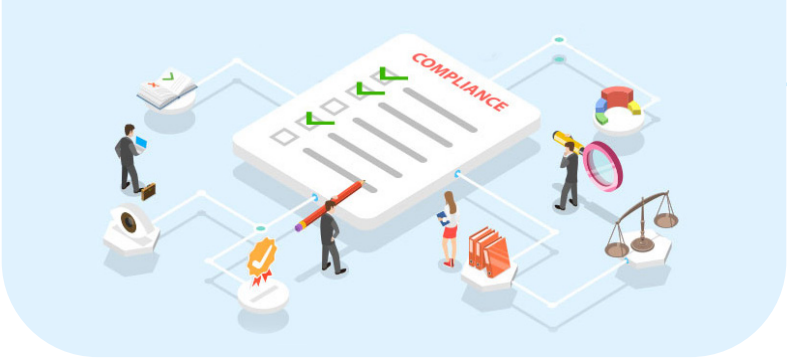
ARTICLE

Dropsuite



Business Compliance: A Look Behind and Beyond the Acronyms

Business compliance is a relatively new term that sounds simple but is anything but. Businesses must follow all the industry-specific and general regulations as well as privacy laws that have come into being over the years to protect people's privacy. The constantly changing landscape of laws and regulations leaves many organizations struggling simply to stay on top of changes.

There are two types of regulations that are constantly changing and being added to:

Data privacy laws govern/regulate/specify how organizations use and manage personal data and personally identifiable information (PII) - this often includes ensuring that individuals have some control over how their data is collected and used.

Regulatory compliance addresses an organization's adherence to laws, regulations, guidelines, and specifications relevant to its business processes[i]. Some regulations directly relate to protecting data, but others, especially in highly regulated industries such as financial services, focus more on ethical behavior consumer protection.

> "If you think compliance is expensive - try non-compliance."
>
> **Former U.S. Deputy Attorney General Paul McNulty**

Business compliance is both a benefit and an obligation for organizations. On the positive side, being compliant can reduce the risk of a costly data breach and lead to greater consumer confidence and trust. The downside is that violations can result in fines and even civil and criminal sanctions. Unfortunately, being compliant (and proving it) is not simple. There are hundreds of laws and regulations that may or may not impact a business, and it's no small matter to figure out which ones are important, and how to comply.

The evolution of business compliance

Back in the early 1970s, the term business compliance wasn't even in our vocabulary. Instead, companies established codes of conduct that were implemented by personnel and legal departments. Contrast that situation with today, where we face an alphabet soup of regulations and laws – with more coming online every day. Privacy laws and corporate/industry governance mandates have evolved rapidly over the past decades. Most, however, had their genesis in a public push to make businesses accountable for ethical shortcomings.

PRIVACY LAWS

Data privacy laws have been around for longer than most people think. Stemming from World War II-era concern over state-controlled abuse of personal data to identify minority groups, both Sweden[ii] in 1973 and Germany[iii] in 1978 passed acts that criminalized data theft and gave data subjects the freedom to access their records. An uproar over the invasive nature of a national census survey caused legislators to replace the German law with one that gave individuals the right to protect against unlimited collection, storage, usage, and disclosure of their personal data collected in the census[iv]. Then, with the formation of the EU, regulations became more generally enforceable thanks to the EU Directive on Data Protection[v], followed in 2016 by the General Data Protection Regulation (GDPR)[vi].

The US mirrored these efforts with the passage of numerous regulations to establish fair information practices surrounding the collection and use of personal information. The first, the Privacy Act of 1974, established a Code of Fair Information Practice governing the collection, maintenance, use, and dissemination of PII by federal agencies. The Data Protection Act of 1984 introduced basic rules of registration for users

of data and rights of access to that data for the individuals to which it was related. These rules were revised ad superseded by the Data Protection Act of 1998. Other relevant acts included the Children's Online Privacy Protection Act (COPPA) of 1998 designed to protect children in the Internet age; FERPA (the Family Educational Rights and Privacy Act) to protect the privacy of student education records; and recent state-level initiatives such as the California Consumer Protection Act (CCPA). In Brazil, the LGPD similarly calls for secure methods of storing, discovering, retrieving, and auditing personal data, but the definition is much broader than that of GDPR.

