

Economic and Social Commission for Western Asia

# Best Practices for Protecting Personal Data

## A GRC Perspective

Workshop on Building Trust in Digital Government Services, Beirut, 11-12 September 2023



Shared Prosperity Dignified Life



Internet  
Society





## Adel Abdel Moneim

### Cybersecurity & GRC Expert

Head of Information Security Workgroup – Egyptian CIT

Registered cybersecurity Expert – ITU-ARCC

Globally recognized cybersecurity influencer (IFSEC 2019 , 2020 & 2021)

Certified Trainer ISC2 , PECB , EC-COUNCIL , ISACA , APMG & CertNexus

25 years experience in cybersecurity fields as a Consultant / Trainer / Auditor

CISSP , ISSEP , ISSMP , ISSAP , CIPP-E , CIPM , CIPT , CISA , CISM , CRISC , CGEIT CDPSE  
CCISO , CGRC , HCISPP , Master ISO 27001/27701, CCSP , CSSLP , NCSP , TOGAF, COBIT ,  
SABSA-CSF , IoTSP , PECB MS Auditor

# Agenda

- Data Security vs Data privacy
- PIMS ( Privacy Information Management System)
- Introduction to PET ( privacy enhancing technologies)
- Privacy challenges (Banking sector example)
- Exploring Privacy Global best practices Samples from Arab world



Shared Prosperity **Dignified Life**



# Data Security vs Data privacy

# Differentiating between Data privacy and Data Security

- ***Data privacy*** is the right of individuals to control how their personal data is collected, Stored ,used, and shared. It is about giving people the power to decide who has access to their data and how it is used.
- ***Data security*** is the protection of data from unauthorized access, use, disclosure, disruption, modification, or destruction. It is about keeping data safe from malicious threats.

# Data life Cycle



# Differentiating between: DPIA and PIA

- ***DPIA*** stands for Data Protection Impact Assessment. It is a process that organizations must follow under the General Data Protection Regulation (GDPR) to identify and mitigate the risks associated with processing personal data.
- ***PIA*** stands for Privacy Impact Assessment. It could refer to any assessment of the privacy implications of a project or activity. It ensures and enable privacy by design in an organization

# Privacy By Design

## key principles

- Proactive not reactive, preventative not remedial
- Privacy as a default setting
- Privacy embedded into design
- End-to-end security – full lifecycle protection
- Visibility and transparency

## Examples of technical and organizational measures include:

- Minimizing personal data processing.
- Minimizing personal data Collection.
- Anonymizing personal data.
- Ensuring transparency through policies.
- Implementing security safeguards



# The key differences between DPIA and PIA

<b>Features</b>	<b>DPIA</b>	<b>PIA</b>
purpose	To identify and mitigate the risks associated with processing personal data under the GDPR	To assess the privacy implications of a project or activity
Legal requirement	Required under the GDPR	Not required under any specific law, but may be required by other regulations or best practices
Scope	Specific to the processing of personal data	Broader and can apply to any project or activity that may impact privacy
Methodology	Structured and systematic approach	More flexible and can be tailored to the specific project or activity
Output	Document that identifies and mitigates the risks	Document that assesses the privacy implications of the project or activity



