Legal, Risk, and Compliance for CCSP®

Cloud Privacy and Legal Issues

Dr. Lyron H. Andrews
CISSP/CCSP/SSCP/CRISC/CISM/CCSK

https://www.profabula.com/whyprofabula

CCSP Certification Examination

Domains	Weights
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance 13%	13%

Overview

- Describe common legal terms despite jurisdiction differences
- Review the implications of data privacy in the cloud
- Delineate roles and responsibilities of protecting the subject's data

Common Legal Definitions

Basic Legal Terms

Warrant

Subpoena

Extradition

Jurisdiction

Law vs. Regulation

Laws apply to all citizens and visitors

Regulations are industry and or practice specific

Legal Issues in the Cloud

Local

Regional

Global

Global Legal Organizations

International Court of Justice

Interpol

Regional Concerns in the Cloud

Harmonization of law

Mutual legal assistance treaty

Local Legal Issues

Municipal laws

Local laws

Township laws

Ordinances

Commonwealth statues

General rules of incorporation

Major Focus of Legal Impact

Tort - preponderance of negligence and damage

Criminal - graduated and various losses with guilt

Understand Jurisdictional Differences in Data Privacy

International Privacy History

1970 German Data Protection Act

1980 OECD

1995 EU Data Protection Directive

2016 GDPR

1970 German Data Protection Act

First enacted in a state

Later adopted into federal law

1980 OECD

Collection Limitation Principle

Data Quality Principle

Purpose Specification Principle

Use Limitation Principle

1980 OECD

Security Safeguards Principle

Openness Principle

Individual Participation Principle

Accountability Principle

1995 EU Data Protection Directive (95/46/EC)

Individuals' rights on collection and use

Single market dimension

Police and criminal justice integration

Protection on data transfer outside of EU

2016 GDPR

Harmonize data privacy laws throughout Europe

Protect EU citizens data

Additional protections

Countries that adhere to GDPR outside of EU

Countries that don’t have adherence

Enumerate Country-specific Legislation

Law

ARGENTINA

Change country

Article 43 of the Federal Constitution, third paragraph, provides, in relevant part that any person may file an action to have access to personal data about such person and to information about the purpose with which they are kept, included in public data registries or banks, or in private data registries or banks, and to request the suppression, correction, confidentiality or updating of the data where inaccurate or discriminatory.

These provisions do not create an express constitutional right to privacy or data protection, but do create the basic framework for the protection of such right, as well as the foundation for the legislation, subsequently enacted, which regulates the details of that protection.

Law 25,326 - the Personal Data Protection Law (PDPL) includes the basic personal data rules. It follows international standards, and has been considered as granting adequate protection by the European Commission. Decree 1558 of 2001 includes regulations issued under the PDPL. Further regulations have been issued by the relevant agencies.

BELGIUM

Change country

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes

African Personal Data Protection

- **Choice and consent**
- **Data security**
- **Data retention and destruction**
- **Registration with a data protection authority (DPA)**
- **Cross-border data transfers**
- **Personal data breach notification**
- **Appointment of a data protection officer (DPO)**

Asia–Pacific Economic Cooperation (APEC) Privacy Framework

Aim of greater regional prosperity

Implementation of APEC Cross-Border Privacy Rules (CBPR)

Certified by accountability agent

Australia and New Zealand Privacy Principles

EU styled privacy principles mandating protection of sensitive data

Regulates collection, storage, security, processing and disclosure

Revised privacy principles in 2014

EU–U.S. Privacy Shield

Strong data protection obligations on companies receiving personal data from the EU

Safeguards on U.S. government access to data

Effective protection and redress for individuals

An annual joint review by EU and U.S. to monitor the correct application of the arrangement

Maintaining Legal and Regulated Privacy

Generally Accepted Privacy Principles (GAPP)

Management

Notice

Choice and consent

Collection

Use, retention, and disposal

Generally Accepted Privacy Principles (GAPP)

Access

Disclosure

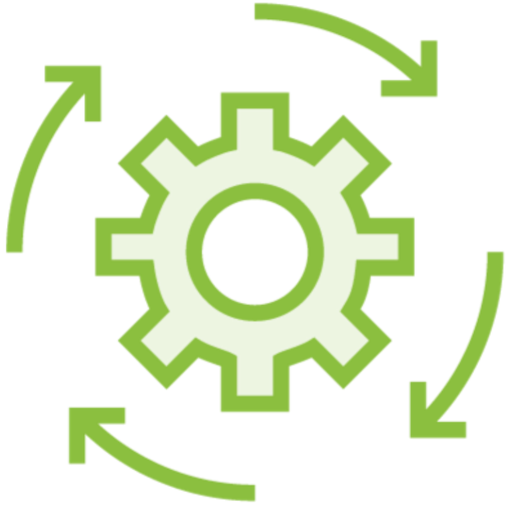
Security for privacy

Quality

Monitoring and enforcement

General Data Privacy Concerns

Where is the location?