BUSINESS COMPLIANCE and ETHICS REGULATIONS

Many of the regulations related to business ethics, in contrast, did not come about due to concerns about personal data protection. Rather, they were a response to the excessive risk-taking and lack of effective controls that caused massive corporate and accounting scandals, such as those related to Enron and Worldcom. To restore investor confidence, the Sarbanes-Oxley Act of 2002[viii] (SOX) was passed by the US Congress to require companies and their management to fully disclose their financial and accounting practices and activities – including a requirement to audit data management and backup data. Similar regulations include Germany's Deutscher Corporate Governance Kodex (DCGK), and Australia's Corporate Law Economic Reform Program Act of 2004 (CLERP 9).

> "The biggest corporation, like the humblest private citizen, must be held to strict compliance with the will of the people as expressed in the fundamental law[vii]."
>
> **Theodore Roosevelt**

The financial services industry has seen multiple regulations over the past decades. To address a crisis of confidence due to scandals involving bribes of foreign officials, the US passed the Foreign Corrupt Practices Act of 1977. In contrast, FINRA[ix] was created to protect investors and safeguard market integrity in a manner that facilitates vibrant capital markets. The Gramm-Leach Bliley Act (GLBA) of 1999 aimed to modernize the US financial services industry by removing historical barriers between sectors. All these regulations contain provisions related to data retention. Similarly, on a global level, BASEL II requires financial institutions to manage risk, including retaining 3-7 years of data history[x].

HIPAA, the Healthcare Insurance Portability and Accountability Act of 1996, focused on ensuring that people who left their jobs would not be without health insurance coverage. Like most industry-specific regulations, it had a parallel objective: to protect private health information. Similar regulations exist in Canada (The Canadian Health Act of 1984) and other countries. The energy sector is not exempt: FERC[xi] and NERC regulations in the US, and the Directorate-General for Energy of the European Commission[xii], aim to help protect critical infrastructure and require record retention for varying periods. As with the data privacy laws, these regulations require strict adherence to how data is stored and communicated, with requirements that it be auditable and discoverable.

The landscape today

Businesses around the world face a bewildering multitude of regulations that are constantly changing and bring a unique set of challenges. Among these:

- **Scope:** Which regulations apply to my organization?
- **Constant changes:** How can I stay current?
- **Different standards:** How do I ensure compliance when the regulations have different, sometimes contradictory, requirements?
- **Solutions for usability:** How can I make ensure the data I collect and process is searchable, retrievable, and auditable when needed?

Scope: It is difficult to determine which regulations and laws affect an organization: the answer is, "It depends." It can depend on the industry, geographical location, nature of the customer base, location of data stores, and much more. MSPs and small businesses are subject to many more regulatory requirements than they think. For example, many organizations are subject to GDPR, even if they are not located in the EU. The same could hold true for CCPA (with similar regulations in Vermont, Washington and other states, not to mention Canada, Australia, and Argentina). As states and countries begin to implement their own regulations, the onus is on the organization to find out which might apply.

Changes: It is difficult to keep abreast of constantly changing regulations. For example, HIPAA[xiii] has undergone four major updates since its passage in 2003: the language has tightened, loopholes closed, and requirements fine-tuned. HIPAA Security Rules in 2005 dealt with electronically stored PHI; later the Enforcement rule introduced fines and penalties for failure to comply, HITECH extended HIPAA rules to business associates and third-party suppliers, and the Final Omnibus Rule (2013) filled in gaps such as defining encryption standards and retention periods. HIPAA compliance is still evolving, in response to the COVID pandemic.

Standards: It is important to understand the requirements of each relevant regulation and find ways to deal with inconsistencies. For example, in the EU people can opt in to allow companies to process their data, but in California, they must opt out. When it comes to data retention periods, the differences can be huge: some call for months-long retention periods, SOX requires seven years of auditing data, and other regulations necessitate keeping data "forever." Regardless of the timeframe, it can be difficult for an organization to comply. The CCPA includes a "look back" requirement obligating organizations with information on California residents to retain data for the previous 12 months, but studies[xiv] show it is very difficult for an organization to produce emails older than six months.

