Personalized Communications & Compliance

4 Steps to Mitigate Risk in Your Data-Driven Operations

NAPCO MEDIA

PERSONALIZED COMMUNICATIONS & COMPLIANCE 4 STEPS TO MITIGATE RISK IN YOUR DATA-DRIVEN OPERATIONS

Have you ever thought about who defines what compliance means for your business? Have you ever thought about who defines what compliance means for your business, and how compliance requirements are met?

When it comes to business, "compliance" refers to meeting the requirements of accepted industry practices, legislation, prescribed rules and regulations, and specified standards or terms of a contract. These regulations and standards vary from country to country and cover a wide array of topics, from storing and retaining business records in IT systems and opting in and out of commercial email communications to securing electronic health records and protecting personal data privacy.

Compliance requirements can be internal (those created within a company) or external (imposed and regulated by federal, state, or local agencies) and they can also be industry-driven.

The number of regulations meant to protect your business' customers and employees is continually increasing. Your company must be vigilant about maintaining a current understanding of all relevant compliance requirements, including industry regulations and government legislation in each country, state, and county in which your business operates. For example, if you are a commercial printer transitioning to digital and want to start doing highly personalized direct mail printing, having the proper tools and processes to help manage data privacy and security compliance should be a primary consideration before starting to create personal data communications.

For every commercial, in-plant, or transactional print shop, regardless of size or location, compliance should be a part of your overall strategic business plan. The failure to mitigate the risks of non-compliance can be devastating. Breaches can result in fines, public relations disasters, lost sales due to eroded trust and damage to the company's reputation, and in extreme cases, legal and other potential liability implications. Imagine being a senior leader of a printing operation that just printed and mailed a marketing solicitation piece that mistakenly went, not to the intended recipients, but to their neighbors, complete with the original recipients' birthdate and financial details.

Such breaches do not have to happen, however. Read on to learn how to prevent them.

A 4 STEP PLAN TO HELP LOWER RISK

How compliance is managed within a company, no matter the size, should be a widespread effort across all employees and functions.

In order to have an effective compliance program, the first step is to get your owner's or management's buy-in. The second is to get key players involved. Employees in areas such as IT, security, internal auditing, and management add their own unique value to a company's compliance program. Even businesses that have made large capital investments and devoted

years of work on compliance plans can have one single oversight — sometimes by one person — that dilutes or even cancels all of the work that has been done. This is why technology should be a key part of any effective compliance program.

Here are four steps you can take to develop a strong approach to compliance and mitigate your company's specific risks:

1. CREATE A COMPANY-WIDE COMPLIANCE PROGRAM

The goal of creating a compliance program is to create a formal structure with written policies, procedures, processes, systems, and standards of conduct to address internal and external compliance requirements. This includes preventing, detecting, and correcting any compliance issues or fraudulent or illegal behavior. However, compliance programs are not one-size-fits-all. Although you can follow these guidelines on how to create a compliance program and what to include, you'll need to develop a tailored plan that meets your company's specific needs.

Establish and adopt written policies, procedures, and standards of conduct. Having clear written policies and procedures in place that describe compliance expectations fosters uniformity within your company. Included should be comprehensive compliance protocols detailing information such as who can access customer data, how that data can be accessed, and for what duration that data will be stored, etc.

Create program oversight and consider centralizing its function. Determine who will oversee, monitor, and enforce the compliance program and serve as your go-to company "watchdog" with questions and concerns. As your business' compliance requirements expand, whether due to operating in multiple countries or multiple sites, centralizing the function of compliance management will help you maintain accountability and navigate the many business requirements and data handling regulations specific to printing and related industry verticals. Many companies have added compliance roles such as a chief compliance officer, whose main responsibilities include ensuring that an organization is able to both manage compliance risk and pass a compliance audit.

Provide staff training and education. Employees at every level need to understand your compliance program expectations and standards in order to be able to comply with them. Implement a training program that clearly communicates your company's program requirements. Include an annual refresher course that reminds employees of your code of conduct and incorporates any changes.

