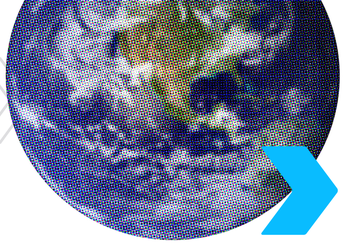
CHECKLIST

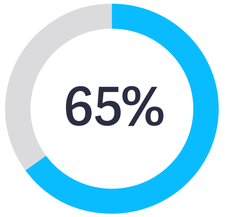
The Complete Compliance Checklist

Zix®



Regulation is eating the world

If the first two decades of the 21st century were about capturing data, the third is about being accountable for what's being kept. Regulations—many, a direct response to abuses and breaches—are multiplying, and growing in depth and breadth.



By 2023, **65% of the world's population** will have its personal information covered under privacy regulations, up from 10% today, reports Gartner.

In healthcare, there's HIPAA, the HITECH Act, MACRA, and PSQIA. In finance, there's GLBA, EGRRCPA, PSD2, NYDFS, PCI-DSS 3.2, and the Dodd-Frank Act. Within the U.S., there's CCPA, SHIELD, and FERPA. Globally, there's the EU's GDPR, Canada's PIPEDA, Brazil's LGDP, Chile's CDPL, Bermuda's DABA, Australia's Open Banking, Singapore's MAS guidance, and Malaysia's regulation.

Plus many more.

There are also innumerable internal workplace harassment policies, internal governance, and voluntary regimes like The National Institute of Standards and Technology (NIST) privacy framework.

For those upon whom the burden falls, it's easy to see this as a cascade of additional work and liability. But the severity of the challenge presents an equally great opportunity. As some companies struggle to meet the minimum requirements, those that excel will be at a competitive advantage in myriad and seemingly unrelated areas. Compliance, in this view, can be seen as a tool for enabling the entire business to achieve its goals.

Compliance can help teams:

- Respond faster to audits and litigation
- Save on storing, locating, and retrieving data
- Inspire and maintain digital trust
- Attract and retain top talent
- Create business intelligence
- Improve financial performance
- Attract buyers and cement deals
- Enhance relationships with regulators

What is PII?

Any data that can be used to identify specific individuals or information that is linked or linkable to an individual, such as a medical record.

No single, exhaustive list exists, but PII can include:

- Name
- Social Security number
- Passport number
- Drivers license number
- Taxpayer Identification Number
- Patient identification number
- Credit or debit card number
- Financial account number
- Vehicle identification number
- Mail address
- Email
- Phone number
- IP address
- MAC address
- Login ID
- Social media posts
- Digital images (particularly of a face or identifying mark)
- Biometric records: fingerprint, retina scans, voice signatures, facial geometry
- Handwriting
- Account security questions

Typically, this data does not count as PII:

- Date of birth
- Place of birth
- Business telephone number
- Business email
- Business mailing address
- Race
- Religion
- Geographical indicators
- Employment information
- Education information
- Some financial information]

Tools of the Trade

The key to proactive compliance is interlock. The right people need access to the right data at the right time, but that's easier said than done. Legacy systems such as on-premise archiving tools that only capture emails create troubling gaps—what happens when a lawsuit involves communications over Salesforce Chatter or Slack? Or, if incomplete cyber threat protection devices leave room for hackers to intercept emails, what's to guarantee data hasn't been tampered with? A good compliance program consists of:

Policies and procedures

Companies need teams or individuals dedicated to crafting internal policies and procedures that satisfy regulation, but also internal demands like workplace harassment. Where new threats arise daily and regulatory demands change monthly, most teams must rely on vendors that update their systems and policies automatically.

Data retention policies

Companies need defined and verifiable data retention and deletion policies that satisfy regulation. That includes not holding data longer than its required, and giving consumers secure access so they can know what data is held on them, and to request it be deleted. Teams that don't know what data they're holding can be exposed and yet unaware of it.

Threat protection

Companies need an active defense against malware and malicious actors. All things connected are increasingly vulnerable and breaches are a common trigger for audits and litigation. Under GDPR alone, $474 million in fines were levied in 2019, many due to breaches that exposed improper storage policies.

Encryption

Secure email is critical—business email compromise (BEC) is the most common way many hackers get in the door to access sensitive data. Some 79% of organizations consider secure email a vital need according to research by Pulse Q&A.

