



CCPA compliant email security

Remain CCPA compliant by preventing breaches, protecting regulated data, fulfilling DSARs, and auditing your email network.

The California Consumer Privacy Act AB-375 (CCPA) will transform the way organizations share personal data via email, with huge penalties and daunting litigation putting hard-earned reputations on the line for those unable to protect residents' new privacy rights. Egress helps organizations achieve CCPA compliance for their email systems by preventing data leakage, automating protection for personal data, and generating reports to fulfill Data Subject Access Requests (DSARs) and for broader compliance requirements.



Using Egress, organizations can achieve CCPA compliance through:

- ✓ Rapid discovery and mapping of data flows and risks for emails and attachments sent internally and externally
- ✓ Recipient analysis to prevent emails being sent to the wrong people
- ✓ Content analysis to ensure message body and attachments are appropriate for email recipients
- ✓ Applying the correct protection to personal data
- ✓ Easy-to-use message-level encryption for email body and attachments, including large files
- ✓ Advanced rights management, including watermarking; email recall; time and date restrictions; and preventing actions, such as forwarding
- ✓ Fulfilling DSARs for personal data shared via email, including redaction of non-pertinent information
- ✓ Compliance reports for ongoing improvements

Customer story: Insurance provider

Situation

- ✓ Under regulatory pressure to enhance email security
- ✓ Needed to analyze plaintext and encrypted content
- ✓ Required to produce reports to demonstrate ongoing compliance

Solution

- ✓ Dynamic detection of data leakage
- ✓ Message-level encryption for sensitive data shared internally and externally
- ✓ Reporting across all email content and attachments, for compliance purposes and DSAR fulfillment

Results

- ✓ Prevents emails and attachments being sent to unauthorized recipients
- ✓ Protects personal data shared by email
- ✓ Monitors ongoing compliance
- ✓ Provides assurance for clients that personal data is protected

How Egress helps with CCPA compliance

Section	Relevant requirements	How Egress helps
1798.100	<p>Right to access and applicability</p> <p>Consumers can request that the organization disclose the categories and specific pieces of PI collected, including web request submissions.</p>	<p>Egress Email Classification provides simple and efficient data mapping.</p> <p>Egress eDiscovery and Analytics rapidly produces DSAR results (including encrypted emails).</p>
1798.105	<p>Right to request disclosure of info</p> <p>Consumer can request information on what specific PI an organization has collected.</p>	<p>Egress Email Classification can be used for data mapping.</p> <p>Egress Secure Web Form can be used by consumers to submit DSARs.</p> <p>Egress eDiscovery and Analytics can provide DSAR responses within minutes, including content in encrypted emails and redaction of unnecessary PI.</p>
1798.105 1798.120 1798.130	<p>Right to deletion</p> <p>Consumers can request the organization delete PI collected about them and to not to sell their PI. To comply with CCPA, the organization can associate information about the data subject with other data held.</p>	<p>Egress eDiscovery and Analytics provides fully automated workflows for rapid DSAR fulfillment, including redaction for non-pertinent information and secure communication with requestors.</p>
1798.140	<p>Definitions</p> <p>Organizations can use PI in order to detect security incidents; protect against malicious, deceptive, fraudulent or illegal activity; and prosecute those responsible for that activity.</p> <p>Users can submit DSARs in multiple ways.</p>	<p>Egress greatly reduces the likelihood that employees will accidentally send data to the wrong person, or will fall victim to a spear phishing attack.</p> <p>Egress Secure Web Form provides a safe method to submit DSARs</p>
1798.150	<p>Civil action</p> <p>Any consumer whose non-encrypted or non-redacted PI is subject to unauthorized access and exfiltration, theft or disclosure (because the organization violated its duty to secure) may institute a civil action.</p>	<p>Egress reduces and simplifies responses to litigation claims via automated e-discovery. Egress also empowers legal and compliance teams with easy-to-use tools that don't rely on IT involvement. Egress produces legal investigation data within minutes.</p>

About Egress

Egress takes a people-centric approach to data security – helping users receive, manage and share sensitive data securely to meet compliance requirements and drive business productivity. Using machine learning, Egress ensures information is protected relative to the risk of a data breach and reduces user friction to ensure smooth adoption.



info@egress.com

1-800-732-0746

@EgressSoftware

www.egress.com

