DATA PRIVACY DAY: TOP 5 CONSIDERATIONS AND CHECKLIST FOR 2026

© 2026 Constangy, Brooks, Smith & Prophete. All Rights Reserved.

Data Privacy Day:
Top 5 Considerations and Checklist for 2026

We recently wrote about trends we expect to see in 2026. To mark the occasion we are providing our thoughts and recommendations on key actions that any organization should be taking to support both compliance and capabilities for managing cybersecurity and data privacy.

1. Validate Your Website Compliance

Almost anyone can access your website, making it a prime target for scrutinizing your organization's compliance posture. The past year has seen a significant increase in activity from both regulators and litigious plaintiffs—to help stay out of their crosshairs:

- ☐ Review your privacy policy, cookie banners and legal disclosures—these are not "boilerplate" terms, and need to satisfy specific requirements under applicable laws.
- ☐ Understand the use of cookies and tracking technologies—how individuals are notified and what options they have to manage non-essential cookies/tracking is a key priority for regulators as well as the basis for the proliferation of "CIPA" type lawsuits.

2. Stay Ahead of Regulations (and Regulators)

The regulatory landscape is becoming increasingly complex. New laws are being passed, existing regulations are being amended to keep pace or adapt to AI and other emerging technologies, and various regulators are issuing more detailed rules than ever.

- ☐ Conduct an assessment to understand compliance obligations or risks—while a deep-dive analysis may be particularly suited for organizations in highly-regulated industries (e.g., finance, healthcare and professional services) even a simple "health check" can be extremely beneficial to understanding your current exposure in order to develop an informed (and realistic) prioritized remediation or implementation plan.
- ☐ Validate that you have a process for "horizon scanning" and identifying if laws have changed or if changes to your organization make you subject to requirements—ensure that you are able to efficiently update or adapt your compliance and governance programs accordingly.
- ☐ Regulators' new rules are more expansive, and being backed up with more stringent enforcement—make sure to verify whether you are subject to specific filing obligations (e.g., if you are a data broker), that you are prepared to submit all your annual certifications on time, and that you understand new reporting obligations that are taking effect (notably audits/assessments in California, and CMMC 3 for federal contractors).

Data Privacy Day:
Top 5 Considerations and Checklist for 2026

3. Make "Resilience" a High Priority

Organizations are subject to more and more accountability for compliance requirements as well as mitigating vulnerabilities and risk across the entire data lifecycle.

- ☐ Make sure your organization is educated about the evolving risk landscape—not only should you be aware of new "high tech" threat actors and exploits, but also how "low tech" threats like social engineering remain a top risk and are being augmented by AI.
- ☐ Review your incident and continuity policies/procedures—incidents are inevitable, so proactively developing robust response and continuity plans helps address regulatory requirements, contractual obligations, as well as strengthen defensibility against investigations or legal actions when (not if) an incident occurs.
- ☐ Simulate incidents to strengthen defense—tabletop exercises should be conducted annually to make sure both technical and executive teams are able to act confidently and efficiently in chaotic situations.
- ☐ Determine what data you really need, and dispose of anything expired. Less data = less risk! Data retention and minimization is not just required by statute, but can help reduce likelihood and negative impacts of an incident (while also providing positive effects by streamlining data management and costs at the same time).

4. Manage Supply Chain Risks

Organizations are more reliant than ever on integrations across a wide network of partners, service providers, and other third parties. While this interconnectedness can help businesses expand their reach and efficiency, it also creates avenues for heightened risk.

- ☐ Evaluate your due diligence and procurement processes—make sure your organization is not becoming enmeshed in arrangements that jeopardize your compliance obligations (or do not align with the business' risk tolerances) particularly when it involves the highly-fluid landscape of AI.
- ☐ Ensure that your agreements include robust data protection terms—particularly if you are sharing personal data with any third parties, your contracts may have to include specific requirements or otherwise set standards that are high enough to satisfy statutory obligations.
- ☐ Make sure you understand your contractual obligations—in addition to reading draft terms very closely (since more and more negotiations involve shifting indemnification and liability as far as possible) it is important to understand what your reporting obligations may be in the event of an incident (which often have extremely short deadlines across hundreds if not thousands of contracts).

Data Privacy Day:
Top 5 Considerations and Checklist for 2026

5. Don't Neglect the Basics

While requirements will continue to evolve and inevitably become more sophisticated or form a larger complex ecosystem of regulations, certain fundamentals will remain the same.

- ☐ Make sure your organization has a comprehensive governance program documented—formal policies and procedures demonstrate that your organization understands its obligations and has processes in place to manage requirements or risk, which can support a stronger position of defensibility in an investigation or litigation.

- ☐ Make sure your entire workforce completes annual training—policies and procedures only go so far if personnel are unaware that they exist, and employees cannot exercise good judgment in ambiguous situations if they do not have an understanding of what the organization's standards and expectations are.

6. BONUS: Embrace Change and a Long-Term Vision

For data privacy practitioners, the rapid changes in laws and enforcement is what makes our work exciting, but we recognize that it can seem overwhelming for many others whose day-to-day may not involve such issues all the time. It is helpful to keep things in context:

- ☐ Data privacy is fundamentally about "trust"—your organization's competitiveness is reliant onstrengthening consumer, employee, and stakeholder confidence in your ability to uphold the highest standards of privacy, security, and ethics.

- ☐ Change does not have to be "all or nothing"—developments such as the proliferation of Artificial Intelligence may feel like the Wild West, but organizations should not let uncertainty be paralyzing or to conversely try to "boil the ocean" in response.

- ☐ The best approach is "risk based" and proactive—you will not be able to do everything at once, but developing a prioritized plan that is both adaptable and scalable will provide clarity, assurance, and defensibility.

- ☐ If you think compliance is expensive (or hard) try noncompliance—plain and simple.

© 2026 Constangy, Brooks, Smith & Prophete. All Rights Reserved.