BRAIDED

August 2024

Unlock Revenue Opportunities with GDPR Compliance

A Case Study in Compliance Success

Braided Achieves GDPR Success for Bright Innovation Labs using Drata

In early 2024, a top client of US-based Bright Innovation Labs (Bright) asked Bright to complete a GDPR compliance assessment. Bright specializes in product research and fulfillment for the beauty industry. While Bright's operations are entirely within North America, their client list spans the world.

When a major international client of Bright sought to tighten up their data privacy efforts, they extended the same requirement to their entire supply chain, including Bright. Hackers often target smaller companies within a supply chain, typically with weaker data protections.

The client requested that companies within their supply chain complete a GDPR assessment to shine a light on the state of each company's data security. With client retention and data protection at stake, Bright prioritized this cybersecurity effort.

At that time, Bright had recently engaged Braided Technologies (Braided) to assist with technical infrastructure and cybersecurity concerns. During a technical meeting in March 2024, Simonette Ignacio, Bright's Director of Information Technology, informed Braided of the upcoming GDPR compliance assessment and Bright's need for technical assistance and evidence gathering.

Ignacio, who is experienced in heavy compliance efforts like the International Organization for Standardization (ISO), understood the substantial workload ahead. This included: Drafting, reviewing, and approving policies and procedures.

1. Reviewing and updating ancillary documents, like the Employee Handbook.
2. Performing a gap analysis to identify immediate tasks.
3. Implementing high-priority tasks.
4. Gathering and organizing evidence.
5. Completing the assessment using third-party compliance software.

Ignacio planned to shoulder this workload alongside her normal responsibilities. To say there was stress would be an understatement.

Why Comply?

Legal Protection:

Avoid the legal consequences and contractual defaults that result from non-compliance.

Financial Safeguards:

Compliance irregularities can result in fines and penalties ranging into seven figures—if not more.

Competitive Advantage:

Meet the stipulations of RFPs that require organizations to meet specific data protection standards.

Operational and Security Benefits:

Eliminate operational silos and inconsistencies within your business while improving your data security.

Marketing Edge:

Be seen as a responsible and trustworthy citizen of the world. Enhance your reputation and build consumer trust.

Avoid Bad Press:

Dodge the negative publicity associated with data breaches and non-compliance.

Braided's Expert Approach to Compliance

Braided is highly capable on the technical front and takes a compliance-first approach. They considered Bright's deadline, requirements, and what was needed to pass Bright's GDPR assessment successfully. Braided felt confident they could positively impact Ignacio and Bright.

The Pitch

Braided proposed a two-phase approach to GDPR compliance at Bright:

Phase 1: Ignition	
1. Roll out a compliance tool to assist with the efforts.	2. Craft policies and procedures focused on GDPR, and general compliance requirements needed for potential future frameworks (e.g., ISO 27001, CCPA).
3. Gather enough evidence to pass the assessment.	4. Orchestrate answering the urgent assessment.

Phase 2: Low Stress and Continuous Compliance	
1. Transition Bright to a proactive and continuous approach.	2. Develop procedures to make compliance business as usual and compliance efforts low stress.
3. Involve stakeholders across the entire organization.	4. Target additional compliance frameworks while leveraging current efforts.

Are North American Companies Impacted by GDPR?

GDPR impacts companies that are part of the supply chain of a global or European company, as well as contractors and subcontractors of such companies. GDPR's reach extends even further, serving as a benchmark for other compliance frameworks, such as CCPA (California's GDPR-comparable framework).

Braided can help you to better understand how GDPR relates to your business. Many compliance frameworks essentially mirror GDPR controls and penalties. Compliance with GDPR can also mean compliance with your particular frameworks.

Compliance Cadence

Braided proposed that Bright address its GDPR initiative by breaking it down into smaller, more manageable parts. Taking consistent, “small bites” to systematically chip away at compliance tasks. Additionally, Braided encouraged Bright to treat its compliance documents as living documents.

