



Accedere

Privacy Assessment & Attest Services

Contents

- About us
- Increasing Privacy Penalties
- GDPR
- CCPA
- Some New Privacy Laws
- Privacy Compliance
- Risk Assessment
- Privacy Assurance
- How can we help



About Us



Colorado Licensed CPA Firm

Focusing on Cyber Security Audits

Cloud and Data Privacy Experts

Specializing in SOC Attest Reports

Why Accedere



We are a firm focusing on Cloud Security and Data Privacy



Our team carries extensive experience in the field and are listed with Cloud Security Alliance as Auditors



Our team has several years of Cybersecurity experience with leading industry certifications.



We have specific experience working with cloud controls for clients such as Cisco, Reliance Jio etc.





Accedere

Some hefty privacy, data breach fines

- Yahoo: \$117.5 million
- Anthem: \$16 million
- Uber: \$148 million
- Tesco bank: \$21 million
- Equifax: \$ 700 million
- Google: \$50 million
- British Airways: \$230 million
- Marriott: \$126 million
- Facebook: \$5 billion
- Other GDPR fines



Yahoo \$117.5 million fine

Fine	\$117.5 million
Country	United States of America
Date	August 2013
Incident	Malicious actors were able to gain access to Yahoo's user database and took records for all existing Yahoo accounts, which was approximately 3 billion. This data breach wasn't disclosed until years later 2016

YAHOO!



Anthem \$16 million fine

Fine	\$16 million
Country	United States of America
Date	December 2014
Incident	Cyber attackers gained access to Anthem's IT system via an undetected continuous and targeted cyberattack. Following the breach report, Anthem discovered that hackers accessed its system through phishing emails, a common method for cyberattacks. Hackers sent the phishing emails to an Anthem subsidiary after at least one employee responded to a malicious email, opening the door to further attacks.



Uber \$148 million fine

Fine	\$148 million
Country	United States of America
Date	May 2016
Incident	The data was compromised in 2016 by hackers, who obtained 607,000 U.S. driver's license numbers as well as tens of millions of consumer email addresses and phone numbers, a leak that Uber failed to disclose for more than a year after discovering the attack.



Tesco bank \$21 million fine

Fine	\$21 million
Country	United Kingdom
Date	November 2016
Incident	<p>In November 2016 cyber attackers exploited deficiencies in Tesco Bank's design of its debit card and in its financial crime controls.</p> <p>The deficiencies left Tesco Bank's personal current account holders vulnerable to a largely avoidable incident that occurred over 48 hours and which netted the cyber attackers 2.26 million pounds.</p>



Equifax \$700 million fine

Fine	\$700 million
Country	United States of America
Date	May 2017
Incident	<p>The data breach affected 146 million customers</p> <p>The Information Commissioner's Office (ICO) issued Equifax with \$ 6 million dollar for failing to protect the personal information of up to 15 million UK citizens during a cyber attack in 2017.</p> <p>The ICO investigation found that, although the information systems in the US were compromised, Equifax Ltd was responsible for the personal information of its UK customers.</p>



Google \$57 million fine

Fine	\$57 million
Country	France
Date	May 2018
Incident	An investigation in May 2018 found that Google failed to obtain a valid legal basis for processing personal data for ad personalization, in violation of the GDPR's requirements for specific and unambiguous consent for all forms of personal data processing



British Airways \$ 123 million fine

Fine	\$123 million
Country	United Kingdom
Date	June 2018
Incident	Poor security at the airline allowed hackers to divert about 500,000 customers visiting the British Airways website last summer to a fraudulent site, where names, addresses, login information, payment card details, travel bookings and other data were taken.



Marriott \$ 126 million fine

Fine	\$126 million
Country	United Kingdom
Date	November 2018
Incident	<p>An investigation has revealed that unknown parties gained access to the database sometime in 2014, copying and encrypting information that had been stored there. Marriott said it was alerted to unauthorized activity and began an investigation in September 2018.</p>



Facebook \$ 5 billion fine

Fine	\$5 Billion
Country	United States of America
Date	July 2019
Incident	The Federal Trade Commission announced a \$5 billion settlement with Facebook, resolving a sweeping investigation by regulators into how the company lost control over massive troves of personal data and mishandled its communications with users. It is the largest fine in FTC history — and yet still only about a month's worth of revenue for Facebook.



Other GDPR fines

Date	Country	Company	Fine	Incident
January, 2019	France	Google	€50,000,000	Google was fined from France's data regulator, citing a lack of transparency and consent in advertising personalization, including a pre-checked option to personalize ads.
August, 2019	Bulgaria	National Revenue Agency	€2,600,000	Records of 6 million people was accessed in a security breach.
October, 2019	Germany	Deutsche Wohnen	€14,500,000	Unlawful storage of personal information in an archive system that did not have an option to delete old data.
November, 2019	Netherlands	Uber	€600,000	A 2016 data breach concerning 57 million Uber users, of which 174,000 were Dutch citizens, was not reported within 72 hours



Privacy Assessment

Privacy Assessments are important in order to understand the organization's privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships etc.

The main goal of a privacy assessment include:

- The information collected should comply with all privacy-related legal and regulatory compliance requirement.
- Identifying the privacy risks, defining the same and monitoring incidents.
- Taking actions to mitigate the risks.



GDPR

Introduction

GDPR stands for the European Union General Data Protection Regulation. GDPR replaced the older EU Data Protection Directive and has been in effect since 25 May 2018.

Applicability of GDPR Privacy Framework

The GDPR applies to all EU organizations, whether commercial business or public authority, that collect, store or process the personal data of EU individuals.

It is also applicable to a company established outside the EU and is offering goods/services (paid or for free) or is monitoring the behavior of individuals in the EU.



The Regulation also requires such organizations, controllers and processors, to appoint an EU representative based in one of the member states in which the relevant individuals are based. This is unless the processing is occasional and does not include large scale processing of special categories of data or processing of data relating to criminal convictions and offences.

