cavelo

Guide to

Data Discovery for Regulatory Compliance

Introduction

As a digitally-driven business, you're constantly collecting and storing data. The types of data you collect and the number of data sources you use grows every day. You know how important it is to have visibility to all of the assets and data on your network, but managing rapid sprawl and unstructured data is difficult, especially if you're using disparate tools and methods.

Data sprawl and unstructured data are leading to increased cybersecurity risk – and regulatory requirements.

Regulators take data privacy seriously and recognize how vulnerable unclassified and orphaned personally identifiable information (PII) is, especially if it falls into malicious hands. Today's regulations focus on measures that ensure businesses are taking appropriate steps to safeguard the sensitive data that lives on business networks. They're designed to give individuals greater control over their own data privacy, while holding companies responsible as custodians of personal data.

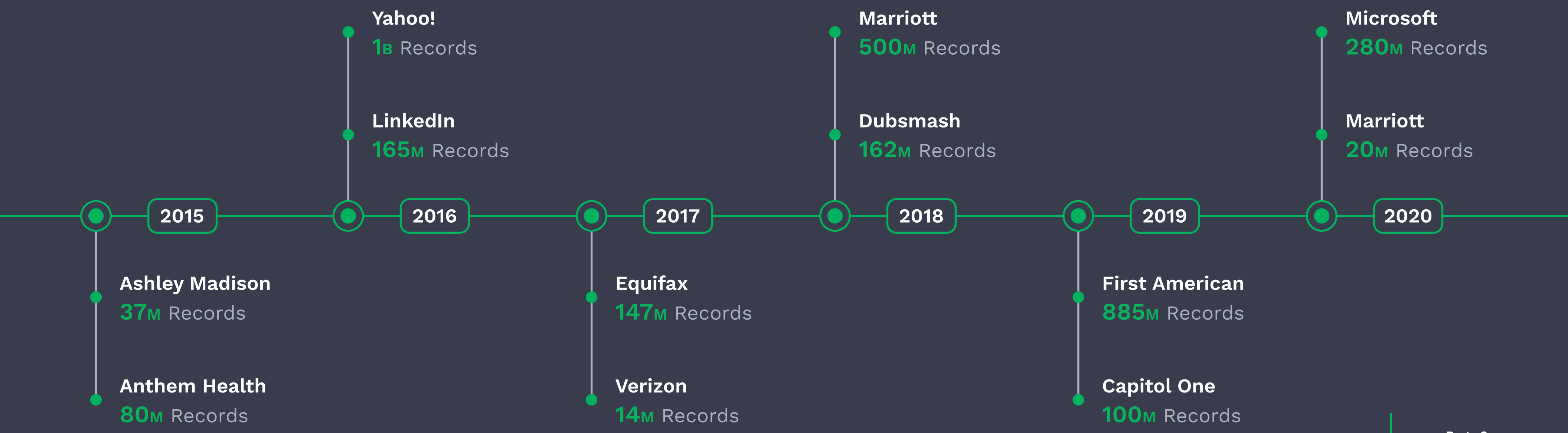
While many regulations look and sound similar, they vary depending on the audience and purpose they serve. Some provide frameworks that help businesses stand up data privacy and protection policies and procedures, while other acts have audit cycles that come with non-compliance fines and legal measures.

As an under-staffed or under-funded team, it's hard to juggle increasing regulatory requirements. But with data proliferation and evolving cyber-attacks, it's never been more important to take stock of current measures and identify the ones that matter most to your business. This guide takes a look at the most common frameworks and regulations to offer data discovery, classification and management insights you can apply within your organization to simplify compliance exercises.

Cyber-risk Climate Change

As we map a path to future data protection and privacy, we need to look to our past and the chain of events that changed information security. In less than 10 years, cyber-attacks have risen to become the most common form of criminal activity targeting businesses. The Home Depot breach in 2014 was a bellwether for every industry and triggered many of the data protection standards and regulations that exist today. The big breach events that followed the Home Depot attack seemed never-ending, and every one of them shattered records along the way. Over the years, the path to criminal wealth has taken a more indirect route, with attackers targeting sensitive personal information. As attackers acquire different kinds of personal information, they can build greater context, leading to larger potential targets - with greater payouts.