Archiving

Storage is important, but so is proving it—88% of companies aren't certain what data they hold on consumers. A good modern archiving tool can help if it's flexible and allows teams to enforce both regulatory requirements and internal policies.

eDiscovery

Surprise litigations and audits have a hidden cost: The time of employees who are drawn into the process to help auditors or litigators access data. IT and information security teams, for instance, rarely plan for or budget this time. A modern eDiscovery tool can help if it allows for roles and permissions, tagging, and has an interface as simple as Google Search, to democratize data access.

Considerations for security and compliance solutions

- Intuitive interface design for non-technical teams (legal, HR, management)
- Search Indexing, tagging, and automated document organization
- Pre-configured search templates for simplified eDiscovery
- Flexible policy creation with no retention hold limits for supervision
- Enforced litigation holds with simple secure sharing
- Extensive library of in-house developed data connectors
- Encrypted, redundant, and highly available cloud-native storage
- Integrated email security and encryption to keep the archive clean and accessible
- Flexible enforcement of Data Loss Prevention (DLP) regulatory violations
- Continuous updates of pre-configured DLP policies via in-house compliance experts.
- Use of military grade encryption standards
- Automated enforcement of encryption with zero user intervention
- Automated best method of encryption enforcement for optimal recipient experience
- Two-way encryption delivery for on-going email communications
- DLP incident remediation workflow
- Zero cost data import or exports

Compliance by Industry

Healthcare

By some estimates, healthcare companies face one lawsuit per fifty beds. “The most risk-avoidant thing you can do is encrypt,” says Leon Rodriguez, Director of the Department of Health and Human Services’ Office for Civil Rights, which enforces HIPAA.

Healthcare companies:

- Deal with lots of sensitive info PII /PHI
- Highly targeted by criminals—the value of a healthcare record is 50 times higher than financial data - HIPAA Journal
- Embrace digital to improve service delivery and collaboration
- Privacy is a big patient concern—33% withhold healthcare info - ONC
- Breaches impact care—cancelled procedures, service performance declines
- Highly regulated—HIPAA / HITECH data privacy
- Litigious by nature

Email threat:

- Increase trust and patient care by mitigating cyber intrusion and data breaches
- Protect against ransomware and BEC

Email encryption:

- Enable secure sharing of sensitive data with healthcare partners and clients

Email and communications archive:

- Classify and retain communications to provide immutable records for future investigation or litigation

Compliance by Industry

Finance

Today, fintech disruptors have set a pace of change that's sometimes incompatible with security and compliance. Accenture reports that 79% of business leaders feel that new technology is introducing big new vulnerabilities. And that's in a sector where businesses are 300 times more likely than others to be targeted by cybercriminals, reports the Boston Consulting Group.

Finance companies:

- Top industry for digital transformation, but 79% say new business models introduce risk
- Reliant on sensitive PII and financial data
- Often deliver services through partners such as brokers, dealers, and retailers
- Highly regulated—GLBA and PCI-DSS for data privacy and FINRA for records management
- Highly targeted—300 times more likely - BCG

Security

- Increase trust and patient care by mitigating cyber intrusion and data breaches
- Protect against ransomware and BEC

Encryption:

- Permit secure sharing of sensitive data with ecosystem partners and clients

Archive:

- Enforce record keeping across all communications (email, social, IM, new media), including for brokers and dealers
- Ensure FINRA compliance

Compliance by Industry

Education

The education sector is rightly prioritizing student outcomes, but at a cost. Customized learning, online classwork, and remote participation introduce PII vulnerabilities. And regulations such as FERPA, designed to protect education records and student administration, introduce compliance costs that weigh heavily on an already cash-strapped sector.

Educational institutions:

- Digital provides a huge opportunity to improve learning outcomes for Higher-Ed and K-12
- Dramatic rise in cyber risks
- Online learning, course management, parent engagement
- Customized learning, modern digital media
- Improved accessibility
- Increased regulation FERPA, PCI-DSS

Security:

- Increase trust and protect student accounts by mitigating cyber intrusion
- Protect against ransomware and BEC

Encryption:

- Enable secure sharing of sensitive data with students, parents, learning partners, and collaborators

Archive:

- Retain communications to provide immutable records for future investigation or litigation

Compliance by Industry

Real Estate

Client communications that include nonpublic personal information (NPI) are coming under increased scrutiny. The Consumer Protection and Financial Bureau as well as the American Land Title Association have published guidelines restricting the sharing of NPI, which can restrict the flow of information and potentially deals, if the communication isn't secured.