Solutions for usability: The key element in most regulations is proving compliance, which means not only storing data securely but making sure the data is accessible and retrievable when needed. For regulations like GDPR, the organization must be able to quickly access all personal data belonging to a user. For FINRA, it is common to have to quickly access years' worth of transaction records, communications, and other data to facilitate an e-discovery request. With ever-increasing volumes of data (almost 320 billion emails are sent each day[xv]), simple backup is not enough. There is simply too much data, and it is too easy to delete or modify it, not to mention the impossibility of searching for and finding needed information. Compliance calls for an archiving system that can index content and enable robust search capabilities for archived content.

Looking forward

New regulations are emerging constantly in response to existing problems, and key issues plaguing businesses and organizations today will, in turn, generate new laws with their own specific requirements for privacy, security, and compliance. An obvious example is ransomware: we have seen a proliferation of attacks, as well as a change in methodology (cybercriminals may no longer simply encrypt the data but steal it before locking down systems so they can auction it off if no ransom is paid). This is triggering further evolution in laws for data capture and retention. The SEC and FINRA have both published reports that outline regulatory examination priorities for 2021, with an emphasis on ransomware recommendations[xvi]. Bear in mind that MSPs can be liable if a company pays a ransom.

Supply chain issues that are developing around the globe will undoubtedly trigger more regulations. The EU is attempting to respond to these challenges through a draft European Supply Chain Law, with an agreement expected in 2022[xvii]. A recent US executive order called for the Departments of Commerce, Energy, Defense and Health and Human Services to report on risks in the supply chain and recommendations to address those risks. Undoubtedly, new regulations will come out of this effort. This places the onus on the legal departments to stay abreast of new developments so they can comply with the latest directives. Even insurance companies are in on the movement: they offer cyber liability insurance, but it is tied to a thorough risk analysis to ensure the small business or MSP complies with all relevant regulations. They warn that state and federal regulators are not easing up on their expectations, so they expect higher levels of accountability and enforcement moving forward[xviii].

Guidance for MSPs and small businesses

Business compliance means doing everything necessary to adhere to regulatory requirements, protect important business information, recover data when requested, and ensure data privacy and security for all customers and stakeholders. No organization around the world that uses email to communicate with customers, prospects, and partners is immune. The list of privacy and data access requirements is long and growing, and customers are increasingly aware of their rights. For MSPs, it's not enough to secure and manage client data; the burden extends to identifying the regulatory requirements that apply to their clients and taking steps to ensure compliance, especially in cloud environments. Failure to ensure compliance – and reassure customers that you are implementing best practices – can be costly.

Best practices start with secure data backup and archiving and include data security (protecting data in archives from loss, corruption, breaches, and theft), data retention in compliance with all relevant regulations, and rapid, effective data search and retrieval. Organizations that institutionalize broad and deep data privacy and retention practices are well-positioned to respond to changing and emerging requirements, leading to improved customer trust and confidence. Remember, it's not just good business – it's the law.

Resources:

i. https://searchcompliance.techtarget.com/definition/regulatory-compliance
ii. https://scandinavianlaw.se/pdf/47-18.pdf
iii. https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz
iv. https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_2
v. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046
vi. https://gdpr-info.eu/
vii. https://www.loc.gov/resource/mss38299.mss38299-425_0984_1097/?sp=5
viii. https://www.investopedia.com/terms/s/sarbanesoxleyact.asp
ix. https://www.finra.org/#/
x. https://www2.pacinfo.com/PDF/asigra/Asigra_Compliance.pdf
xi. https://www.ferc.gov/sites/default/files/2020-04/mou-eu-05-05-2016.pdf
xii. https://www.devex.com/organizations/european-commission-directorate-general-for-energy-dg-ener-74962#:~:text=The%20Directorate%2DGeneral%20for%20Energy,consisting%20of%2017%20individual%20units
xiii. https://www.hipaajournal.com/hipaa-history/
xiv. https://www.archive360.com/whitepaper-osterman-key-issues-for-ediscovery
xv. https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/
xvi. https://www.reuters.com/legal/legalindustry/ransomware-state-union-regulations-trends-mitigation-strategies-2021-10-14/
xvii. https://www.aeb.com/intl-en/magazine/articles/eu-supply-chain-law.php
xviii. https://www2.deloitte.com/us/en/pages/regulatory/articles/insurance-regulatory-outlook.html

CONTACT US

For more information, please contact us:
www.dropsuite.com | sales@dropsuite.com