The Brexit effect

GDPR is enforced in UK by the Information Commissioner's Office (ICO). So, UK organizations handling personal data still need to comply with the GDPR, regardless of Brexit.



GDPR principles



GDPR PRINCIPLES:
Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime. The principles are similar to principles in the Data Protection Act 1998.

- 1 Lawfulness, fairness and transparency
- 2 Purpose Limitation
- 3 Data Minimisation
- 4 Accuracy
- 5 Storage Limitation
- 6 Integrity and Confidentiality
- 7 Accountability



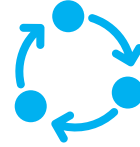
Privacy for Consumers



The right to be informed



The right to rectification



The right to restrict processing



The right to object



The right to access



The right to erasure



The right to data portability



Rights in relation to automated decision making and Profiling.



Personal Information (PI)

The GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data.

The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organizations collect information about people.

For most organizations, keeping HR records, customer lists, or contact details etc. the change to the definition should make little practical difference.



CCPA

CCPA Privacy

- On June 28, 2018, Governor Brown signed Assembly Bill 375, now known as the California Consumer Privacy Act of 2018, which grants consumers new rights with respect to the collection of their personal information. The regulations aim to establish procedures to facilitate consumers' rights under the CCPA and provide guidance to businesses for how to comply.
- The CCPA is now effective from January 1, 2020



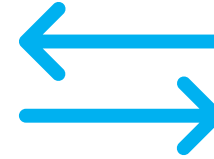
Individual Rights in CCPA



Right to notice



Right to access



Right to opt out (or right to opt in)



Right to request deletion



Right to equal services and prices



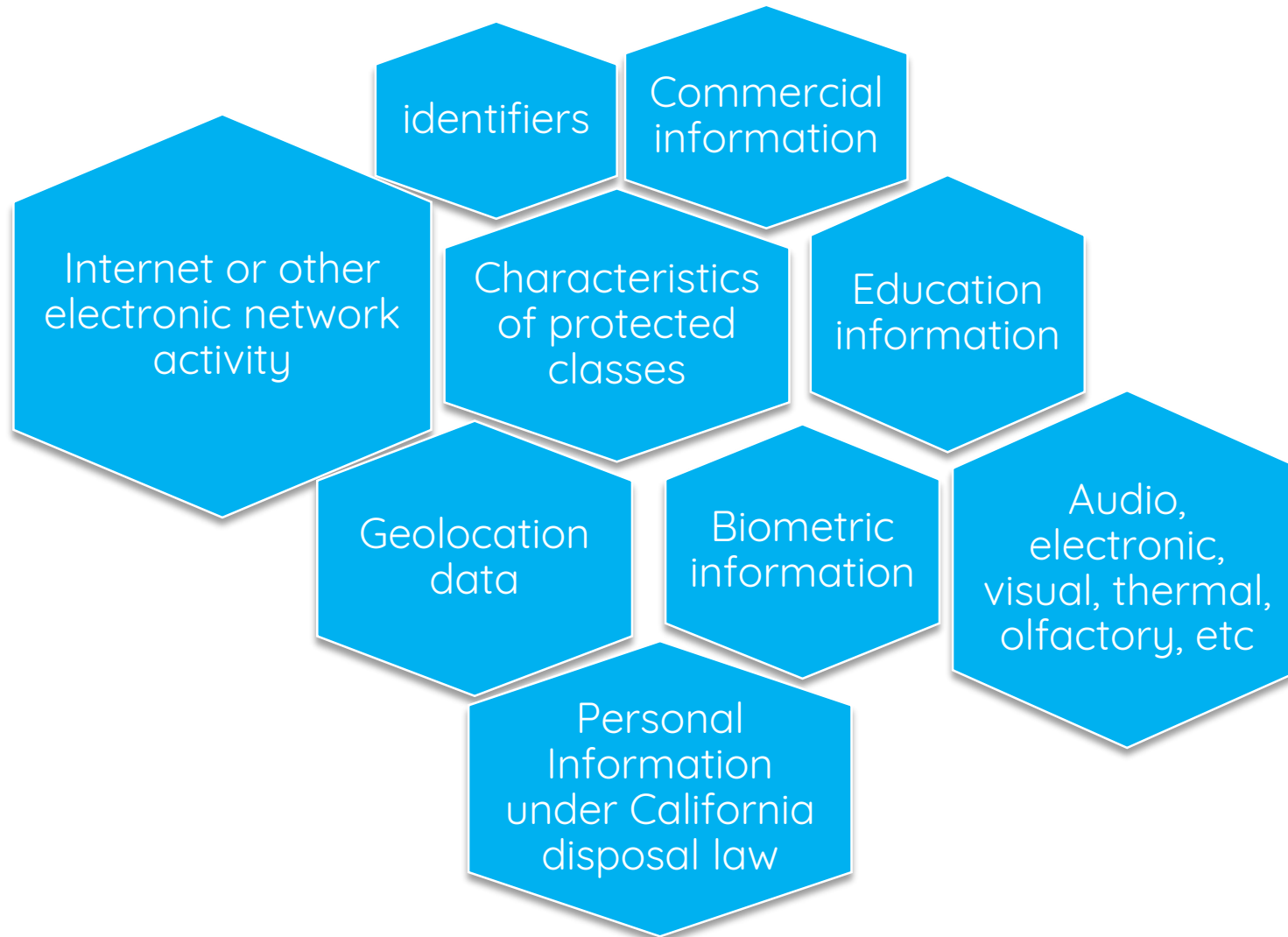
CCPA Privacy

The CCPA controls the manner in which “businesses” treat the “personal information” of California residents. The CCPA defines “business” to mean any for-profit legal entity doing business in California that:

- (1) Has annual gross revenues in excess of \$25 million
- (2) Alone, or in combination, buys, receives, sells or shares the personal information of 50,000 or more California residents, households or devices.
- (3) Derives 50% or more of its annual revenues from selling California residents’ personal information.



