Everything the Finance Industry Should Know About SOC 2, GDPR and Data Security

Financial institutions are handling a growing amount of highly sensitive data on a daily basis. Data privacy must be a top priority for them. Not only are financial companies some of the biggest targets for cyberattacks, but they also risk severe consequences if their customers' data gets into the wrong hands.

Financial institutions that suffer a breach are likely to experience damaged reputations, long-term declines in consumer trust, fines and monetary penalties. To protect against threats, understanding different privacy standards that might apply to them and their vendors, such as **SOC 2** and the **GDPR**, can make all the difference.

As a key accessibility partner for financial institutions, Verbit takes data security seriously, and ensures that its captioning and transcription services meet or exceed all relevant protection standards.

Frightening Financial Data Breach Facts

Financial motivations lead to **71%** of data breaches.	The banking industry has the highest average data breach costs at **$18.3 million** per company each year.
47% of financial data breaches targeted banks.	In 2017, **65%** of the US's top 100 banks failed web security tests.
80% of US adults are afraid that companies cannot secure their financial data.	Financial companies face **300x** the risk of cyber-attacks compared to other types of businesses.[1]

SOC 2 reports and the GDPR both serve roles in protecting your data. However, they are different. Take a moment to read and identify how each might impact your business practices.

What are SOC 2 Reports?

Like most modern businesses, financial institutions are not islands, but rather connect to a complex and intertwined network of tech companies and SaaS providers. Using efficiency-boosting technology isn't optional in today's fast-paced world, so companies must know how to protect the sensitive information they handle.

Unfortunately, a financial institution's security is only as strong as its weakest link. Gauging the level of security for outside vendors is now a critical practice. SOC 2 reports offer an opportunity to vet potential partners' security to ensure that its security is up to snuff.

Make sure to understand the difference between the two types of SOC 2 reports: SOC 2 Type I reports describe but don't test a vendor's security practices.

SOC 2 Type II reports involve a lengthy auditing process that details the effectiveness of the current protections.

Soc 2 Type II reports look at five different trust criteria:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

Although all reports will include security, the other four may or may not appear on the report depending on the type of vendor and their relevance.

1. Top 25 Financial Data Breach Statistics

Who Needs a SOC 2 Report?

When it comes to data security in the US, the laws are a complex web of federal, state and other regulations, but there is no comprehensive legislation that protects information. Even if no relevant law requires SOC 2 reports, they are an essential part of data protection, and customers typically request them from vendors that they outsource to perform specific tasks.

In most cases, financial service providers, insurance companies, banks and investment advisors will require SOC 2 reports from any outside vendors. Vendors that should have SOC 2 reports include:

- FinTech services
- Loan services
- Insurance claim processors
- Payroll processors

Beyond these examples, any SaaS provider that touches confidential information should be able to provide these reports. This expectation extends to accessibility service providers that offer captioning and transcription solutions for meetings, interviews and other recorded audio content.

Also, although SOC 2 reports aren't mandatory, other legal regulations might apply, even to US-based institutions.

What is the GDPR?

In contrast to the US, the EU has a comprehensive law related to data privacy. In fact, the EU treats data privacy as a human right, and therefore, the penalty for violating the General Data Protection Regulation (GDPR) is severe. Non-compliance can result in fees of up to 20 million euros, or 4% of the "total worldwide annual turnover," whichever is larger.[2]

The law became effective in May 2018 and has already led to massive fines for some leading companies. Amazon[3] received the largest fine to date, which amounted to 746 million euros- although the retail giant is appealing that decision. Other companies that have faced large fines since the law's inception include Google, WhatsApp, British Airways, Caixabank, Banco Bilbao Vizcaya Argentaria and H&M.[4]

The EU publishes a four-category checklist for businesses to comply with the GDPR.

2. Data Privacy Laws by State, **3.** GDPR Fines **4.** 25 Biggest GDPR Fines

The GDPR checklist categories and examples[5]

Category	Examples
Lawful basis & transparency	Companies must be transparent about data they collect and have legal justifications for gathering personal information
Data security	Businesses need to account for data protection at all times, encrypt personal information where possible and have a process for notifying the appropriate authorities in the event of a breach
Accountability and governance	Organizations should have data privacy policies that apply to their employees and vendors and appoint someone responsible for ensuring GDPR compliance within the organization
Privacy rights	Customers should be able to request information about what data the organization has about them, ask for it to be deleted, correct data and request that the company not process their data

5. GDPR checklist for data controllers

Who needs to comply with the GDPR?

The GDPR impacts all companies that collect data from persons in the EU. The reach of the law is broad and applies to foreign companies that do business in the EU. In fact, the language does not even limit the protected class to citizens or residents of the EU but includes people in the EU, which could extend to visitors.

The EU created a checklist specifically for US companies.[6] The law even addresses the EU's ability to enforce the GDPR against foreign companies through treaties. Fortunately, companies based in the US that meet the GDPR's standards will be in an excellent position to also comply with those of several recent state laws that create similar requirements. California, Colorado and Virginia are some of the jurisdictions that have already enacted statewide data privacy laws.

Financial institutions handle some of the most sensitive and at-risk personal data. As your organization strives to become more inclusive and meet the requirements of accessibility laws, consider incorporating tools like captioning, transcription and audio description into your business. These tools will allow more potential investors, job candidates and customers to connect with your organization.

Verbit's SOC 2 reports and GDPR compliance make it an essential partner for leading financial institutions striving to meet accessibility standards, build more inclusive workplaces and reach a wider audience. Contact us to learn more about how our solutions for financial institutions protect data privacy, while also helping to promote greater inclusivity. Together, we can make your earnings calls, meetings, webinars, and marketing videos more accessible.

6. GDPR compliance checklist for US companies