What is the practice?

Who is involved?

Data Privacy Primary Roles

Data Subject

Data Controller

Data Processor

Data Custodian

Data Steward

Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds ISO27018:2019

Consent

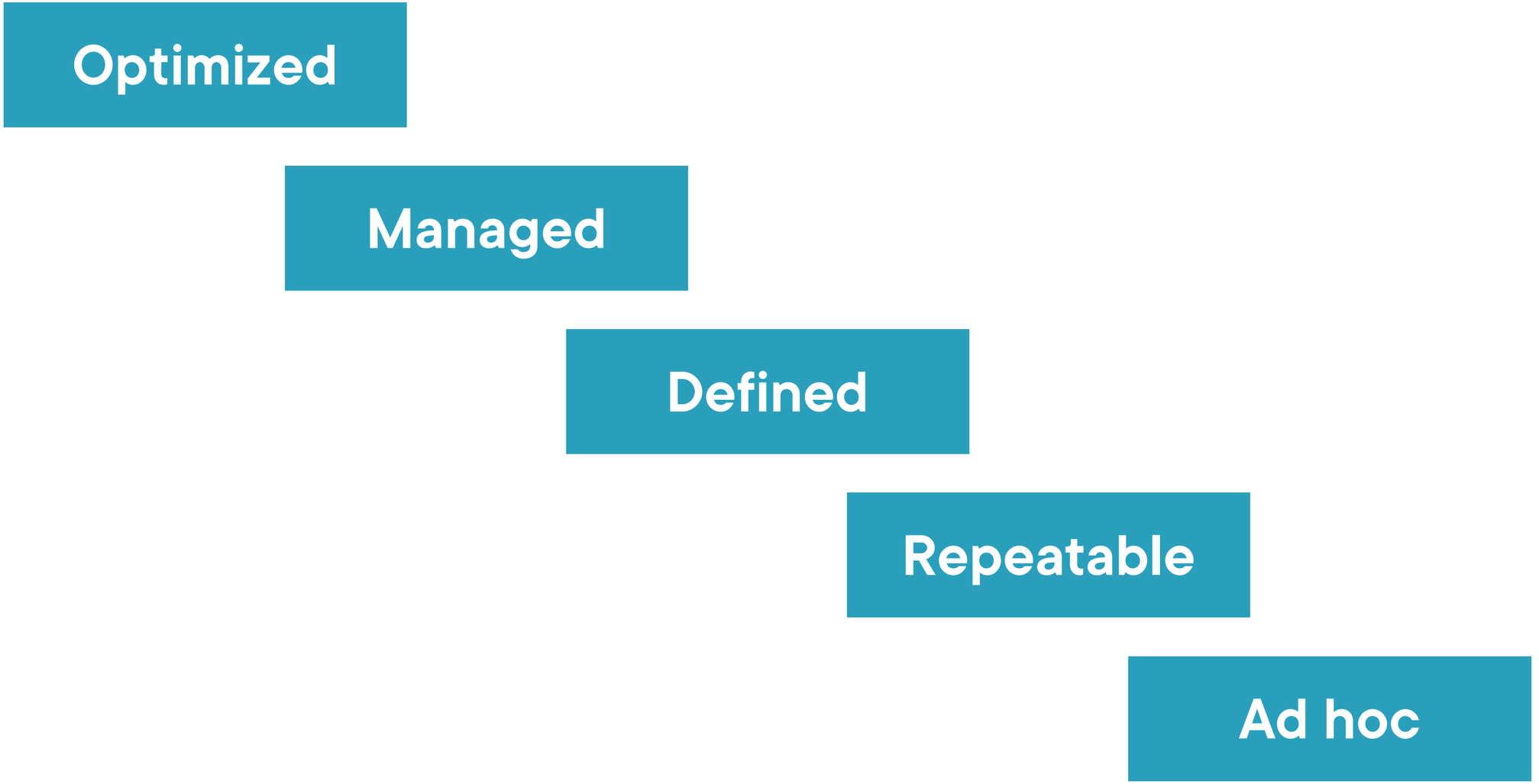
Control

Transparency

Communication

Independent annual audit

Privacy Maturity Model



Summary

What regulatory practices are relevant for your cloud consumption?

What are the legal regimes that affect your cloud consumption?

How do the roles and responsibilities of data privacy affect your strategy?

Up Next:
Organizational and Cloud Risk Management