CCPA categories of Personal Information



CCPA and GDPR

Differences

Compliance Area	GDPR	CCPA
Compliance Deadline	May 25, 2018	January 1, 2020
Applicability	In the EU and organizations offering goods and services to people in the EU.	California and organizations doing business in California.
Who it Protects	All the individuals in Europe Union as data Protection is seen as a fundamental human right.	Focus is on California residents.
Area of Focus	It covers almost all aspects of data protection.	Focus is on data subject rights, transparency, third party management and training but compliance is dependent on privacy program accountability.









CCPA and GDPR

Similarities

Compliance Area	GDPR and CCPA
Individual Rights	Having a mechanism containing a broad scope of requests, timely responding to requests and keeping an audit trail should be a part of an individual rights program.
Consent	Having mechanism for ensuring that data processing is permitted and lawful, such as consent management should be a part of an overall data privacy management programs.
Notice	Notice should be a part of the overall data privacy management programs.
Data Inventory	Having an up-to-date inventory that shows what data is being collected, why is it being collected and who is using it is a part of the compliance requirement.



OTHER DATA PRIVACY LAWS

LAW	Country	Applicable from
General Data Protection Law (Brazil)		2020
India's Personal Data Protection Bill		2020
Vermont Act 171		2019
New Zealand Privacy Bill		1 March, 2020
PIPEDA Privacy (Canada)		13 April, 2000
POPI – Protection of Personal Information Act (South Africa)		26 November, 2013



Brazil's General Data Protection Law (LGPD)

Effective date : Early 2020

August 14, 2018, Brazil approved the General Data Protection Law (in Portuguese). The law will come into effect after its 18th adaptation period, in early 2020.

The scope:

Like the European Union's General Data Protection Regulation, the LGPD will have extraterritorial application. It means that the law will also affect every foreign company that offers services to the Brazilian market and collects and processes the personal data of data subjects located in Brazil.

Maximum Penalty: 2% of a private legal entity's, group's, or conglomerate's revenue in Brazil, for the prior fiscal year, excluding taxes, up to a total maximum of 50 million reals (\$1,24,21,435)



India Personal Data Protection Bill

Effective date : Early 2020

in July 2017, the Government of India formed a committee of experts to study the issues related to data protection in the country. The Bill is expected to become a law or an Act in 2020.

The scope:

Through the proposed law, the Government of India is rooting for data sovereignty by mandating certain class of data to be stored within Indian borders.

The Bill also allows processing of data by fiduciaries with the consent of the individual. A data fiduciary is an individual or entity that decides the purpose of processing personal data.

Maximum Penalty: Any organization sharing customers' data without their consent will entail a fine of INR 15 crores (around US\$ 2.1M) or 4 percent of its global turnover. Data breach and delay to address/report the same will result in a fine of INR 5 crores (US\$ 0.7M) or 2 percent of global turnover.



Vermont Act 171 (Data Broker Regulation)

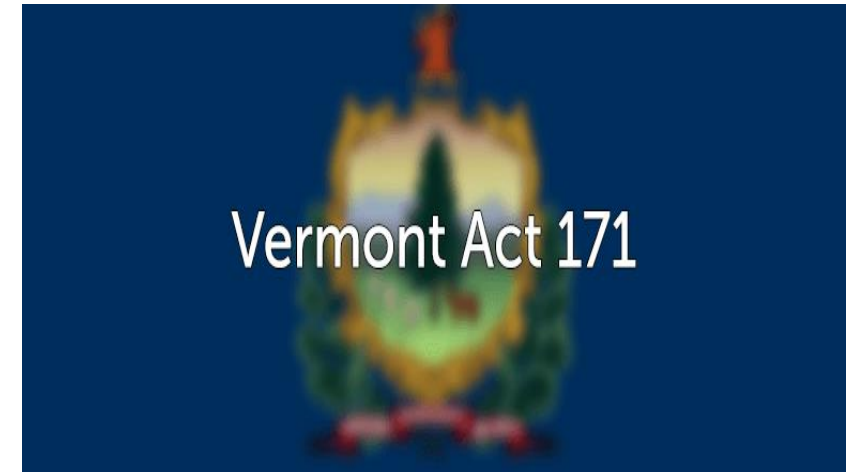
Effective date : January 1, 2019

On December 11, 2018, the Vermont Office of the Attorney General published new guidance on the state's data broker law (Act 171 of 2018), which imposes new data breach notification requirements on “data brokers”.

The scope:

Businesses that qualify as “data brokers” must register with the Vermont Secretary of State annually. Data brokers must track and report to the Secretary of State annually the number of security breaches they experience during the prior year and, if known, the number of Vermont consumers affected.

Maximum Penalty: Companies who met the definition of a “data broker” in 2018 are obligated to register with the Vermont Secretary of State by January 31, 2019 to avoid a penalty of \$50 per day, up to a maximum of \$10,000 per year.



New Zealand Privacy Bill

Effective date : March 1, 2020

The Bill if passed into law, it will repeal and replace New Zealand's existing Privacy Act 1993.

The scope:

Bill would apply to the actions taken by and all personal information collected or held by:

New Zealand agencies, both inside and outside New Zealand and Overseas agencies carrying on business in New Zealand, regardless of where the personal information is held.

Maximum Penalty: The penalty for non-compliance will be \$10,000.



PIPEDA Privacy (Canada)

Effective date : April 13, 2000

The act originally went into law on April 13, 2000 to foster trust in electronic commerce but has expanded since to include industries like banking, broadcasting, and the health sector with new changes applicable from November 1, 2018.