Engagement

Braided delivered a firm quote for tools and services to Bright about a month before the assessment date. After a rigorous approval process, and with only two weeks remaining to complete the necessary work, we began implementing the steps to enable Bright to pass their assessment.

To minimize cash flow impacts for Bright, Braided bills for consulting expertise together with the compliance tool on a monthly, recurring basis. This user-friendly approach aligns with our compliance philosophy, emphasizing consistent, manageable efforts.

Implementing Drata for Compliance

To make the magic happen, Braided outfitted Bright with Drata—a governance, risk, and compliance (GRC) platform. Drata automates compliance and evidence collection, providing a significant lift in both the initial and maintenance phases. Drata manages a company's policy documentation and integrates with its technology stack to provide:

Evidence Collection via Tech Stack Integrations	With a library of over 120 tools, Drata natively connects to the client’s tech stack to collect up-to-date evidence.
Unified Framework Controls	Drata breaks down multiple complex compliance frameworks into a common set of controls, allowing extreme clarity around how these frameworks overlap.
Policy Management	Drata provides a comprehensive library of over 20 auditor-approved policies. Clients can customize, deploy, and document directly within the platform.
Process Control	To help you get compliant fast, Drata highlights on its audit dashboard important tasks that need to be completed.

Braided felt that Drata’s unified framework approach would boost Bright’s future compliance efforts—which include several additional compliance frameworks—with a minimum of repetitive work. Braided focused on crafting policy and procedure drafts within Drata, meeting Bright’s specific compliance needs.

The Assessment

Bright and Braided gathered technical and procedural evidence to support the approved policy and procedure documents. Completing the GDPR assessment took less than one business day to complete, and the deadline was met!

Compliance Achieved

Four weeks after completing the GDPR assessment, Bright received a passing grade. Ignacio was pleased, and Bright was well-positioned to start making compliance a part of their daily operations.

Braided's Approach: Compliance-as-a-Habit

At Braided, we are transparent in our approach to compliance. Compliance should become a reflex—a set of simple habits that you consistently implement. We view your policies and procedures as living documents that should be regularly reviewed and updated. Developing these habits pays off by ensuring that future compliance assessments are smooth and do not disrupt your business operations.

Our process begins by establishing policy and procedure documents. Creation of these documents serves as an opportunity to eliminate information silos, making your business more efficient and resilient in the face of change. These documents are the foundation of all compliance work.

Once your goals are identified and codified, we work with you to:

- Onboard the integration of the GRC tool with your tech stacks to monitor compliance.
- Identify and interface with key stakeholders (e.g., HR, technology, and operations).
- Review cyber and general insurance coverages.
- Assign responsibilities throughout the organization.
- Work with stakeholders to update procedures.
- Gather compliance evidence.
- Perform a full gap analysis to identify remediation tasks.

With compliance in place, we then schedule regular reviews of your documents while evaluating them against current business needs to identify improvement opportunities.

This is just the start of how Braided can simplify compliance with minimal interruption to your daily work. We keep meetings short and to the point, respectful of your time.

Once in place, Braided's approach and fractional compliance officers work continuously in the background, requiring no dedicated teams or extensive time commitments from you.

We believe setting reasonable, easily- achieved compliance deadlines is the path to continual improvement within an organization's fabric. We recommend letting Braided guide you through the process, making compliance into a painless effort.

Slow and steady wins the race!

GDPR's Global Impact

Privacy is a top priority for individuals online, leading companies to implement robust measures to protect personal and sensitive information. The European Union's General Data Protection Regulation (GDPR), enforced since 2018, mandates strict data protection practices, with hefty fines for non-compliance. This regulation applies to any entity handling EU citizens' data, regardless of location, and has become a global benchmark for privacy standards. As a result, GDPR compliance often ensures adherence to similar regulations worldwide, effectively reducing the risk of data breaches across various industries.

Delivering a Competitive Advantage Through Habitual Compliance and Technology Innovation.

Visit braided.tech or set up a free consult to see how Braided's compliance services can fit your exact needs.