Shared Prosperity **Dignified Life**



# PIMS

## ( Privacy Information Management System)

# Definition of (PIMS) ISO/IEC 27701

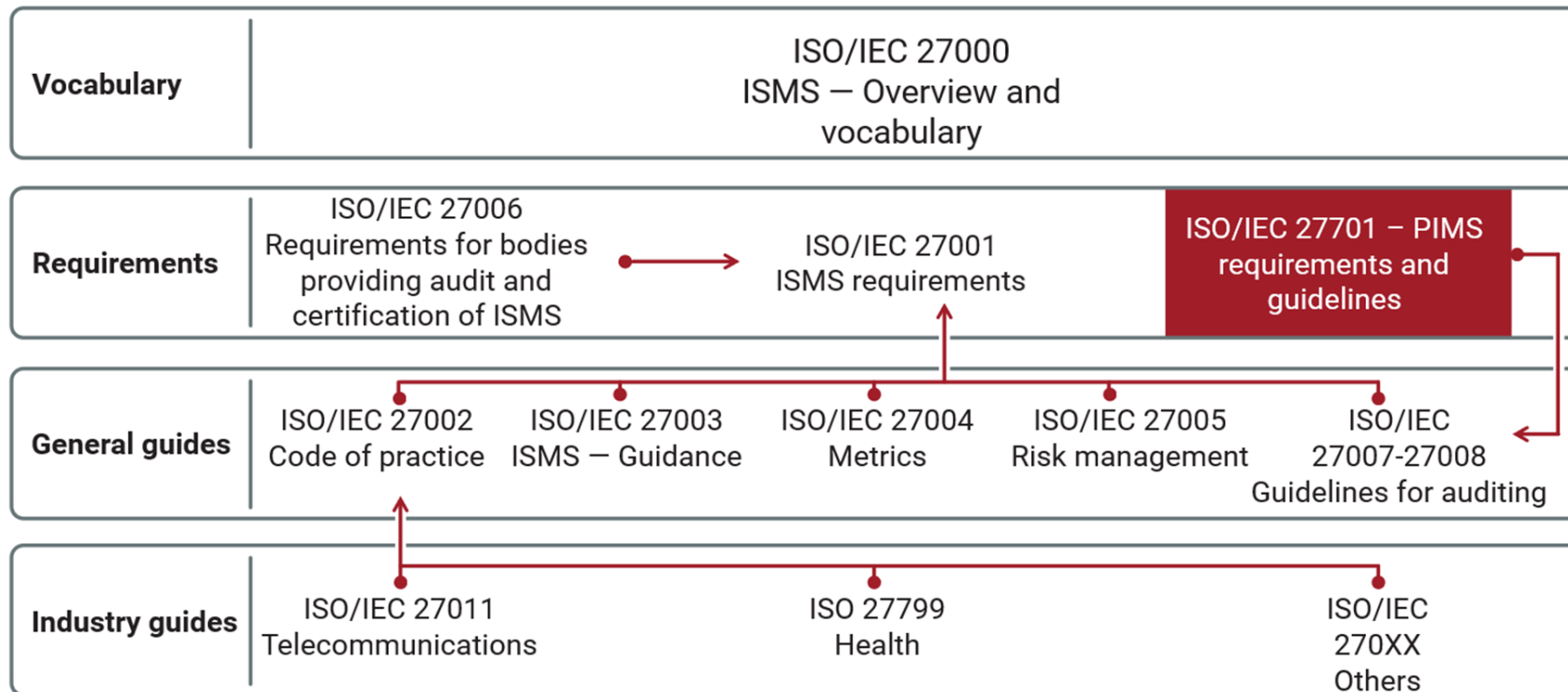
Information security management system which addresses the protection of privacy as potentially affected by the processing of PII The privacy information management system (PIMS) is a system which makes it easier for organizations to control and manage people's personal data and their online identity by permitting them to allow, deny, or withdraw consent to third parties

# Definition of Management System

ISO defines a management system as a set of interrelated or interacting elements of an organization to establish policies and objectives, as well as the processes to achieve those objectives. Continuous improvement is central to a management system, the so called PDCA cycle

# PIMS relation with ISMS & other security standards

## The ISO/IEC 27000 Family



# The Structure of ISO 27701 Standard

Clause # 5 PIMS-specific requirements related to ISO/IEC 27001

Clause # 6 PIMS-specific guidance related to ISO/IEC 27002

Clause # 7 Additional ISO/IEC 27002 guidance for PII controllers

Clause # 8 Additional ISO/IEC 27002 guidance for PII processors

# ISO 27701 Standard - Annexes

- A- PIMS-specific reference control objectives and controls (PII Controllers)
- B- PIMS-specific reference control objectives and controls (PII Processors)
- C- Mapping to ISO/IEC 29100
- D- Mapping to the General Data Protection Regulation
- E- Mapping to ISO/IEC 27018 and ISO/IEC 29151
- F- How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