The scope:

The Act applies to interprovincial and international transactions by organizations that flow across borders, along with federally regulated organizations like banks, telecommunications and transportation companies. The Act, even in provinces with similar legislation on the books, does apply to personal information collected, used, or disclosed by federally regulated organizations.

Maximum Penalty: Failure to report the potential for significant harm could expose private-sector organizations to fines of up to \$100,000 for each time an individual is affected by a security breach.



POPI – Protection of Personal Information Act

Effective date : November 26, 2013

In 2013, South Africa passed the Protection of Personal Information Act (POPI). But is not active yet. It is expected to be brought in practice by 2020.

The scope:

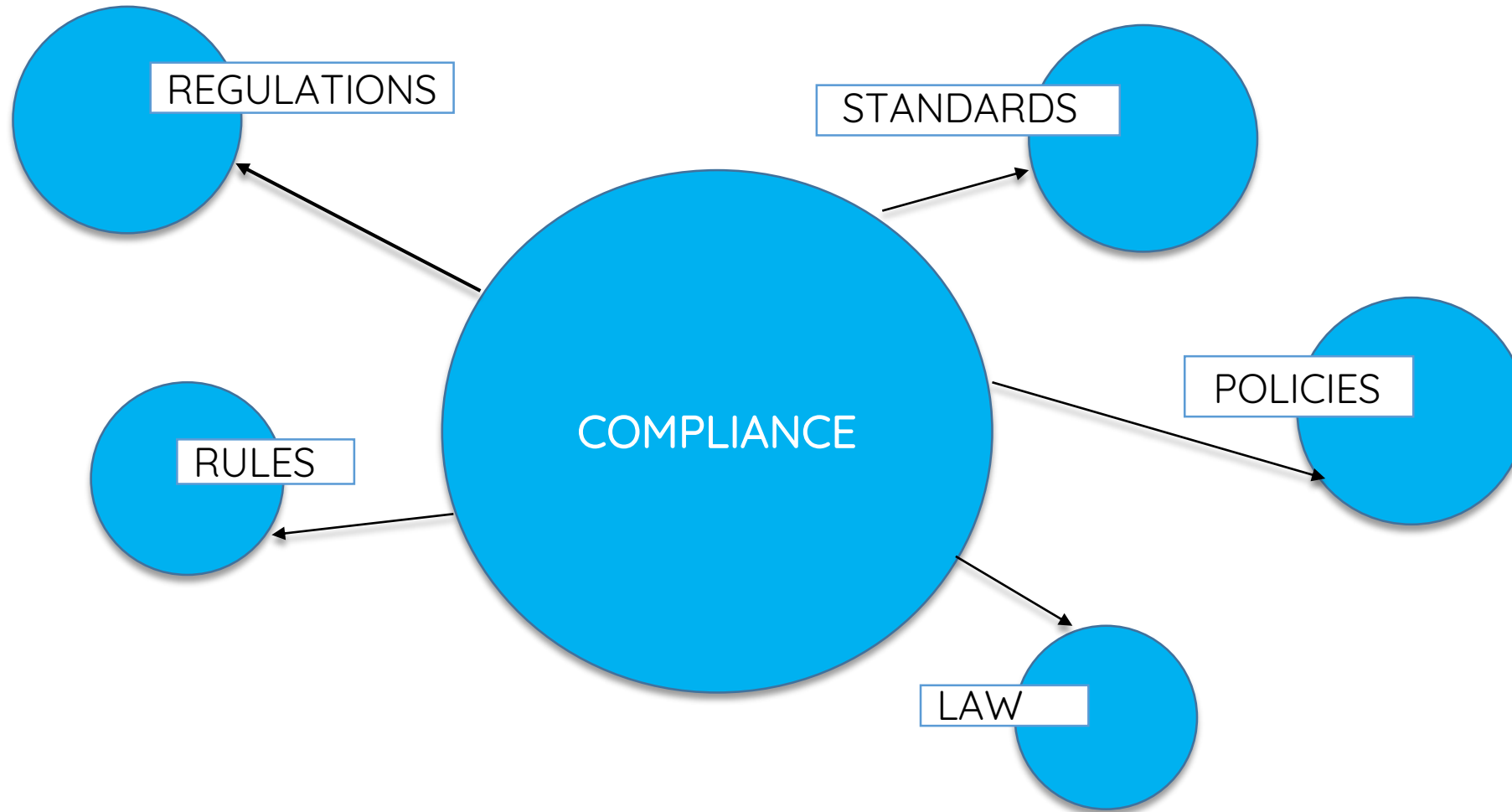
POPI applies to data processors or responsible parties who are either domiciled in the Republic of South Africa or who are domiciled elsewhere but "makes use of automated or non-automated means" in South Africa.

Maximum Penalty: Fines can go up to R10-million Rand (\$6,99,409) and, in extreme cases, there is also the possibility of spending up to 10 years in jail.



