

One organization. Dozens of websites, each with its own rules.

Some sites were built in-house. Others arrived through an acquisition or sat with an outside agency. Different brands use different vendors and processes — and a website-level compliance task quietly becomes an organization-wide digital risk problem.

01 What each stakeholder actually says

SIX ROLES, ONE PROBLEM

CISO

"I need visibility into digital risk across every brand without adding more tools for my team to manage."

PRIVACY & COMPLIANCE

"I need to know our websites are keeping pace as privacy requirements change."

COO · OPERATIONS

"I need a scalable way to manage this across acquired companies without recreating the process every time."

MARKETING & DIGITAL

"I need to keep campaigns and tracking running without becoming the compliance expert."

WEB & TECHNOLOGY

"I need something that's easy to deploy and doesn't create another maintenance burden."

GENERALIST LEADERSHIP

"I don't have a dedicated privacy or compliance team, so I need something that helps us manage this without adding headcount."

02 What changes with Clym

THE OPERATING MODEL

MAINTAINED FOR YOU

190+

global regulations supported

JURISDICTION-AWARE

including GLBA Financial Privacy Rule considerations

1,200+

third-party services classified

TODAY

A tool per brand

Duplicated vendor costs

Configure each site by hand

No portfolio-wide view

Each acquisition starts over

Ownership spread thin

WITH CLYM

One framework across properties

Reduced duplication

Per-property configuration, centrally managed

Centralized visibility

New brands join an existing framework

Consent, accessibility and DSRs in one place

ONE JAVASCRIPT SNIPPET · ~30-MINUTE DEPLOYMENT · 23 LANGUAGES · UPDATES AS LAWS CHANGE

SAID PLAINLY

The underlying compliance work does not disappear. Each website still needs attention, technologies change, and acquisitions keep arriving. What changes is how the organization manages that work — one operating model instead of a separate project per site.

CLYM FOR

Multi-brand insurance

Privacy · Consent · Accessibility · DSR



CLYM.IO

03 What running this centrally actually requires

THE SHORTLIST

- ✓ **Portfolio-wide visibility.** See what is happening across every digital property, not one at a time.
- ✓ **Less duplication.** Reduce repeated configuration and overlapping vendor management.
- ✓ **Room for each brand.** Individual properties stay configurable for their own audience and stack.
- ✓ **One place to work.** Manage related compliance responsibilities together rather than tool by tool.
- ✓ **Jurisdiction-aware settings.** Adapt what a visitor sees based on where they are.
- ✓ **Room to grow.** Add a new property without recreating the whole process.

04 Why this is harder in insurance

THREE COMPOUNDING FACTORS

Acquisitions carry baggage

Buying a business means inheriting its websites, policies, trackers, vendors and accessibility debt — all built independently of yours.

Visitors cross borders

Requirements vary by where the visitor sits, not where the company does. Maintaining that by hand, per site, becomes an ongoing operational load.

Industry obligations stack on top

Insurance organizations may also carry sector-specific duties, including under the Gramm–Leach–Bliley Act's Financial Privacy Rule.

05 Questions that come up

FREQUENTLY ASKED

Does an insurance company need a cookie consent banner?

Most insurance websites use cookies and tracking for analytics, marketing and basic function. Depending on where visitors are and how those technologies are used, privacy laws may call for disclosure, consent, opt-out or other controls. A consent platform presents the appropriate choices based on visitor location.

Is website accessibility a legal requirement for insurance companies?

It varies by jurisdiction, organization type and applicable law — the ADA, Section 508 and the European Accessibility Act among them. Many organizations treat accessibility as customer experience and digital risk regardless of whether a specific requirement applies.

How does data subject request handling change across brands?

A request can arrive through any website or brand in the group. Handling them through one process helps track deadlines, documentation and internal follow-up rather than discovering later that a brand handled it differently.

06 Where this usually starts

NEXT STEP

01 Inventory the portfolio

List the properties, who owns each, and which tools are already in place.



02 Scan a representative few

See how far consent, tracking and accessibility have drifted apart between brands.



03 Model the consolidation

Compare the current stack against one framework, including staff time.

THE BIGGER OPPORTUNITY

The larger an insurance organization becomes, the less practical it is to treat every website as an isolated compliance project. The opportunity is not simply consolidating tools — it is a consistent operating model for digital risk across the group, while individual brands keep the flexibility they need.