 2 takes a month. Phase 3 takes a few hours per quarter. Compliance is not a project with a deadline — it is a process. But the initial setup is manageable, and the cost of not doing it is far higher than the cost of doing it right.

Next chapter: Templates and resources to save you time. Templates and resources to save you time.

Chapter 8: Templates and Resources

This chapter gives you the templates you need to get compliant quickly. You can adapt each one to your specific business.

Template 1: Privacy Policy Checklist

Your privacy policy should cover these sections:

- **Who we are — Company name, address, email, VAT/registration number** — Company name, address, email, VAT/registration number
- **What data we collect — List all personal data you collect (name, email, IP, cookies, payment data, etc.)** — List all personal data you collect (name, email, IP, cookies, payment data, etc.)
- **How we collect it — Forms, cookies, analytics, third-party tools** — Forms, cookies, analytics, third-party tools
- **Why we collect it — The legal basis for each purpose (consent, contract, legitimate interest, legal obligation)** — The legal basis for each purpose (consent, contract, legitimate interest, legal obligation)
- **How long we keep it — Retention periods for each data category** — Retention periods for each data category
- **Who we share it with — Each third-party processor, with links to their privacy policies** — Each third-party processor, with links to their privacy policies
- **Where data is stored — EU/EEA or third countries (with adequacy decision or SCCs)** — EU/EEA or third countries (with adequacy decision or SCCs)
- **Your rights — Access, rectification, erasure, restriction, portability, objection** — Access, rectification, erasure, restriction, portability, objection
- **How to contact us — Email, address, response time commitment** — Email, address, response time commitment
- **Complaints — How to file a complaint with the supervisory authority** — How to file a complaint with the supervisory authority

Template 2: Accessibility Statement Structure

Your accessibility statement should include:

- **Commitment — "We are committed to making our website accessible to all users..."** — "We are committed to making our website accessible to all users..."
- **Standards — "We aim to conform to WCAG 2.2 Level AA / EN 301 549"** — "We aim to conform to WCAG 2.2 Level AA / EN 301 549"
- **Current status — "Partially conformant" (if not fully compliant, list what is being worked on)** — "Partially conformant" (if not fully compliant, list what is being worked on)
- **Known limitations — Honest list of known issues (e.g., "PDFs from 2023 are not fully accessible")** — Honest list of known issues (e.g., "PDFs from 2023 are not fully accessible")

• **Feedback — Email or form to report issues** — Email or form to report issues

• **Enforcement — Contact for the national enforcement body** — Contact for the national enforcement body

• **Date — Date of last review and update** — Date of last review and update

Template 3: Data Processing Agreement (DPA) Coverage

A DPA with your vendors should cover:

• **Subject matter and duration of the processing** of the processing

• **Nature and purpose of the processing** of the processing

• **Type of personal data involved** involved

• **Categories of data subjects**

• **Obligations and rights of the controller** of the controller

• **Confidentiality obligations for the processor** obligations for the processor

• **Security measures the processor must implement** the processor must implement

• **Sub-processor authorization (general or specific)** (general or specific)

• **Data breach notification procedures** procedures

• **Data deletion upon termination** upon termination

• **Audit rights for the controller** for the controller

Where to Get Templates

• **EUComply Compliance Store (eucomplypro.com/store) — Full DPA, NIS2 clauses, NDA sets, EAA statement templates** (eucomplypro.com/store) — Full DPA, NIS2 clauses, NDA sets, EAA statement templates

• **European Data Protection Board (EDPB) — Free guidelines and template documents** — Free guidelines and template documents

• **Your national data protection authority — Country-specific guidance and templates** — Country-specific guidance and templates

• **ICO (UK) — Good practical guidance even for non-UK businesses** — Good practical guidance even for non-UK businesses

Quick Reference: Regulatory Deadlines

Regulation | Effective | Key Deadline

GDPR | May 2018 | Already in force

NIS2 | October 2024 | Already in force

DORA | January 2025 | Already in force

EAA | June 2025 | Already in force

Further Reading

- **GDPR: https://gdpr.eu — Practical guidance** https://gdpr.eu — Practical guidance
- **NIS2: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive** https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- **DORA: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora** https://www.eiopa.europa.eu/digital-operational-resilience-act-dora
- **EAA: https://ec.europa.eu/social/main.jsp?catId=1202** https://ec.europa.eu/social/main.jsp?catId=1202
- **WCAG 2.2: https://www.w3.org/TR/WCAG22/** https://www.w3.org/TR/WCAG22/
- **EN 301 549: https://www.etsi.org/standards/en-301-549** https://www.etsi.org/standards/en-301-549

Conclusion: You Are Ready

You have made it through four EU regulations. Here is a summary of what matters and what to do next.

The One-Page Summary

Regulation | Your Job | Time to Basic Compliance

GDPR | Privacy policy, cookie consent, DPAs with vendors | 1 weekend

NIS2 | Risk assessment, security measures, incident plan | 1 month

DORA | Resilience testing, vendor mapping (if in scope) | 1-2 months

EAA | Accessibility statement, WCAG AA fixes | 1 month initial, ongoing

The Most Important Thing

You do not need to be perfect. Enforcement is real, but it is not aimed at small businesses that are making a documented, consistent effort. The single most important thing you can do is:

- **Run a scan to see where you stand** to see where you stand
- **Fix the critical items (HTTPS, privacy policy, cookie consent)** (HTTPS, privacy policy, cookie consent)
- **Document what you have done and when you did it** and when you did it
- **Keep a schedule to re-check and re-fix** to re-check and re-fix

That is 80% of the value. The remaining 20% — the fine-tuning, the edge cases, the legal review — can wait until you have the resources.

What to Do This Week

- [ ] Run a free compliance scan on your website
- [ ] Fix any critical issues (no HTTPS, no privacy policy, no cookie consent)
- [ ] Publish an accessibility statement
- [ ] Set a reminder to re-scan in one month

What to Do This Month

- [ ] Complete a cybersecurity risk assessment
- [ ] Sign DPAs with your vendors
- [ ] Fix the most common accessibility issues
- [ ] Create a data retention schedule

What to Do This Year

- [ ] Full accessibility audit
- [ ] Test backup restore
- [ ] Review and update all documentation
- [ ] Re-run compliance scan quarterly

Final Thought

Compliance is a competitive advantage, not a burden. When a potential customer visits your website and sees a clear privacy policy, a working cookie consent banner, and an accessibility statement, they trust you more. They know you are professional. They know you take their data and their experience seriously.

That trust is worth more than any fine you are avoiding.

Now go scan your website. You will be surprised how much you already have right — and how easy the remaining fixes are.