Privacy Compliance

Compliance Requirements



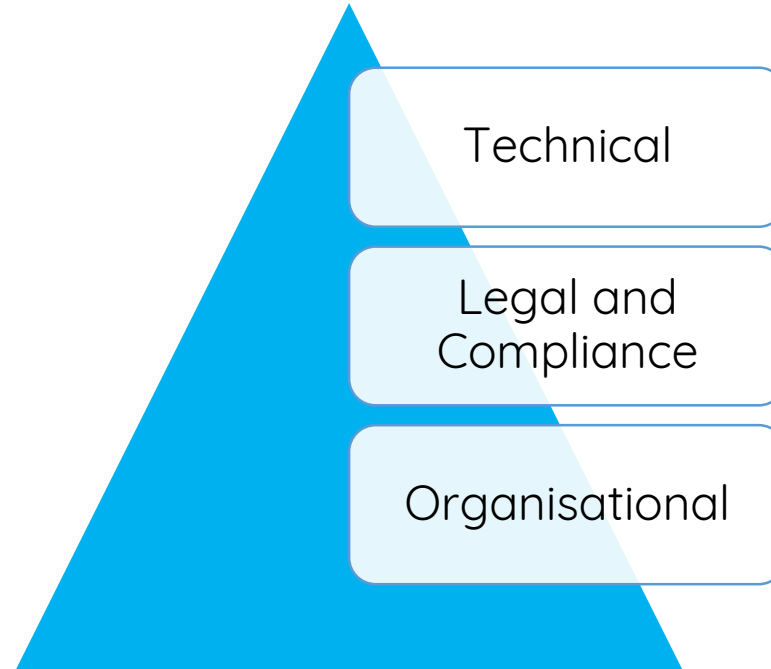
Organizations under Compliance

- Software as a Service (SaaS) and Application Service Providers (ASP)
- Data Centres/Co-Location Centre's
- Health Care Services
- Payroll Organizations
- Business Process Outsourcing (BPO) Entities
- Knowledge Management (KM) Systems
- Customer Relationship Management (CRM) software applications
- Managed Services Centre's
- Mortgage Service and Payment Entities
- I.T. Managed Services Entities
- Cloud Service Providers
- Tax Processing Service Providers
- Payment Collection or Processing Entities
- Other Financial or Intellectual Property Services



How to Comply?

The privacy laws encourages the adoption of certification schemes to demonstrate compliance. Compliance with the international information security standard ISO 27001, can help organizations demonstrate the data security requirements of the various privacy laws. Implementing ISO 27001 and adapting that for privacy compliance involves building a holistic framework of processes, people and technologies to secure information.



How to Comply?

Governance Model : Build a Governance model with a steering committee to comply with Privacy requirements and adapt a framework

Policies/Procedures: Build/Update policies/procedures incorporating privacy law requirements

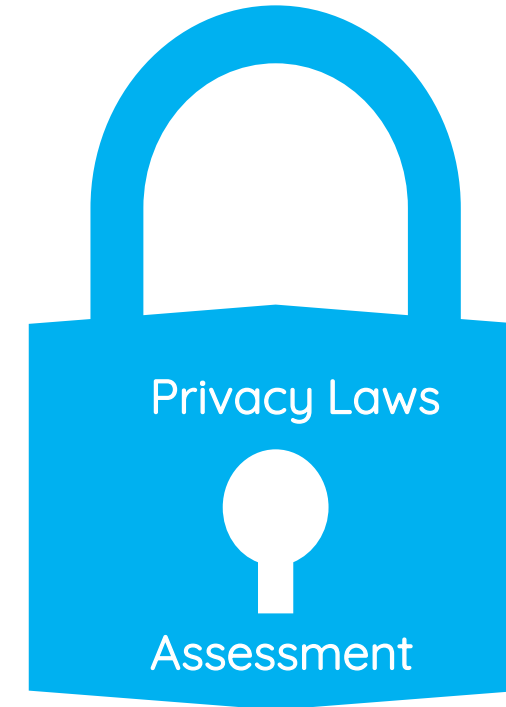
Third Party Agreement Modifications: Review and update Third Party Agreements, and use SOC reports for compliance by Third Parties

Notice of Privacy Practices : Identify and develop a plan for meeting own applicable requirements

Update Forms: Update forms, such as requests for opt out for privacy laws

Training: Train workforce & third parties on the privacy law requirements

Encryption: Encrypting of PI



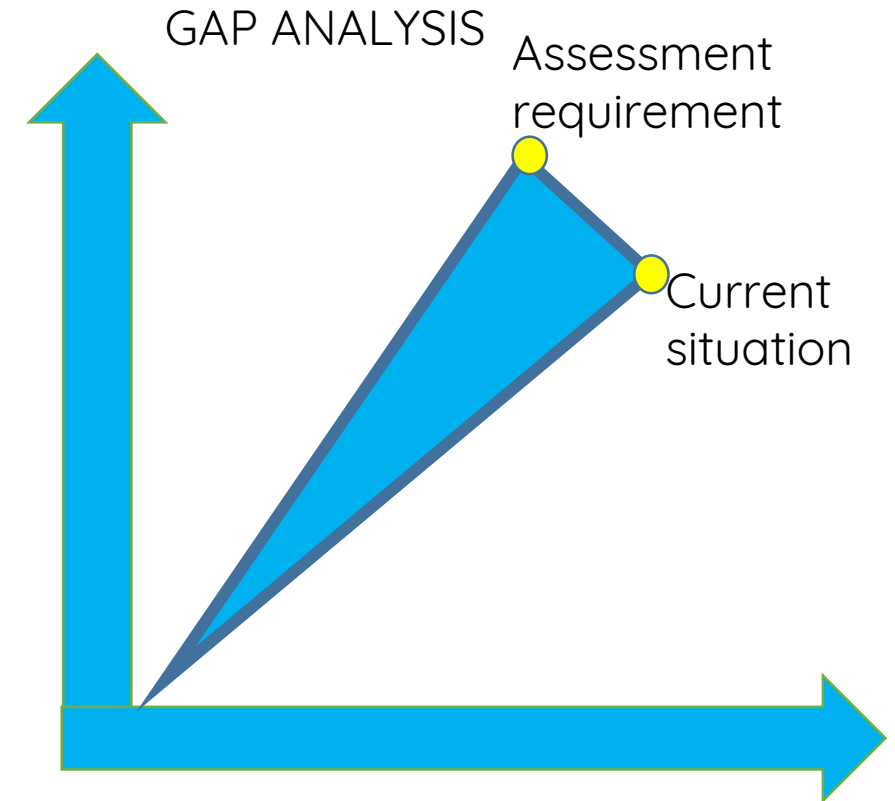
Risk Assessment for Privacy

Risk Assessment

Risk Assessment /Management is a required element for privacy compliance. We provide a framework for your risk management program in your organization specifically covering your end to end processes mapping them to the privacy compliance requirements.

