WEB COMPLIANCE FOR LAW FIRMS

BY BRYCE RIDDLE AND JESSICA KLANDER

In today's digital age, operating a website is an essential tool for lawyers to attract new clients and grow their practice. However, as data privacy regulations, accessibility standards, and compliance laws continue to evolve at both state and federal levels, ensuring your website meets these legal obligations is critical. In recent years, lawsuits targeting businesses over website content, accessibility, and compliance violations have surged, putting firms at significant legal and financial risk. This article highlights significant compliance issues law firms must address when managing a website.

COMPLIANCE WITH DATA PRIVACY LAWS (CCPA, GDPR, CPRA)

Data privacy is one of the most pressing legal obligations for websites. With laws such as the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and the European Union's General Data Protection Regulation (GDPR) governing how personal data is collected, stored, and processed, attorneys need to ensure their websites meet these stringent requirements.

Transparency and Consent Management

Under the CCPA, attorney websites must inform users about the data being collected and provide mechanisms for managing consent. This includes offering a "Do Not Sell My Personal Information" link to give users the option to opt-out of data sharing for marketing purposes and providing control over cookies and other tracking technologies so users can selectively opt-in or out.

The GDPR, applicable to websites targeting EU users, requires even more explicit consent mechanisms. Users must actively opt-in to the collection of personal data, and websites should allow them to withdraw consent at any time easily. Ensuring that cookie consent banners are clear and detailed about the types of data collected is crucial.

User Rights

Under both the CCPA and GDPR, users have rights to access their personal information collected by the website, request corrections or deletion of data, and be informed of data breaches in a timely manner. To comply, websites should provide clear instructions and functionality for users to exercise these rights. This can be accomplished by having user-friendly forms for requesting data access or deletion and providing contact information that directs a visitor to the relevant department that handles such requests.

Data Security

Websites must also implement strong security measures to protect personal data. This includes using HTTPS/SSL certificates for secure connections, conducting regular security audits, and encrypting sensitive personal and financial data.

ADA COMPLIANCE: WEBSITE ACCESSIBILITY

The Americans with Disabilities Act (ADA) requires websites be accessible to individuals with disabilities. Inaccessible web content to people with disabilities means that they are denied equal access to information, so it is imperative that people using screen readers or other assistive technologies be able to navigate and use a website effectively. Websites should therefore include features such as:

- **Text alternatives for images and media:** For any images or non-text content, alt-text, captions for videos, transcripts, and proper use of heading tags (H1, H2, etc.) should be included to help screen readers interpret website content.
- **Keyboard navigability:** Users who cannot use a mouse should be able to navigate the entire website using a keyboard alone.

• **Readable text:** Websites must maintain appropriate color contrast between text and background for readability and allow users to adjust font size easily. Websites should also convey information through more than one color, provide legible fonts, and avoid content that can trigger seizures.

Several tools exist to test ADA compliance by identifying issues like missing alt-text or poor color contrast. Periodic accessibility audits can also help maintain long-term compliance. At this time, the Web Content Accessibility Guidelines (WCAG) is the go-to resource covering every conceivable aspect of accessibility.

TERMS AND CONDITIONS, DISCLAIMERS & PRIVACY POLICIES

Every website should have clear and comprehensive legal documents, including Terms and Conditions, Disclaimers, and a Privacy Policy. These are not just legal formalities – they provide critical protections for your business and ensure transparency with users.

Terms and Conditions

A website's Terms and Conditions sets forth the legally binding agreement between websites and visitors, and typically includes intellectual property rights, liability limitations, and explains what users can or cannot do on a website. For attorney websites, it's particularly important to clarify that users should not submit confidential information through website forms without first establishing a formal attorney-client relationship.

Disclaimers

Attorney websites must also include disclaimers to clarify that the information provided on the website does not constitute legal advice and that visiting the website does not create an attorney-client relationship. This protects the attorney from potential liability arising from misunderstandings about the scope of the information provided.

Privacy Policy

At a minimum, a well-crafted privacy policy should explain:

• What types of data the website collects (e.g., personal information, cookies).

• How the data will be used, including any third-party sharing.

• How users can opt out of data collection or request their information be deleted.

ABA GUIDELINES FOR ATTORNEY WEBSITES

In addition to general legal compliance, attorney websites must also comply with the ABA's Model Rules of Professional Conduct (as well as the firm's own state's rules), which govern how attorneys can ethically advertise their services. This includes:

Truthful Advertising (Rule 7.1): Attorney websites must ensure that all information provided is truthful and not misleading. Claims about the attorney's success rate, abilities, or specialization should be carefully worded to avoid creating unrealistic expectations.

Specialization (Rule 7.2): If an attorney claims to be a specialist in a certain area of law, they must be certified by an appropriate body. Websites must include disclaimers if such certifications are not held so that users understand the attorney's qualifications.

Prohibition of Direct Solicitation (Rule 7.3): ABA Rule 7.3 restricts direct solicitation through real-time communication, which can sometimes apply to chatbots or live consultation features on websites. Attorneys should be cognizant that any such communications adhere to ABA standards and do not violate rules on direct client solicitation.

Client Confidentiality (Rule 1.6): Websites should clearly state that submitting information via contact forms does not establish an attorney-client relationship, and users should avoid submitting sensitive information until they formally engage the attorney.

DATA PRIVACY IS ONE OF THE MOST PRESSING LEGAL OBLIGATIONS FOR WEBSITES.

CONCLUSION

Websites offer attorneys powerful tools to grow their practices and connect with clients, but navigating the complex legal landscape surrounding website compliance is essential. By proactively addressing critical issues like data privacy, accessibility, and ethical standards, attorneys can significantly reduce legal risks while enhancing client engagement and driving business growth. Ensuring your website complies with these regulations not only protects your firm from costly lawsuits but also strengthens your online presence and positions your practice for long-term success.

Disclaimer: *The information conveyed in this article is not an exhaustive treatment of the issues this article focuses on and is not intended to be relied upon as legal advice. There is no attorney-client relationship between Bassford Remele, P.A. and any reader of this article.*

Bryce Riddle, a shareholder and litigator at Bassford Remele, co-chairs its data privacy and cybersecurity practice group. He practices complex commercial litigation, data privacy and cybersecurity, and employment litigation. Bryce also has class action experience in data breach and consumer privacy litigation. briddle@bassford.com, 612.376.1624. Jessica Klander is the chief operating officer at Bassford Remele and co-chair of its Consumer Finance Practice Group. Her practice focuses on defending lawyers, financial entities, healthcare providers, and other organizations against consumer financial protection claims, malpractice, and professional liability claims. She counsels organizations on privacy, data security, and governmental and regulatory affairs. jklander@bassford.com, 612.376.1660.


BRYCE RIDDLE


JESSICA KLANDER