Table 1. Applicability of encryption tools to data protection regulations

Regulation	Requirements	Encryption tool fit		
		Encrypted Text Fields	Salesforce	Protecting data in Apex
NYCRR 500	NIST-compliant, 256-bit Advanced Encryption Standard (AES encryption)	✗ (up to 128 bit)	✓	✓
	Store encryption keys apart from the encrypted financial data in a security device specifically designed for this task	? [1]	✓	✓
	The Key Management Interoperability Protocol (KMIP)	✓ [2]	✓ [2]	✓ [2]
	Encryption of sensitive data both in transit and at rest	✗	✓	✗
PCI DSS	AES encryption (128 bit and higher)	✓	✓	✓
	PGP implemented	✓ [3]	✓ [3]	✓ [3]
	Keep encryption keys and data separate	? [1]	✓	✓
HIPAA	End-to-end encryption (E2EE)	✓ [3]	✓ [3]	✓ [3]
	AES encryption (128 bit and higher)	✓	✓	✓
	OpenPGP implemented	✓ [3]	✓ [3]	✓ [3]
GDPR5 [5]	S/MIME implemented	✓ [4]	✓ [4]	✓ [4]
	End-to-end encryption (E2EE)	✓ [3]	✓ [3]	✓ [3]
	AES encryption (128 bit and higher)	✓	✓	✓
CCPA	End-to-end encryption (E2EE)	✓ [3]	✓ [3]	✓ [3]
	AES encryption (128 bit and higher)	✓	✓	✓

Source
brimit.com

Footnotes:

[1] Salesforce most likely stores them separately and doesn't provide control over the keys.

[2] Requires a third-party solution, which stores software on a KMIP-compliant server.

[3] Features out-of-the-box functionality to ensure regulatory compliance.

[4] Not available out of the box, but there's a workaround.

[5] There are no explicit requirements for encryption. What's required is pseudonymization. If pseudonymization is performed by means of encryption, that’s fine. The developers need to choose the most common encryption method.

Source
brimit.com

brimit