Real estate firms:

- Real estate and land title industry relies on expedient information exchange between parties
- Email is a staple digital technology for efficiency, speed, convenience but introduces risk of data disclosure, privacy breach, and fraud
- CFPB mandates that creditors and their agents safeguard sensitive information such as nonpublic personal information (NPI)

Security:

- Protect systems from cyberattacks to modify transactions details (account numbers) or steal PII
- Protect against ransomware and BEC

Encryption:

- Support secure email exchange of confidential data

Archive:

- Retain communications to provide immutable records for future investigation or litigation

Compliance by Industry

Government

Entities from agencies to state and local governments that have successfully collected big data are now finding themselves targets. The challenge is continuing to improve and deliver services while safeguarding sensitive data.

Government institutions and agencies:

- State and local governments have diverse agencies, complex information systems
- Aging infrastructure that doesn't support new requirements
- Responsibilities to serve the public with critical services and deal with PII
- Increasingly targeted by cyberattacks—ransomware hit 103 federal, state and municipal agencies in 2019
- All states have public records laws which allow the public to obtain documents and other public records from state and local government bodies

Security

- Protect systems from cyberattacks to prevent breaches
- Protect against ransomware and BEC

Encryption:

- Enable secure sharing of sensitive data within government agencies and contractors

Archive:

- Maintain records across all communications (email, social, IM, new media) to satisfy public information requests

Compliance by Industry

All Industries

Criminals may prioritize finance and healthcare, but breaches are increasingly industry agnostic. A 2017 report by the Ponemon Institute and IBM revealed the average total cost of a data breach in the U.S. reached a record-breaking $7.35 million, a 5% increase from the previous year. These numbers are only growing.

All industries:

- Virtually every business must protect against cyber risk and sensitive data loss
- Professional services, high tech, manufacturing, utilities, hospitality, media, insurance, retail, non-profits
- Storage of PII, credit cards, healthcare, social insurance, intellectual property, business plans, digital login credentials
- Virtually every business must manage HR issues around workplace harassment

Security:

- Protect systems from cyberattacks to prevent data breaches
- Protect against ransomware and BEC which lead to financial loss and business disruptions

Encryption:

- Enable secure sharing of sensitive data within partners, customers, and external partners

Archive:

- Retain communications to provide immutable records for future investigation or litigation

Complete compliance with Zix | AppRiver

Zix's mission is to protect its clients' communications, and this extends beyond email into social media, IM, and emerging platforms.

Zix can help you protect customer, partner, and employee data in communications, and help the right people access it quickly when needed.

The combination of **Email Encryption** and **Information Archiving** provides customers with an end-to-end solution for establishing external and internal trust by enforcing regulatory requirements and internal policies. Zix can help you protect customer, partner, and employee data in communications, and help the right people access it quickly when needed.

Zix's Research Center team also employs in-house lexicographers who constantly release Data Loss Prevention (DLP) regulatory content filters and provide ready-made templates to keep customers compliant. Zix can also archive new data sources as they emerge.

Relying on Email Encryption and Information Archiving helps you maintain a high level of ongoing, passive compliance through:

- Continuously updated DLP regulatory filter templates
- In-house lexicographers
- Frequent updates
- Email encryption
- Multiple data source support as needed
- Flexible retention rights
- Custom policy creation, enabling you to determine what data to archive, where, and for how long, ranging from the global and broad to the specific and granular
- Quick, efficient e-discovery
- Fast response to records requests
- Universal governance and enterprise information archiving of all business communications with one tool, enforcing one policy consistently across all media, including email, Facebook, Twitter, LinkedIn, Pinterest, YouTube, Vimeo, Instagram, RSS feeds, blogs, Slack, Workfront, Yammer, Salesforce Chatter, and more

Zix's subscription-based compliance helps you adapt quickly to changes in the regulatory landscape and ensures you're automatically protected with the latest efficiencies and updates, which enables you to capitalize on new business opportunities and accelerate business growth.

Learn more at Zix.com.