GAP Analysis

After conducting a Risk Assessment /Management process, we can help you with conducting a GAP analysis or a readiness assessment for your organization specifically covering your processes mapping them to the privacy compliance requirements.



Privacy Risk Assessment

Once the organization has understanding of its data assets and usage the next step is to conduct a privacy risk assessment.

The purpose of a Privacy Risk Assessment is to provide an early warning system to detect privacy problems, enhance the information available internally to facilitate informed decision-making, avoid costly or embarrassing mistakes in privacy compliance, and provide evidence that an organization is attempting to minimize its privacy risks and problems.



Privacy Risk Assessment

identify

Describe the project, including the aims, whatever any personal information will be handled, inherent privacy principles.

analyse

Identify the personal information flows, classify data, identify relevant regulations, privacy requirements, privacy impact.

verify

Validate that only essential data is collected and processed for legitimate purposes required by the product or service.

simplify

Change system and processes to only collect/store/process essential data for minimum period with a data deletion plan



Privacy Risk Assessment

secure

Use industry best practices for safeguarding personal data through life cycle, providing consumer control over their data.

remediate

Identify remaining risk, level of harm and mitigate plan to eliminate or reduce risk to acceptable level.

attest

Record findings, gain sponsor commitment to implement any needed changes report results to management.

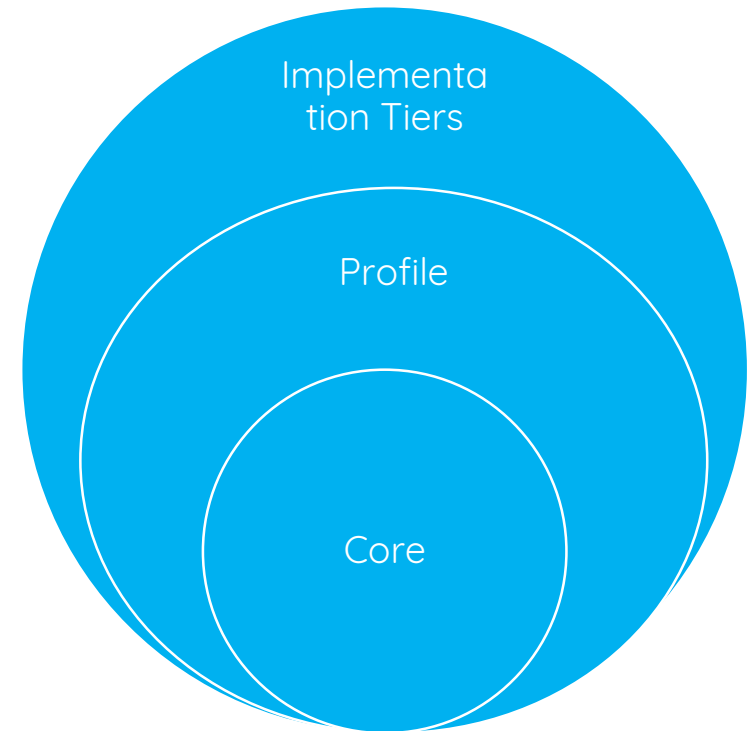


NIST Privacy Risk Assessment Framework

The NIST Privacy Framework is designed to be a tool to help an organization determine the risk levels of data privacy within their systems.

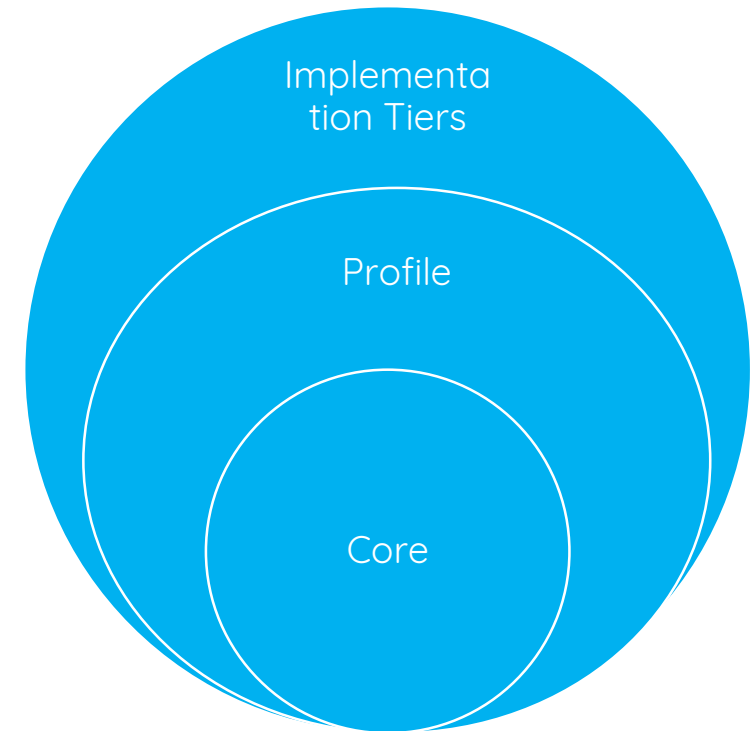
The framework is split into three parts:

- Core: It gives you the tools to determine the specific activities needed to manage the risk when a system, app, device, service, etc. processes data. The core has five key functions upon which your privacy risk management turns:
 1. Identify (data and risks)
 2. Govern (legal and organizational policies)
 3. Control
 4. Communicate
 5. Protect



Privacy Risk Assessment Framework

- Profile: This covers an organization's current privacy policies and/or where they are trying to get to, in terms of privacy.
- Implementation Tiers: An organization's "tiers" allow it to stand back and look at processes and procedures around privacy



ISO Privacy Risk Assessment Framework

Scope: Defining what is critical to protect in your organization.

Risk Management: Regularly evaluating risks and developing the best Risk Treatment Plans to help thwart risks.