# PIMS specific Guidance related to ISO 27002

<b>6.2</b>	<i>Information security policies</i>	<b>6.9</b>	<i>Operations security</i>
<b>6.3</b>	<i>Organization of information security</i>	<b>6.10</b>	<i>Communications security</i>
<b>6.4</b>	<i>Human resource security</i>	<b>6.11</b>	<i>System acquisition, development and maintenance</i>
<b>6.5</b>	<i>Asset management</i>	<b>6.12</b>	<i>Supplier relationships</i>
<b>6.6</b>	<i>Access control</i>	<b>6.13</b>	<i>Information security incident management</i>
<b>6.7</b>	<i>Cryptography</i>	<b>6.14</b>	<i>Information security aspects of business continuity management</i>
<b>6.8</b>	<i>Physical and environmental security</i>	<b>6.15</b>	<i>Compliance</i>





Shared Prosperity **Dignified Life**



# PET Privacy Enhancing Technologies

## EMERGING PRIVACY ENHANCING TECHNOLOGIES

CURRENT REGULATORY AND  
POLICY APPROACHES

OECD DIGITAL ECONOMY  
PAPERS

March 2023 No. 351



## Privacy Enhancing Technologies

These are technologies that are designed to protect privacy while still allowing for the collection, processing, and use of personal data.

PETs can be used to protect personal data at different stages of its lifecycle, from collection to storage to us

Types of PETs	Key technologies	Current and potential applications*	Challenges and limitations
<b>Data obfuscation tools</b>	Anonymisation / Pseudonymisation	Secure storage	- Ensuring that information does not leak (risk of re-identification)
	Synthetic data	Privacy-preserving machine learning	- Amplified bias in particular for synthetic data
	Differential privacy	Expanding research opportunities	- Insufficient skills and competences
	Zero-knowledge proofs	Verifying information without requiring disclosure (e.g. age verification)	- Applications are still in their early stages
<b>Encrypted data processing tools</b>	Homomorphic encryption	Computing on encrypted data within the same organisation	- Data cleaning challenges
	Multi-party computation (including orivate set intersection)	Computing on private data that is too sensitive to disclose Contact tracing / discovery	- Ensuring that information does not leak - Higher computation costs
	Trusted execution environments	Computing using models that need to remain private	- Higher computation costs - Digital security challenges
<b>Federated and distributed analytics</b>	Federated learning	Privacy-preserving machine learning	- Reliable connectivity needed - Information on data models need to be made available to data processor
	Distributed analytics		
<b>Data accountability tools</b>	Accountable systems	Setting and enforcing rules regarding when data can be accessed Immutable tracking of data access by data controllers	- Narrow use cases and lack stand-alone applications - Configuration complexity - Privacy and data protection compliance risks where distributed ledger technologies are used
	Threshold secret sharing		
	Personal data stores / Personal Information Management Systems	Providing data subjects control over their own data	- Digital security challenges - Not considered as PETs in the strict sense

# PETs Sample Technologies

- ***Data anonymization***: This involves removing or altering personal identifiers from data so that it cannot be linked back to an individual.
- ***Cryptography***: This involves using mathematical techniques to encrypt data so that it can only be read by authorized users.

# PETs Sample Technologies

- ***Pseudonymization***: This is the process of replacing personal identifiers with artificial identifiers so that the data cannot be linked back to an individual.
- ***Differential privacy***: This is a technique that adds noise to data so that it becomes more difficult to identify individuals.
- **Secure multi-party computation**: This involves allowing multiple parties to jointly compute a function on their data without revealing their individual data to each other.