- Establish two-way communication at all levels. Create guidelines for communicating policies and procedures and ensure that every area in the company mentioned in your policy has a detailed description of what to do in order to prevent incidents from occurring and what to do should an incident occur. Set forth the expectation that all employees proactively communicate in a timely manner, whether that means asking compliance questions, reporting issues, or addressing ethical concerns. Include a way for employees to anonymously report compliance issues or fraudulent or illegal behavior without fear of retaliation.
- Implement a monitoring and auditing system. You'll need to measure the effectiveness of

your compliance program and identify risks. To accomplish this, develop a system of both internal and external monitoring, including formal audits. The exact nature of a compliance audit will vary depending upon factors such as whether your company is public or private; what industries it serves; the nature of the data it uses, collects, and stores; and what countries it operates in.

- Enforce consistent discipline. Develop a plan to enforce standards of conduct in a timely manner, outlining appropriate disciplinary measures for employees who fail to comply with the program requirements.
- Take corrective action. When you identify vulnerabilities or violations through monitoring and auditing, take timely, consistent action to correct them.

Data can help drive a business' success, but it can be one of a company's greatest vulnerabilities, too.

2. IDENTIFY DATA SECURITY PROCEDURES

Data can help drive a business' success, but it can be one of a company's greatest vulnerabilities, too. That's why compliance involves not just monitoring and protecting what goes out a company's door, but monitoring and protecting against what comes into the organization, as well.

More than 80 countries now have some form of data privacy laws. It is critical to recognize any regulations relative to the country in which your company is operating or selling goods, such as the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the U.S. Health Insurance Portability and Accountability Act (HIPAA). This list continues to grow over time, and penalties for violations continue to increase. Many of these regulations have incident response requirements that include reporting components.

Here are some recommended steps to help keep sensitive information safe and manage risks effectively:

- Start security at the door. Data security should start with who can enter the building or pass through the lobby, who has access to certain locations, and within those protected areas, who has access to the software, data, and everything else that resides inside the system. Your facility policy should be clearly known by employees and vendors and be visible at all entrances. Common practices include requiring visitor badges so no one unknown enters your shop floor and implement a "no cell phone" policy on plant tours so no photographs can be taken.
- Invest in the right technology. Having the right workflow vendor partner committed

to data security and maintaining its software to the most rigorous standards is critical to mitigating risk. An integrated solution from a single vendor can be more robust than a solution made up of multiple parts from many different vendors. A strong vendor partner can also advise on best practices for a more productive operation while mitigating risk.

- Create an incident response plan. Hackers are creative and relentless, looking for any vulnerability in your business. A secure and tested firewall is key, although it is not always enough to protect your company. Even if you're not required to document incident response procedures by law or industry regulation, it is still necessary to manage risks effectively. Documenting sound processes and procedures when anomalies are identified is also essential.

3. UTILIZE WORKFLOW AUTOMATION

Workflow automation brings process and visibility to your organization and can eliminate costly errors that can sometimes occur with manual processes. As in the example noted earlier, a marketing solicitation piece that is mistakenly sent to neighbors, complete with their birthdates and financial details, because an operator pulled a crumpled letter from the line and didn't replace it (causing subsequent pre-printed envelopes to be stuffed incorrectly). With a robust automated workflow solution in place, this situation could have looked very different: an operator pulls the crumpled letter out and a camera at the end of the inserter detects a missing piece by reading a barcode and notifies the workflow software. This automatically generates a reprint of that missing letter and pulls the pre-printed envelope to avoid a mailing mishap. A piece-level production history is captured by the workflow software for full visibility.

4. MAINTAIN DATA INTEGRITY AND THE AUDIT TRAIL

Compliance requires being able to track individual documents and maintain data integrity from receipt to delivery, so if there is an issue, its source can be located and the appropriate actions taken immediately.

It is imperative that your company be able to produce an audit trail of any document's production history to prove that you process customer data according to appropriate regulations, maintain data integrity and accuracy, protect your systems from misuse or harm, and ensure security of sensitive information. Timestamped records associated with user and system actions for each print job are critical components in building such an audit trail.