Assess: Monitor and assess the environment to ensure efficacy and work toward continuous improvement.

Governance: Senior management should set out to establish reasonable risk tolerance and acceptance.



OR

Privacy Risk Assessment Framework

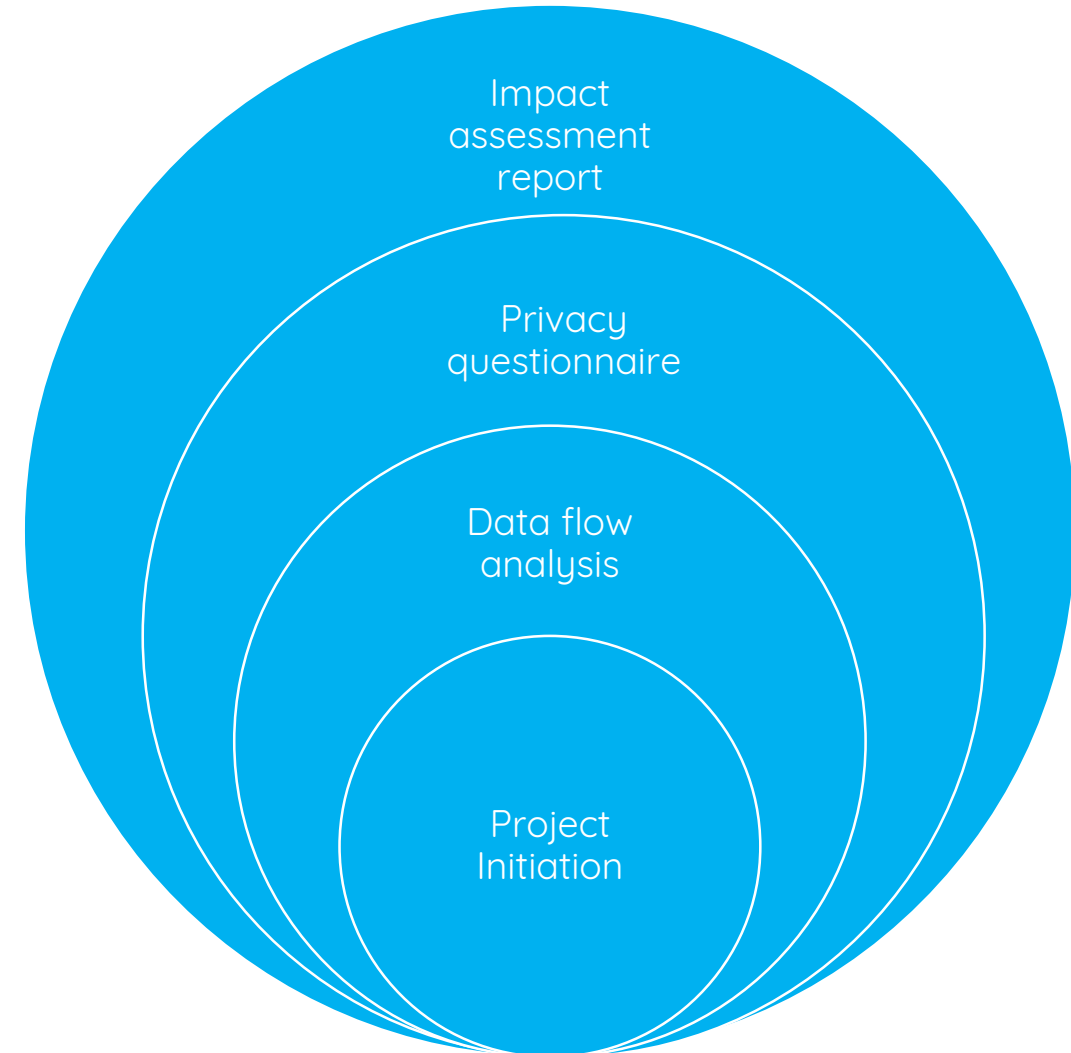
Impact Assessments usually involve approximately four phases:

- The project initiation,
- Data flow analysis,
- Privacy questionnaires and
- Impact assessment report.

In project initiation, the scope of the project is defined. In the data flow analysis, the organization maps out the data flows for the particular process subject to the assessment.

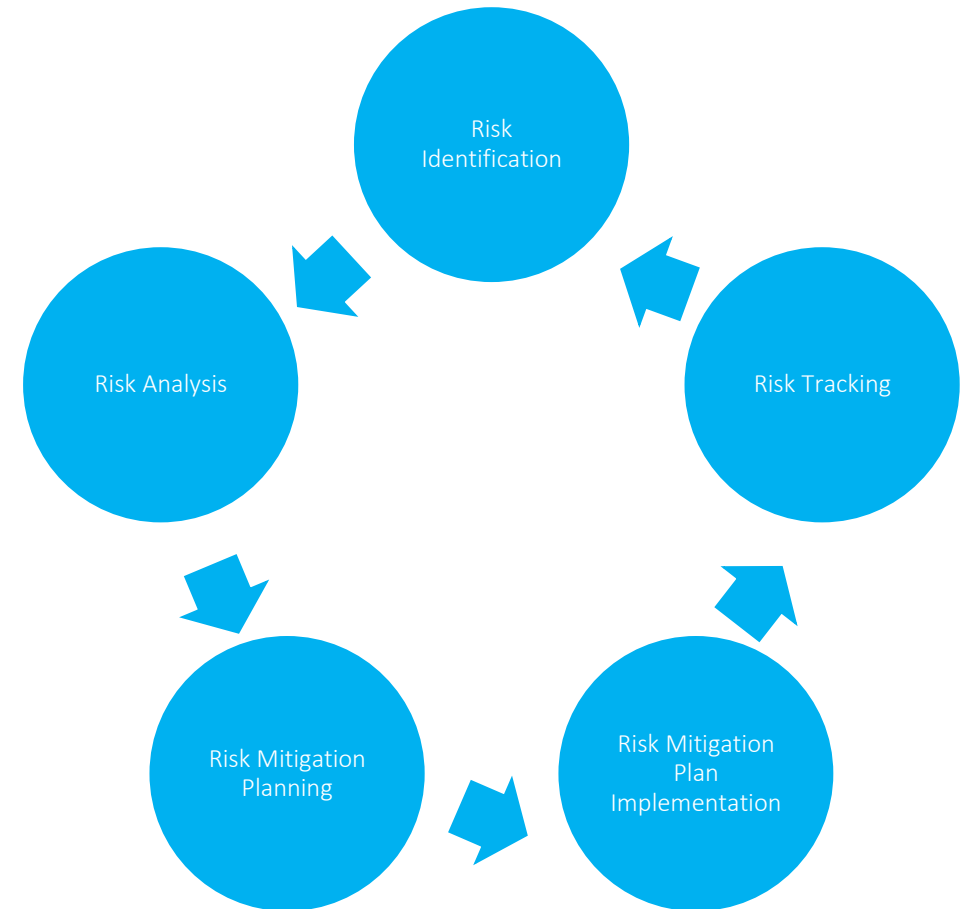
Additional information is gathered in the third phase to identify additional privacy issues, and the implications of concerns analyzed.

