Digioh Security and Compliance: GDPR, CCPA, ADA, and SOC 2 Type II

Last Modified on 06/24/2026 4:30 pm EDT

Overview

Digioh is committed to helping our customers collect, store, and manage data securely while meeting key global privacy and accessibility standards. This document explains how Digioh ensures compliance with major frameworks—including GDPR, CCPA, ADA/WCAG 2.1, and SOC 2 Type II—and outlines best practices for maintaining data protection and accessibility across all campaigns.

When to use this document

Use this guide to understand how Digioh supports data privacy, accessibility, and enterprise-grade security standards. This page is relevant for compliance officers, IT admins, and marketing teams responsible for ensuring campaign data protection and regulatory adherence.

1. GDPR and CCPA Compliance

Digioh provides the tools you need to comply with international data privacy laws such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

How Digioh Supports GDPR and CCPA

- **Affirmative Consent (Opt-In):** Digioh forms support explicit consent checkboxes and links to your privacy policy. This helps ensure compliance with GDPR's affirmative opt-in requirement.
- **Right to Access and Deletion:** All data collected through Digioh is accessible within your account and can be deleted upon request.
- **Data Storage and Security:** Data is stored on secure, SOC 2 Type II–certified servers.
    - Data Storage can also be disabled upon request, allowing Digioh to act as a pass-through.
- **Data Obfuscation:** Personally identifiable information (PII) can be obfuscated or disabled entirely using your account's Data Storage Settings.
- **Custom Privacy Messaging:** Add custom privacy notices and consent fields directly in your form editor.

Note: While Digioh provides the technical capabilities for compliance, customers are responsible for configuring their campaigns in accordance with applicable laws.

2. ADA and WCAG 2.1 Accessibility

Accessibility is a core part of Digioh's platform design. Our widgets, pop-ups, and inline forms are built to meet ADA and WCAG 2.1 AA accessibility guidelines.

Accessibility Features

- **Screen Reader Support:** Digioh's ADA extension automatically sets ARIA labels and tabindex attributes to ensure full keyboard and screen reader accessibility.
- **Keyboard Navigation:** All widgets can be navigated using standard keyboard controls.
- **Contrast and Readability:** Form fields, buttons, and text are designed to meet WCAG contrast ratios.

3. SOC 2 Type II Certification

Digioh maintains SOC 2 Type II certification, verifying that our systems and processes meet industry standards for security, availability, and confidentiality.

What This Means for You

- **Secure Data Centers:** All Digioh infrastructure is hosted in SOC 2–compliant environments.
- **Regular Audits:** Our controls are independently audited annually to ensure continued compliance.
- **Access Controls:** Strict role-based access permissions prevent unauthorized data exposure.
- **Incident Response:** Digioh maintains a robust incident response process aligned with SOC 2 requirements.

A copy of Digioh's SOC 2 Type II report is available to customers upon request.

4. Account Security: SSO and MFA

Digioh offers secure authentication options for enterprise and team accounts:

- **Single Sign-On (SSO):** Integrate Digioh with your company's identity provider (e.g., Okta, Azure AD, Google Workspace).
- **Multi-Factor Authentication (MFA):** Protect user accounts with an additional verification layer.

To enable these features, contact your Digioh Customer Success Manager or email support@digioh.com.

5. Additional Security Measures

Beyond compliance frameworks, Digioh implements additional controls to protect customer and end-user data:

- **TLS Encryption:** All data is transmitted over HTTPS with TLS 1.2+ encryption.
- **Data Minimization:** Customers can choose to collect only essential data fields.
- **Access Logging:** User access and activity within the Digioh platform are logged for audit purposes.

Automated Backups: Redundant daily backups protect against data loss.

6. Data Privacy & Governance Framework

Digioh is built with privacy by design. We act as a data processor on behalf of our customers and process end-user data solely according to customer instructions and applicable data protection laws,

including GDPR and CCPA/CPRA. Digioh is architected to support pass-through data collection, meaning end-user personal data can be transmitted directly to customer-controlled systems without being persistently stored by Digioh.

Where limited data is retained to operate and secure the platform (such as configuration data, operational logs, and aggregated or de-identified analytics), Digioh enforces strict access controls, encryption in transit and at rest, and continuous security monitoring.

Related Documentation

- Digioh's Data Security
- DDoS and Bot Protection
- Digioh SSO Configuration