Trellix

CHECKLIST

7 essential steps to data compliance

A holistic data protection checklist

It takes planning and effort to build a resilient digital environment that protects your customers' sensitive data. But the benefits—to your reputation, your finances, and to customer satisfaction—are definitely there.

Staying ahead of evolving threats requires coordinated planning and effort, along with the right technology solutions. To make sure you're covered, here are seven key steps you can take to keep your organization compliant and your sensitive data safe.

- [ ] **Help your organization understand the importance of compliance**
- [ ] **Get buy-in from leadership to implement a data protection solution**
- [ ] **Identify the regulations that apply to your area and industry**
- [ ] **Choose the right technology solution**
- [ ] **Empower employees to maintain compliance**
- [ ] **Establish procedures for responding to data breaches**
- [ ] **Run compliance reports regularly**

✔ Why start here? Because non-compliance poses an existential risk to your org.

1. Help your organization understand the importance of compliance

Effective data protection is about more than just technology. It means getting everyone who touches your information into a data-stewardship mindset.

The bottom line on why you should care: non-compliance can be expensive in many ways. And threats to your data are everywhere. They range from careless or even malicious actions by employees to threats from outside attackers.

Let's run through some common outcomes of non-compliance:

- **Fines.** Your organization must be able to prove good stewardship, including responsible data hygiene and protection. If you're found non-compliant, you may be fined until you can prove you've corrected the issue.
- **Legal action.** Depending on the state, federal, and international laws that apply, you may have to meet some requirements, like letting customers know their data has been compromised. You could also be the target of a civil lawsuit. It's smart to have attorneys advise you after a breach, which costs you money.
- **Reputation loss.** Depending on your industry and how you handle a breach, it's possible to recover long term. But in the short term, most organizations can expect a large drop in consumer confidence. Recovering lost trust takes time, effort, and money, with no guarantee of success.
- **Reduced stock price.** Comparitech found that after major data breaches at large enterprises, 21 out of 40 incidents resulted in worse stock performance compared to the NASDAQ in the following six months versus the previous six months.[1]

✔ Give your org its best chance at successful adoption by cultivating advocates in the C-suite.

2. Get buy-in from leadership to implement a data protection solution

Effective compliance needs strong support from the top down.

That's because to do it right, you'll need to weave data loss prevention (DLP) into everything you do. You'll need resources to help you educate employees, update your processes, and keep your efforts on track as threats and regulations evolve.

Leadership will have to approve budget and time to implement a robust DLP solution. They should also be part of updating your information security policies. Your executives can also encourage cooperation from departments across the organization that will need to be involved. And the more your leadership is engaged, the greater the chances that your DLP efforts will be unified across the organization.

1. How data breaches affect stock market share prices, Comparitech, February 2022

✔ Do a full background check on compliance requirements before you choose new solutions or uproot processes.

3. Identify the regulations that apply to your area and industry

It's important to know and follow all the standards that apply to your organization. Compiling your full list will take some research, especially in a global economy where traditional borders don't always apply. Here is a sample list of some of the regulations your organization might be subject to:

- **General Data Protection Regulation,** a EU-based data protection law
- **Japan Act on the Protection of Personal Information**
- In the United States, **California, Colorado, Connecticut, Utah, and Virginia** have enacted comprehensive consumer data privacy laws
- **The Gramm-Leach-Bliley Act/Financial Modernization Act** applies to the financial industry, such as companies that handle and manage money
- **Health Insurance Portability and Accountability Act (HIPAA)** governs healthcare providers

Keep in mind that:

- If you do business with companies that are subject to these laws, you must comply with the regulations, too.
- Local laws apply to the areas where you conduct business and/or where your customers reside, not just where your headquarters are located.
- You need to stay current on regulatory requirements. Laws and industry standards change. You can monitor these changes yourself or choose a DLP solution that proactively provides updates for you.

✔ Find a solution that amplifies your efforts without slowing you down.

4. Choose the right technology solution

A DLP solution should have the features you need to protect data without being overly complex to deploy and manage.

Choose a solution that:

- Has a broad range of robust capabilities, including exact data matching, optical character recognition, and integration with rights management solutions and fingerprinting and data classifications
- Is easy to deploy and simple to manage, so you can stay on top of complex compliance requirements
- Can effectively monitor, detect, prevent, and defend against both insider and outsider threats
- Protects data across all threat vectors, including email, databases, networks, and endpoints
- Has a unified dashboard that helps you stay on top of threats and improve incident response times
- Includes comprehensive, customizable reports so you can know—and prove—your organization is staying compliant

✔ Grow your new compliance culture with the right education, tools, and processes.

5. Empower employees to maintain compliance

Data protection requires effort and awareness from everyone at your organization.

In fact, 57% of insider data breaches are caused by inadvertent or accidental actions by employees.[2]

You can help avoid these breaches by:

- Teaching employees best practices, such as knowing what kinds of data are protected, how to handle sensitive information, and how and when to properly dispose of it
- Choosing a DLP solution that can coach users to be compliant by providing notifications when they handle sensitive data; these systems can even require them to enter a business justification before sharing the most sensitive data
- Applying system-level data classification and controls, and letting end users manually classify data for an extra layer of protection

2. 2022 Cost of Insider Threats Global Report, Ponemon Institute

✔ Add to your peace of mind by preparing for a breach, just in case.

6. Establish procedures for responding to data breaches

You can't eliminate vulnerabilities entirely, so you need a plan for how you'll handle a data breach before it happens.

Plan elements should include:

- Recording every data transfer event (and ensuring your DLP solution can search records forensically); that way, you'll know exactly what happened
- Complying with notification requirements to make affected companies and customers aware of the incident
- Updating rulesets and workflows as necessary after the source of the breach has been identified; this will help you avoid another such incident

✔ Tend your compliance processes as part of your daily operations.

7. Run compliance reports regularly

Data protection is a proactive daily activity. Don't wait for a breach or a new regulation to see how you're doing.

Run reports every week or so to monitor your efforts and prove your compliance over time.

A good DLP solution embraces machine learning to make data protection as easy and thorough as possible. Between regular reporting and machine learning, you can make your processes and policies more effective over time.

Ready to get started?

We hope you'll check out Trellix Data Protection as part of your compliance journey.

Compliance-specific features in Trellix Data Protection include:

- Out-of-the-box compliance with common regulations in every area and industry where you do business, making it fast and easy to deploy
- Monitoring and protection of sensitive data such as Payment Card Industry Data Security Standard, personally identifiable information, and protected health information across all threat vectors via a unified dashboard
- Customizable end-user notifications and manual classification by end users, to increase security
- Proactive updates of rulesets in response to regulatory requirement changes
- Native, automated, and customizable reporting

Compliance doesn't have to be overwhelming. We can help you build a compliant data-protection environment. Schedule a free assessment to learn where you stand and how Trellix can help.

Trellix
6000 Headquarters Drive
Plano, TX 75024
www.trellix.com