Finally, a report is produced to document the potential risks, offer potential solutions to mitigate or remedy the risks identified.



Risk Mitigation

We can help your organization implement the controls or safeguards based on your risk assessment to mitigate those risks and help you with solutions based on People, Process or Technology.





Accedere

Why Privacy Assurance?

SOC 2 reports for privacy

AICPA SOC reports for Privacy

Service Organization Controls (SOC) 2 report for privacy is based on American Institute of Certified Public Accountants (AICPA) SSAE 18 standard and Trust Services Criteria.

When the description addresses privacy, service organization management discloses the service commitments and system requirements identified in the service organization's privacy notice or in its privacy policy that are relevant to the system being described.



SOC 2 reports for privacy

Privacy has become even more important issue in the current environment with several large organizations facing heavy fines.

With about 50 points of focus,
The TSC 2017 organizes privacy criteria as under:

- Notice and communication of objectives
- Choice and consent
- Collection
- Use, retention and disposal
- Access
- Disclosure and notification
- Quality
- Monitoring and enforcement



SOC 2 reports for privacy

SOC 2 report conveys trust and assurance to users of the system that the service organization has deployed an effective control system to effectively mitigate operational and compliance risks that the system may represent to its users.

It addresses System and Organization Controls using Trust Services Criteria (TSC) for service organizations to apply and report on controls that may affect users of their service.



SOC 2 reports for privacy

A SOC 3 engagement is similar to a SOC 2 engagement in that the practitioner reports on whether an entity (any entity, not necessarily a service organization) has maintained effective controls over its system with respect to its system with respect to TSC

The SOC 2 Type II currently provides the Most Reasonable Assurance for the following reasons:

- SOC Type II report can cover the entire year and the effectiveness of the controls in place can be reported
- It is a Third-Party Period- of-Time assessment and so has Accountability



SOC 2 reports for privacy

- Since it is a period-of-time assessment, it is more like a continuous compliance with low risk and high reliability
- Most other assurance programs or audits are only, at a point in time
- Comprehensive Framework for Privacy
- Provides a high reliability SOC Seal by AICPA



SOC 2 reports for privacy

The following are examples of system requirements:

- Workforce member fingerprinting and background checks established in government banking regulations.
- System edits that restrict the values accepted for system input, which are de-fined in application design documents.
- Maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual.
- Data definition and tagging standards, including any associated meta data requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol (SOAP).
- Business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA).



SOC 2 CLOUD AND PRIVACY CONTROL

Soc 2+ Cloud CCM

- CSA, in collaboration with the AICPA, developed a third-party assessment program of cloud providers officially known as CSA Security Trust and Assurance Registry (STAR) Attestation.
- STAR Attestation provides a framework for CPAs performing independent assessments of cloud providers using SOC 2 engagements with the CSA's Cloud Control matrix.

SOC 2+ C5

- The C5 is intended primarily for CSPs, their auditors and customers of the CSPs.
- A SOC 2 report proves that a CSP complies with the requirements of the catalog.

SOC 2+ Privacy

- A SOC 2 report for privacy is based on AICPA SSAE 18 standard and Trust Services Criteria.
- SOC 2 may be applied selectively for specific privacy mandates as “additional subject matter” in the scope of the engagement.



Why SOC 2 reports for privacy?

SOC 2 reporting helps you in providing much needed assurance for compliance with privacy. AICPA has developed a Privacy Maturity Model which can help organizations to ascertain their level of maturity for privacy. With more stringent regulations and enforcement privacy issues are more in focus for organizations.



Advantages

A

- End to end process for SOC Reporting Attest Services
- Project management methodology consistently applied to each engagement

B

- Efficient service delivery with minimal disruption to operations
- Our engagements are executed by senior experienced professionals

C

- 15 years of Information Security & Cyber Security experience
- Reduced time to complete assignments

D

- Licensed CPA firm listed with PCAOB and Cloud Security Alliance
- Prompt services with engagements completed in record time

E

- Ongoing support. We are with you whenever you need us

Our Value Proposition

Knowing how much extra value and assurance a privacy assessment can deliver, many clients find that it makes sense to take steps to ensure a more successful outcome, including hiring experts who are skilled in helping organizations be more thorough and thoughtful in how they approach their engagement. Preparing for a privacy assessment engagement is a matter of clear thinking and smart planning. Working with a cyber security specialist such as ours, helps you dig into areas such as cloud security, data security, privacy, incident response, and much more.





Thank you.

We look forward to the opportunity of working with you.

Accedere

© 2019 Accedere Inc
All Rights Reserved.

accedere.io