It's audit time.
Do you know where your data is?

If your answer is no, you're not alone. Your data is everywhere and the volume of data that collects on your company's servers, applications, computers, devices and hardware multiplies every day.

CAVELO

Nearly 90% of security leaders say they don't have adequate visibility of the data that they are required to protect.*

Why does it matter?

Regulators take data privacy seriously and continue to introduce new requirements to make sure businesses have the right measures in place to protect sensitive personal data from exploits and cyber-attacks. The regulators that matter to your business vary depending on the type of products or services you offer, but odds are your company is expected to comply to multiple frameworks, regulations and acts.

Even if you're confident that your inventory is up-to-date, achieving compliance is more than just ticking a box. You must be able to demonstrate the data you have, its classification and how it's being used.

Which regulations impact your business?

Every framework, regulation and act is unique to the audience or industry it serves, yet they all share common requirements when it comes to data collection, classification, tracking and management. This matrix zeros in on specific (and common) data collection and management definitions and audit requirements.

Source: 2019 Security Leader's Peer Report (Censuswide for Panaseer)

GLOBAL REGULATIONS

Requirement	Description	General Data Protection Regulation (GDPR) Articles	OWASP Privacy
Inventory of Personal Data	Create and maintain a list of personal data that is collected, used, transfered, stored, processed, and created. Includes the data element, as well as the systems and appliicactions that interact with the data.	Art 4 Art 5.2 Art 9	
Data Classification	Data must be classified according to the category and sensitivity as defined by appropriate statutory, regulatory and contractual contexts.	Art 4 Art 9	
The requirements below are made simpler when personal data is inventoried and classified			
Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity and privacy measures of the data controller.	Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5	
Limited Collection & Use	Limit the collection, use, distribution, retention, disclosure, and creation of personal data to what is required, resonably necssary and has legal basis	Art 5.1	P6
Data Minimization	Take steps to minimize the collection, use, distribution, retention, disclosure, and creation of personal data to what is directly relevant and necessary to accomplish a legally authorized purpose.	Art 5.1 Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11	
Data Lifecycle Management	Create the processes and policies around the entitrety of the data lifecycle from creation/collection to storage/ destruction	Art 5.1 Art 18.1 Art 18.2 Art 21.1 Art 21.2 Art 21.3 Art 32.1 Art 32.2	P4 P8
Data Custodians	Identify the owners or operators of systems/products/services that process data, or with which data subjects are interacting.		
Retention of Personal Data	Ensure that all records containing personal data are maintained in accordance with the organization's records retention schedule and comply with applicable statutory, regulatory and contractual obligations.	Art 5.1	P4
Quality Management	Maintain quality assurances throughout the information lifecycle with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual.	Art 5.1 Art 21.5 Art 22	
Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive data is maintained throughout the data lifecycle.		P10
Data Lineage	Maintain records of the inputs, entities, systems, applications and processes that influence data of interest, providing a historical record of the data and its origins.		
Data Subject Rights	Provide individuals with appropriate access to their personal data.	Art 12.1 Art 12.2 Art 13.2 Art 14.2 Art 15.1 Art 15.2 Art 15.3 Art 15.4 Art 16 Art 26.3	
Inquiry Management	Maintain a capability to receive and respond to privacy-related requests, complaints, concerns or questions from individuals.	Art 18.1 Art 18.2 Art 18.3 Art 19 Art 21.1 Art 21.6 Art 22 Art 26.3	
Updating Personal Data	Provide individuals with appropriate opportunity to correct or amend their personal data.	Art 5.1	
Right to Erasure	Provide individuals with appropriate opportunity to request the deletion of personal data where it is used, disseminated, maintained, retained and/or disclosed, including where the personal data is stored or processed by third-parties.	Art 17.1 Art 17.2 Art 17.3	
Risk Management	Implementation of a risk managememt framework that identifies and addresses risk in a way that alligns with protection, trust, and resiliience.	Art 32.1 Art 32.2	