Below are just some of the record-breaking attacks that have exposed names, addresses,
phone numbers, passport details or credit card information.



2015

Ashley Madison
37M Records

Anthem Health
80M Records

2016

Yahoo!
1B Records

LinkedIn
165M Records

2017

Equifax
147M Records

Verizon
14M Records

2018

Marriott
500M Records

Dubsmash
162M Records

2019

First American
885M Records

Capitol One
100M Records

2020

Microsoft
280M Records

Marriott
20M Records

What does data discovery have to do with it?

Sensitive data is everywhere.

In our rush to achieve digital transformation, we’ve driven up overall cyber risk. Cloud adoption, remote workforces, digital commerce and connected IoT have transformed the way businesses work and the kinds of data they collect, store and share. Keeping data types organized is difficult. Regulators at every level recognize how exposed and vulnerable sensitive personal data has become. They also recognize how lucrative personal data is to attackers, which is why they’ve developed guidelines, regulations and acts to help companies protect sensitive data, and to give consumers and citizens more control over their data privacy.

Having the ability to understand the data you have on your network (data discovery), and the types of data you're accumulating (data classification) underpins every data privacy and security regulation. Simply put – if you don't know what data you have, you can't protect it. Many companies believe that compliance is ticking a box on an audit form, yet in reality, achieving compliance means you have to be able to demonstrate how you tick the box. In other words, you must be able to define specific processes, tools and measures you have in place to accomplish specific requirements.

Myth

Being able to 'tick the box' guarantees compliance.

Fact

Being able to demonstrate how you tick the box achieves compliance.

Data privacy is priority - but whose job is it?

Data privacy and data protection have become mutually exclusive. That makes it harder to figure out who owns data management, reporting and compliance within the business. Historically, legal departments managed data privacy and championed compliance work, especially if a company lacked security compliance headcount. More recently, the nature of cyber events have fused data privacy with data protection. As a result, CISOs and IT leaders are tasked with operationalizing data privacy and compliance within larger cybersecurity initiatives.

In many small and midsize organizations, data privacy and data protection responsibilities span several roles within the business. Data privacy, protection and compliance programs need representation from stakeholders across the business, and those stakeholders need tools that make data and reports accessible, regardless of their role or how data-savvy they are.

CIO
CFO
Compliance Officers
IT Directors & Managment
Legal
SOC or Security Managers
Clerks

Every stakeholder has vested interest in ensuring data privacy within the business. From preventing data breaches and fines, to managing lawsuits and company reputation, data discovery, classification and management are essential to risk mitigation.

> *Data privacy and security frameworks, regulations and acts support the processes needed to achieve and sustain robust data management at scale.*

Which regulations and frameworks apply to your business?

Every business is unique and, depending on the industry you operate in, the regulatory requirements that apply to your organization will vary. Regardless of the type of business you are, odds are you'll have multiple governing bodies that you need to align with, report on and adhere to. We'll dive into some of the more universal and wide-reaching data privacy and security regulations to help you narrow your focus – and pinpoint where data discovery, classification and management are necessary for compliance.

Global Regulations

Regional Regulations

Industry Regulations

Global Regulations

General Data Protection Regulation (GDPR)

GDPR is arguably the most well-known (and most feared) data privacy and security law on the planet. The law was designed to protect the data privacy of European Union (EU) citizens through regulations aimed at companies who collect and/or process EU-citizen data, regardless of what country they operate in. The regulation was introduced in 2016 and officially came into effect in 2018. Regulators issued some of the largest fines on record in 2020, including a 56M USD fine to Google, 41M USD fine to H&M and 23.4M USD fine to Marriott.

ⓘ Who does this affect?

The regulation gives citizens more control over how their sensitive data is collected, stored and shared. It's the first regulation of its kind. Any company handling EU-citizen data can be fined in the event of a breach or non-compliance.

ⓘ Why does it matter?

This regulation sets a global standard and serves as a model for other regions implementing similar measures to protect their citizen's sensitive data. GDPR also set a precedence in terms of fines, with violations costing companies up to 10M Euros or 2% of their annual revenue, or the higher of the two.