Many compliance breaches can be prevented. If they do happen, measures can be put in place for quick correction and recovery, while providing an audit trail of what went wrong. This will help to mitigate future concerns.

KEY RECOMMENDATIONS

Your compliance program should be company-wide, ongoing, and proactive in protecting your business over time. The return on investment could be significant, helping you avoid

waste, fraud, and other disruptions that put your company at risk. Maintaining compliance equips your employees to do their jobs well, keeps customers happy, and in turn, helps your company achieve its goals — perhaps even helping to expand your business with highly personalized communications and allowing you to grow faster.

What is your next step in managing compliance? Implementing a scalable, automated workflow solution that can drive your data-driven operations. Should this be a purchased solution or a home-grown one? Think through your risks carefully. No one knows your business better than the people in it. However, if you now have or are considering creating a homegrown workflow system, here are some questions to ask:

- Does your internal team have the skills to help ensure 100% integrity?
- Does your IT team have the bandwidth to stay current with changing technologies and new risks with continual updates?
- Do you have a historical data repository and adequate audit trail to track and monitor an error path and the associated costs to implement a correction and prevent a future event?
- Can your system identify problems before they occur and shut down the system to stop a pending disaster?
- Are there measures in place for when a problem arises and what it will take to fix it?
- Does your system conduct automated penetration testing to find security vulnerabilities?

Maintaining compliance equips your employees to do their jobs well, keeps customers happy, and in turn, helps your company achieve its goals — perhaps even helping to expand your business with highly personalized communications and allowing you to grow faster.

In other words, does your company have the compliance expertise, sufficiently deep pockets, and sustainable resources to adequately protect your evolving risk vulnerabilities now and in the future?

Data processing and security is complex and interdependent, and the increased risks of operating manually are high. Therefore, ensure that your company has an end-to-end automated workflow solution to help mitigate compliance risk in your data-driven operation.

USING RICOH PROCESSDIRECTOR™ TO MITIGATE YOUR COMPLIANCE RISK

RICOH ProcessDirector™ can automate processes in many different mixed production environments, from high-volume continuous-feed to smaller commercial print sheetfed operations, thanks to its vendor-neutral design.

This leading workflow management solution can capture, transform, and manage both printed and digital communications in ways that streamline operations to help achieve 100% output integrity, provide document-level audit trails, and initiate a disaster recovery plan. With rules-based processing and the use of data driven insights, RICOH ProcessDirector can correct errors before jobs leave a shop and maximize efficiency through automation.

Tracking is essential to meeting compliance goals. With connections to inserters or cameras mounted on other shop floor equipment, RICOH ProcessDirector can track documents throughout their manufacturing process and trigger automatic reprints for near zero-defect printing. Production history, which includes manually deleted jobs damaged during insertion, can be saved in an archive to serve as an audit trail for each individual document. Users can research their production history to respond to queries or audit requests.

As a commercial, in-plant, or transactional printer responsible for personalized communications, you need an experienced partner who can help you mitigate your compliance risk with a proven automated workflow solution.

ABOUT RICOH

Ricoh is empowering digital workplaces using innovative technologies and services enabling individuals to work smarter. For more than 80 years, Ricoh has been driving innovation and is a leading provider of document management solutions, IT services, communication services, commercial and industrial printing, digital cameras, and industrial systems.

Headquartered in Tokyo, Ricoh Group operates in approximately 200 countries and regions. In the financial year ended March 2020, Ricoh Group had worldwide sales of 2,008 billion yen (approx. $18.46 billion).

For more information, visit ricohsoftware.com

ABOUT NAPCO

NAPCO Media is a leading B2B media company specializing in creating community through content via integrated media programs, video services, marketing services, events and event management, custom content, eLearning, and market research. NAPCO Media has rapidly expanded its portfolio to include NAPCO Video Services, NAPCO Events, NAPCO Marketing Services, and NAPCO Research.

For more information, visit napcomedia.com