REGIONAL REGULATIONS

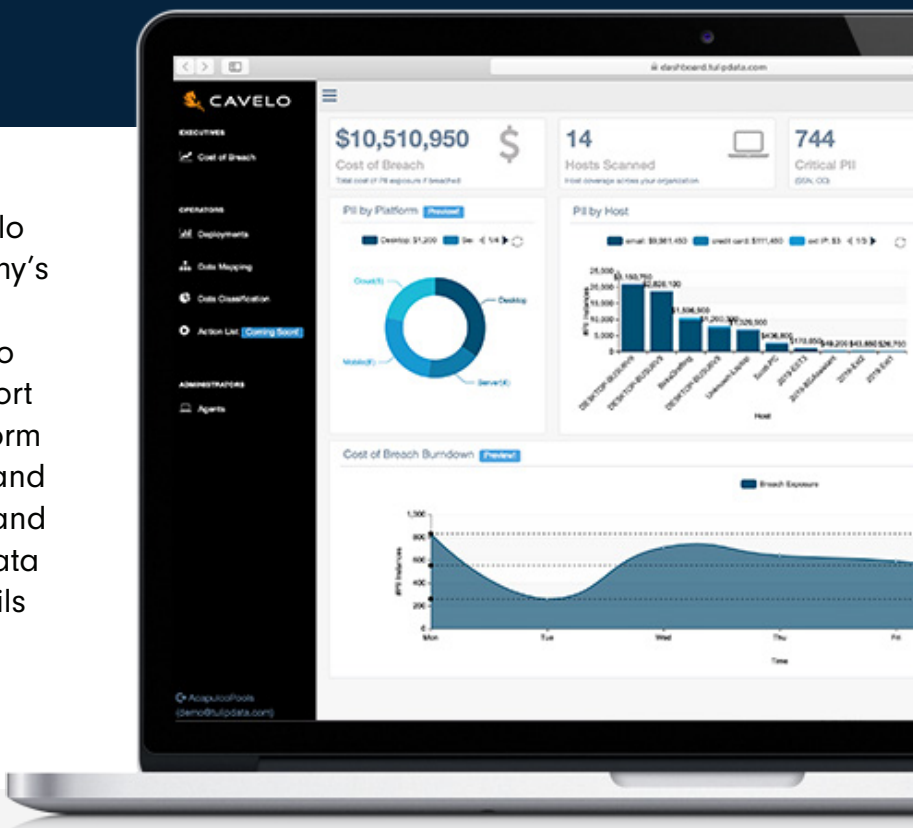
Requirement	Description	Personal Information Protection and Electronic Documents Act (PIPEDA) Principles (Canada)	California Consumer Privacy Act (CCPA)
Inventory of Personal Data	Create and maintain a list of personal data that is collected, used, transfered, stored, processed, and created. Includes the data element, as well as the systems and appliications that interact with the data.		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	Data must be classified according to the category and sensitivity as defined by appropriate statutory, regulatory and contractual contexts.		
The requirements below are made simpler when personal data is inventoried and classified			
Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity and privacy measures of the data controller.		
Limited Collection & Use	Limit the collection, use, distribution, retention, disclosure, and creation of personal data to what is required, resonably necssary and has legal basis	4 - Limited Collection	
Data Minimization	Take steps to minimize the collection, use, distribution, retention, disclosure, and creation of personal data to what is directly relevant and necessary to accomplish a legally authorized purpose.	4 - Limited Collection	
Data Lifecycle Management	Create the processes and policies around the entitrety of the data lifecycle from creation/collection to storage/ destruction	5 - Limited Use, retention and disclosure	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	Identify the owners or operators of systems/products/services that process data, or with which data subjects are interacting.		
Retention of Personal Data	Ensure that all records containing personal data are maintained in accordance with the organization's records retention schedule and comply with applicable statutory, regulatory and contractual obligations.	5 - Limited Use, retention and disclosure	
Quality Management	Maintain quality assurances throughout the information lifecycle with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual.	6 - Accuracy	
Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive data is maintained throughout the data lifecycle.		
Data Lineage	Maintain records of the inputs, entities, systems, applications and processes that influence data of interest, providing a historical record of the data and its origins.		
Data Subject Rights	Provide individuals with appropriate access to their personal data.	9 - Inidvidual Access	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©
Inquiry Management	Maintain a capability to receive and respond to privacy-related requests, complaints, concerns or questions from individuals.	10 - Challenging Compliance	1798.100(c) 1798.100(d) 1798.130(a)(2) 1798.130(a)(7) 1798.130(b) 1798.130(c)
Updating Personal Data	Provide individuals with appropriate opportunity to correct or amend their personal data.		
Right to Erasure	Provide individuals with appropriate opportunity to request the deletion of personal data where it is used, disseminated, maintained, retained and/or disclosed, including where the personal data is stored or processed by third-parties.		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	Implementation of a risk managememt framework that identifies and addresses risk in a way that alligns with protection, trust, and resiliience.		1798.81.5