General Data Protection Regulation (GDPR)

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.		
Data Classification – classifying data by category and by data sensitivity.		
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.		
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.	✓	Section: P6
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.		
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Sections: P4, P8
Data Custodians – identifying the owners or operators of systems, products and services that process data.		
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.	✓	Sections: P4, P8
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.		
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.	✓	Sections: P10
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.		
Data Subject Rights – providing individuals with appropriate access to their personal data.		
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.		
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.		
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.		
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.		

Global Regulations

Open Web Application Security Project (OWASP)

The OWASP Foundation is a non-profit organization working to improve software security through community-led, open-source software projects. The Foundation has hundreds of global chapters and tens of thousands of members. The OWASP Application Security Verification Standard (ASVS) Project provides security standards for software and web application developers and designers.

ⓘ Who does this affect?

The ASVS standards help companies and development teams designing software and applications to mitigate data privacy risks by ensuring appropriate measures are built around data classification and how applications control data collection, storage and processing.

ⓘ Why does it matter?

At the end of the day, software and application designers have to make sure their products meet current data security and protection measures. In many cases, software must align with standards in the industry it's intended to serve; the ASVS standards provide the baseline for broader compliance.

Open Web Application Security Project (OWASP)

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.	✓	Articles: 4, 5.2, 9
Data Classification – classifying data by category and by data sensitivity.	✓	Articles 4 and 9
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.	✓	Articles: 30.1, 30.2, 30.3, 30.4, 30.5
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.	✓	Article 5.1
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.	✓	Articles: 5.1, 35.1, 35.2, 35.3, 35.6, 35.8, 35.9, 35.11
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Articles: 5.1, 18.1, 18.2, 21.1, 21.2, 21.3, 32.1, 32.2
Data Custodians – identifying the owners or operators of systems, products and services that process data.		
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.	✓	Article 5.1
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.	✓	Articles: 5.1, 21.5, 22
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.		
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.		
Data Subject Rights – providing individuals with appropriate access to their personal data.	✓	Articles: 12.1, 12.2, 13.2, 14.2, 15.1, 15.2, 15.3, 15.4, 16, 26.3
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.	✓	Articles: 18.1, 18.2, 18.3, 19, 21.1, 21.6, 22, 26.3
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.	✓	Article 5.1
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.	✓	Articles: 17.1, 17.2, 17.3
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.	✓	Articles: 32.1 and 32.2

Regional Regulations

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is a Canadian law designed to govern the way that private companies collect, process and use personal information for commercial purposes. PIPEDA was introduced through federal legislation in 2001 and implemented in 2004, making it one of the oldest regulations we cover in this guide.

Who does this affect?

The law holds companies accountable to the protection of citizen data. Any company engaged in commercial and transactional activities must comply with PIPEDA.

Why does it matter?

The law has been grandfathered over time and navigated a few revisions along the way. It upholds many of the fundamental data privacy and protection requirements of modern digital environments and remains relevant as a means to mitigate the risks that come with the proliferation of personal data. PIPEDA also carries mandatory breach reporting requirements. In the event of a breach or non-compliance, companies can be fined up to $100,000 per violation. Failure to meet compliance requirements may bring additional penalties.

Personal Information Protection and Electronic Documents Act (PIPEDA)

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.		Articles: 4, 5.2, 9
Data Classification – classifying data by category and by data sensitivity.		Articles 4 and 9
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.		Articles: 30.1, 30.2, 30.3, 30.4, 30.5
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.	✓	Section 4 - Limited Collection
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.	✓	Section 4 - Limited Collection
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Section 5 - Limited Use, retention and disclosure
Data Custodians – identifying the owners or operators of systems, products and services that process data.		
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.	✓	Section 5 - Limited Use, retention and disclosure
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.	✓	Section 6 - Accuracy
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.		
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.		
Data Subject Rights – providing individuals with appropriate access to their personal data.	✓	Section 9 - Individual Access
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.	✓	Section 10 - Challenging Compliance
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.		
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.		
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.		

Regional Regulations

California Consumer Privacy Act (CCPA)

CCPA is a law introduced in California that came into effect on January 1, 2020, though companies had 6 months to prepare before enforcement began on July 1, 2020. The law is designed to protect the privacy of California residents. In addition to non-compliance or breach fines issued by regulators, residents are given authority to file suit against companies who experience a breach as a result of non-compliance.

ⓘ Who does this affect?

The law applies to companies collecting, using, storing or processing the data of California residents. While it's similar to GDPR, the law extends the definition of what constitutes sensitive and private data, making data classification critical for compliance.

ⓘ Why does it matter?

Like GDPR, CCPA non-compliance nets significant fines. Unlike GDPR, CCPA allows residents to file lawsuits against companies responsible for data leaks and breaches, pushing potential financial consequences to a higher bracket. Regional and state-level regulators look to CCPA as a model for their respective data privacy and security laws, so expect to see similar laws introduced at state and provincial levels.

California Consumer Privacy Act (CCPA)

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.	✓	Sections: 1798.130(a)(3),1798.130(a)(3)(A), 1798.130(a)(3)(B),1798.130(a)(4),1798.130(a)(4)(A), 1798.130(a)(4)(B), 1798.130(a)(4)(C)
Data Classification – classifying data by category and by data sensitivity.		
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.		
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.		
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.		
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Sections: 1798.110(a),1798.110(a)(1),1798.110(a)(2), 1798.110(a)(3),1798.110(a)(4),1798.110(a)(5),1798.110(b), 1798.110(c),1798.110(c)(1),1798.110(c)(2),1798.110(c)(3), 1798.110(c)(4),1798.110(c)(5),1798.135(a)(4),1798.135(a)(5), 1798.135(a)(6)
Data Custodians – identifying the owners or operators of systems, products and services that process data.		
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.		
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.		
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.		
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.		
Data Subject Rights – providing individuals with appropriate access to their personal data.	✓	Sections: 1798.100(a),1798.115(a),1798.115(a)(1), 1798.115(a)(2),1798.115(a)(3),1798.115(b),1798.115(c), 1798.115(c)(1),1798.115(c)(2),1798.130(a),1798.130(a)(1), 1798.130(a)(1)(A),1798.130(a)(1)(B),1798.130(a)(7),1798.130(c)
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.	✓	Sections: 1798.100(c),1798.100(d),1798.130(a)(2), 1798.130(a)(7),1798.130(b),1798.130(c)
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.		
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.	✓	Sections: 1798.105(a),1798.105(b),1798.105(c),1798.105(d), 1798.105(d)(1),1798.105(d)(2),1798.105(d)(3),1798.105(d)(4), 1798.105(d)(5),1798.105(d)(6),1798.105(d)(7),1798.105(d)(8), 1798.105(d)(9)
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.	✓	1798.81.5

Industry Regulations

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA covers a series of data privacy and security standards designed to protect health information. It outlines procedures that healthcare providers, organizations and associations must follow to ensure patient confidentiality and the security of protected health information (PHI).

Who does this affect?

At its core, HIPAA ensures that sensitive patient data is protected, no matter the medium in which it's been shared (written, digital or oral). Digitally, HIPAA data privacy and security measures guard patient information from potential breach events. Contrary to belief, HIPAA's reach extends beyond traditional healthcare delivery organizations (hospitals and doctors' offices), and requires any organization handling patient data to comply.

Why does it matter?

If healthcare organizations and related supply and partner organizations experience a breach event, compromised patient data can lead to life-impacting scenarios. An extreme example, but poignant as a model that other industries can follow when handling sensitive personal data and mitigating the risk that comes through service extensions and supply chains.

Health Insurance Portability and Accountability Act (HIPAA)

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.		
Data Classification – classifying data by category and by data sensitivity.		
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.		
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.	✓	Section: 164.506
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.	✓	Sections: 164.502, 164.514
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Sections: 164.502, 164.504
Data Custodians – identifying the owners or operators of systems, products and services that process data.		
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.		
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.		
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.		
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.		
Data Subject Rights – providing individuals with appropriate access to their personal data.	✓	Sections: 164.502, 164.522, 164.524
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.	✓	Section: 164.522
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.	✓	Section: 164.526
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.		
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.		

Industry Regulations

ISO 27701

ISO 27701 is an international IT governance standard that applies to all data processors and controllers. It's relevant to all organizations addressing personal data privacy and security risks. ISO 27701 is a foundational framework that supports broader compliance to other global, regional and industry security and data privacy standards and laws.

ⓘ Who does this affect?

All businesses can refer to and apply the standard within their own environment. Information Security Management Systems (ISMS) can work toward and achieve certification, which further supports security measures and a more robust security posture.

ⓘ Why does it matter?