INDUSTRY REGULATIONS

Requirement	Description	ISO 27701	NIST (rev 5)	NIST Privacy Framework v1.0	CMMC
Inventory of Personal Data	Create and maintain a list of personal data that is collected, used, transfered, stored, processed, and created. Includes the data element, as well as the systems and appliications that interact with the data.	6.5.2.1	PM-5(1)	ID.IM-P1 ID.IM-P3 ID.IM-P6	
Data Classification	Data must be classified according to the category and sensitivity as defined by appropriate statutory, regulatory and contractual contexts.		PT-7 PT-7(1) PT-7(2)		
The requirements below are made simpler when personal data is inventoried and classified					
Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity and privacy measures of the data controller.		PL-2 SA-4(1) SA-4(2)	ID.IM-P1 ID.IM-P4	
Limited Collection & Use	Limit the collection, use, distribution, retention, disclosure, and creation of personal data to what is required, resonably necssary and has legal basis	7.2.2 7.3.1 7.3.2 7.4.1 8.2.1	PT-2	CT.PO-P1 CT.DM-P1	
Data Minimization	Take steps to minimize the collection, use, distribution, retention, disclosure, and creation of personal data to what is directly relevant and necessary to accomplish a legally authorized purpose.	7.4.4	PM-25 SI-12(2) SA-8(33) SA-15(12)	CT.DP-P4	
Data Lifecycle Management	Create the processes and policies around the entitrety of the data lifecycle from creation/collection to storage/ destruction	6.5.2 6.5.3.3 7.4.2 7.4.8 8.2.3 8.4.2	AC-23 MP-1 PM-24 PM-25 PT-2 PT-2(2) PT-3(1) PT-3(2) SI-18	CT.DM-P5 CT.DM-P7	
Data Custodians	Identify the owners or operators of systems/products/services that process data, or with which data subjects are interacting.	6.5.1.2	CM-8(4) PT-3(1) SA-4(12)	CT.DM-P7 ID.IM-P2	
Retention of Personal Data	Ensure that all records containing personal data are maintained in accordance with the organization's records retention schedule and comply with applicable statutory, regulatory and contractual obligations.	6.5.3 6.15.1.3 7.4.7	MP-7 SI-12		
Quality Management	Maintain quality assurances throughout the information lifecycle with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual.	7.4.3	PM-22 PM-23 PM-24	CT.DM-P8 CT.PO-P4	
Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive data is maintained throughout the data lifecycle.	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	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	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	Maintain records of the inputs, entities, systems, applications and processes that influence data of interest, providing a historical record of the data and its origins.		PL-2	ID.IM-P7 ID.IM-P8 ID.BE-P3 IN.AW-P6	
Data Subject Rights	Provide individuals with appropriate access to their personal data.	7.3.6 8.2.5	AC-3(14) SI-18(4)	CT.DM-P1	
Inquiry Management	Maintain a capability to receive and respond to privacy-related requests, complaints, concerns or questions from individuals.	7.3.9	PM-26 SI-18(4)	CM.AW-P2 CT.DM-P1 GV.MT-P4 GV.MT-P7	
Updating Personal Data	Provide individuals with appropriate opportunity to correct or amend their personal data.	7.3.6 7.4.3 8.2.5	SI-18(4)	CT.DM-P1 CT.DM-P3	
Right to Erasure	Provide individuals with appropriate opportunity to request the deletion of personal data where it is used, disseminated, maintained, retained and/or disclosed, including where the personal data is stored or processed by third-parties.	7.3.6		CT.DM-P4	
Risk Management	Implementation of a risk managememt framework that identifies and addresses risk in a way that alligns with protection, trust, and resiliience.	6.8.1.4		GV.MT-P1 GV.PO-P4 GV.RM-P1 GV.RM-P2 GV.RM-P3 ID.DE-P1	
Controlled Unclassified Information (CUI)	Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13536 or the Atomic Energy Act, as amended.				NIST 800-171

Don't know where to start?

The first step to achieving compliance is to discover your data.



Powered by machine learning, the Cavelo platform continuously scans your company's cloud applications, cloud hosted servers and on-premises servers and desktops to identify, classify, track, manage and report on sensitive data. With the Cavelo platform you can classify and tag sensitive data and personally identifiable information (PII) and build a comprehensive audit trail and data inventory that will arm you with the details you need to manage your next audit.

We're here to help.

We're passionate about data discovery and risk management which is why we want you to try the Cavelo platform for free. Reach out today to info@cavelo.com to schedule your custom demo and sign up for your free account.

CAVELO

Cavelo helps businesses proactively reduce cybersecurity risk and achieve compliance with automated data discovery, classification and reporting. Its cloud compatible data risk management platform continuously scans, identifies and classifies sensitive data across laptops, servers and cloud applications, simplifying compliance reporting and risk remediation. For more information visit www.cavelo.com or follow us on Twitter and LinkedIn.