ISO 27701 is globally recognized as a framework to support a hardened security posture. In terms of data privacy, the framework helps organizations cover the basics and implement data classification measures and processes that position companies for better alignment to other security standards and frameworks.

ISO 27701

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.		
Data Classification – classifying data by category and by data sensitivity.	✓	Section: 6.5.2.1
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.		
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.	✓	Sections: 7.2.2, 7.3.1, 7.3.2, 7.4.1, 8.2.1
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.	✓	Section: 7.4.4
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Sections: 6.5.2, 6.5.3.3, 7.4.2, 7.4.8, 8.2.3, 8.4.2
Data Custodians – identifying the owners or operators of systems, products and services that process data.		Section: 6.5.1.2
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.	✓	Sections: 6.5.3, 6.15.1.3, 7.4.7
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.	✓	Section: 7.4.3
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.		Sections: 6.3.1.5, 6.11, 6.11.1, 6.11.2, 6.11.2.1, 6.11.2.2, 6.11.2.5, 7.4, 8.4
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.		
Data Subject Rights – providing individuals with appropriate access to their personal data.	✓	Sections: 7.3.6, 8.2.5
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.	✓	Section: 7.3.9
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.		Sections: 7.3.6, 7.4.3, 8.2.5
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.		Sections: 7.3.6
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.		Section: 6.8.1.4

Industry Regulations

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is arguably the most universal security framework available, which is why the Cavelo platform aligns to the framework's classification and reporting guidelines. The first iteration of the framework was introduced in 2018, with a data privacy framework following two years later.

ⓘ Who does this affect?

The cybersecurity framework is designed to help businesses self-manage cybersecurity risk through policies and controls. IT and security leaders can use the framework to help prioritize cybersecurity efforts.

ⓘ Why does it matter?

The NIST Cybersecurity Framework is a voluntary guideline but following and implementing it will improve your organization's overall security posture and better position your business for other compliance obligations your business might face.

NIST Cybersecurity Framework

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.	✓	Section: PM-5(1)
Data Classification – classifying data by category and by data sensitivity.	✓	Sections: PT-7, PT-7(1), PT-7(2)
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.	✓	Sections: PL-2, SA-4(1), SA-4(2)
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.	✓	Section: PT-2
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.	✓	Sections: PM-25, SI-12(2), SA-8(33), SA-15(12)
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Sections: AC-23, MP-1, PM-24, PM-25, PT-2, PT-2(2), PT-3(1), PT-3(2), SI-18
Data Custodians – identifying the owners or operators of systems, products and services that process data.	✓	Sections: CM-8(4), PT-3(1), SA-4(12)
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.	✓	Sections: MP-7, SI-12
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.	✓	Sections: PM-22, PM-23, PM-24
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.	✓	Sections: CA-2, PM-11, PT-1, RA-9, SA-3, SA-3(1), SA-8, SA-8(30), SA-15(5), SC-1, SC-7(18), SI-1
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.	✓	Section: PL-2
Data Subject Rights – providing individuals with appropriate access to their personal data.	✓	Sections: AC-3(14), SI-18(4)
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.	✓	Sections: PM-26, SI-18(4)
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.	✓	Section: SI-18(4)
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.		
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.		

Industry Regulations

NIST Data Privacy Framework

Like the NIST Cybersecurity Framework, the NIST Data Privacy Framework is a voluntary guideline. It serves as a companion to the security framework, reaching farther to consider data privacy to support an improved cybersecurity posture. Combined, the Cybersecurity and Data Privacy Frameworks help organizations achieve five core functions: identify, protect, detect, respond and recover.

Who does this affect?

Any business, anywhere in the world, can refer to and apply recommendations outlined in the framework. Data discovery and classification underpin the recommendations, setting companies up for greater visibility and control over data processes – and ultimately, greater odds of compliance.

Why does it matter?

Following both the NIST Cybersecurity and the Data Privacy Frameworks can support businesses either revisiting or building out new security controls by helping to identify and properly catalog data.

NIST Data Privacy Framework

Data Discovery, Classification and Reporting Requirements	Is it relevant?	What is it relevant to?
Inventory of Personal Data – maintaining a list of personal data that is collected, used, transferred, stored, processed and created.	✓	Sections: CM.AW-P2, CT.DM-P1, GV.MT-P4, GV.MT-P7
Data Classification – classifying data by category and by data sensitivity.		
Data Flow Mapping – documenting flow of personal data and creating a record detailing geography, contact details, the purpose of storage, transmission and processing.	✓	Section: CT.DM-P4
Limited Collection & Use – limiting the collection, use, distribution, retention, disclosure and creation of personal data beyond what's necessary.	✓	Sections: CT.PO-P1, CT.DM-P1
Data Minimization – minimizing the collection, use, distribution, retention, disclosure and creation of personal data.	✓	Section: CT.DP-P4
Data Lifecycle Management – creating the processes and policies around the entirety of the data lifecycle from creation and collection to storage and destruction.	✓	Sections: CT.DM-P5, CT.DM-P7
Data Custodians – identifying the owners or operators of systems, products and services that process data.	✓	Sections: CT.DM-P7, ID.IM-P2
Retention of Personal Data – ensuring that all records containing personal data are maintained in accordance with a retention schedule.		
Quality Management – maintaining quality assurances throughout the information lifecycle with accuracy, relevancy, timeliness and completeness.	✓	Sections: CT.DM-P8, CT.PO-P4
Secure Data Processing – implementing secure data processing practices to ensure confidentiality and integrity through the data lifecycle.	✓	Sections: CM.AW-P3, CT.PO-P1, CT.DM-P7, CT.DM-P8, CT.PO-P4, ID.DE-P4, ID.IM-P5, PR.PP-P3, PR.PP-P4, PR.PP-P5
Data Lineage – maintaining historical reference and records of inputs, entities, systems, applications and processes that influence data of interest.	✓	Sections: ID.IM-P7, ID.IM-P8, ID.BE-P3, IN.AW-P6
Data Subject Rights – providing individuals with appropriate access to their personal data.	✓	Section: CT.DM-P1
Inquiry Management – maintaining the ability to receive and respond to privacy-related requests, complaints, concerns or questions.	✓	Sections: CM.AW-P2, CT.DM-P1, GV.MT-P4, GV.MT-P7
Updating Personal Data – providing individuals with appropriate opportunity to correct or amend their personal data.	✓	Sections: CT.DM-P1, CT.DM-P3
Right to Erasure – providing individuals with appropriate opportunity to request the deletion of personal data.	✓	Section: CT.DM-P4
Risk Management – implementing a risk management framework that identifies and addresses risk in a way that aligns with protection, trust and resilience.	✓	Sections: GV.MT-P1, GV.PO-P4, GV.RM-P1, GV.RM-P2, GV.RM-P3, ID.DE-P1

The Goal: Simplify Complex Compliance Exercises

Whether you're managing one compliance audit or several, you need systems in place to make the process as painless as possible. Many teams rely on multiple spreadsheets to gather the information and details they need to navigate exercises and audits, but these manual processes are prone to inaccuracies, data gaps and unintentional human error -- and tracking terabytes of data using spreadsheets is neither sustainable nor scalable. The rate of data growth within the average network makes continuous systems scanning essential to properly index data, eliminate redundancies, automate processes and scale for multiplying data sources.

Today's marketplace offers a number of choices when it comes to risk management and compliance, but the challenge comes down to finding a solution that can integrate with all of your data sources and systems (CRMs, SIEM and other logging software) to discover and appropriately classify various data types. Whether you're building new security policies and controls or revising existing cybersecurity frameworks, start with automated processes and data discovery at scale.

Simply put:

Compliance exercises and audits become easier when data is properly managed and classified.

Let Cavelo help you simplify compliance.

Data discovery doesn't have to be complicated – or expensive. The Cavelo data management platform offers all-in-one reporting capabilities designed to simplify data discovery and classification. With its intuitive dashboard and customizable features, you can easily configure the platform to match your business' unique compliance requirements and regulatory frameworks.

Take control of your data – reach out and talk to a Cavelo expert today!

Request a demo

cavelo

Cavelo helps businesses achieve attack surface management with automated data discovery, classification and reporting. Its cloud compatible cyber asset attack surface management (CAASM) platform continuously scans, identifies, classifies and reports on sensitive data across the organization, simplifying compliance reporting, vulnerability management and risk remediation.

For more information, visit **www.cavelo.com** or follow us on **LinkedIn**.