# Challenges associated with PETs

- **Performance:** PETs can often reduce the accuracy or utility of data, which can make them less appealing to businesses and organizations.
- **Complexity:** PETs can be complex to implement and use, which can be a barrier to adoption.
- **Regulation:** There is no clear regulatory framework for PETs, which can make it difficult for businesses and organizations to know how to use them compliantly.



Shared Prosperity **Dignified Life**



# Privacy Challenges







Shared Prosperity **Dignified Life**



# Privacy challenges (Banking sector example)

# Privacy Compliancy Challenge in banking sector

26 JUL 2023 • 7 MIN READ • IN [USE CASES](#)

## 5 Critical KYC Challenges For Identity Verification and How to Overcome Them



**Henry Patishman**  
Executive VP, Identity Verification solutions at Regula



**Emily Andrews**  
27 February 2020


Categories  
[Customer Experience](#), [Search Marketing](#)

Share:




## Consumer Data Privacy and KYC: The Clash of Compliance Titans?

# Privacy Compliancy Challenge in banking sector



**CPO**  
MAGAZINE


HOME NEWS INSIGHTS RESOURCES



DATA PRIVACY INSIGHTS · 3 MIN READ


## For Banks, Data Privacy and Anti-Money Laundering Don't Have to Be Incompatible

RINA SHAINSKI · NOVEMBER 20, 2019



Apr 20, 2020

## Selfie-based identification solutions are not KYC/AML compliant



**Identification solutions** that allow customer identification by taking pictures of ID documents and selfies of the user's face **do not comply with regulations** about money laundering and terrorist financing (AML, Anti-Money Laundering), especially in the financial sector.

# Privacy Compliancy Challenge in banking sector

## KYC: Solving the Regulatory Challenges of Data Privacy

02 December 2016



5



4

0

Data Privacy regulations increase challenges for bank KYC and AML programs

<https://www.finextra.com/blogposting/13427/kyc-solving-the-regulatory-challenges-of-data-privacy>

<https://www.digitaldoughnut.com/articles/2020/february-2020/consumer-data-privacy-and-kyc-clash-of-compliance>

## How Artificial Intelligence is Revamping KYC and AML?



Oliver Smith [Follow](#)

Feb 24 · 3 min read



<https://www.corporatecomplianceinsights.com/5-ways-ai-is-impacting-aml-and-kyc-compliance/>

Getting Started | Adel Abdel Moneim ... | Sonic | Courses | Information ... | Home - eForensics | Google | ISACA | gmail | speedtest

[HOME](#) [ABOUT](#) [ARTICLES](#) [VENDOR NEWS](#) [JOBS](#) [EVENTS](#) [DOWNLOADS](#) [PODCASTS](#)

Home > Financial Services

## 5 Ways AI is Impacting AML and KYC Compliance

by [NIALL TWOMEY](#) — December 19, 2018 in [Financial Services](#), [Fraud](#)

# GDPR fines 2020

France fined **Google** €50,000,000 in January 2019 for a lack of transparency and consent in advertising personalization.

**British Airways** got a steep £183,000,000 fine from U.K. regulators because of inadequate cybersecurity arrangements. Hackers stole 500,000 customer records from the B.A. website in June 2019.

In the **U.S.**, the major **Equifax** data breach cost the company at least \$575 million in penalties and fines. They lost 150 million personal and financial records due to an unpatched database vulnerability.



## EU countries ranked by total GDPR fine amount in 2020 (from January 1, 2020 to August 17th, 2020)

Rank	Country	Total fine amount per country	Number of fines
1	Italy	€45,609,000	13
2	Sweden	€7,031,800	4
3	Netherlands	€2,080,000	3
4	Spain	€1,952,810	76
5	Germany	€1,240,000	1
6	Norway	€742,060	8
7	Belgium	€717,000	7
8	Hungary	€299,300	6
9	Finland	€200,500	4
10	Ireland	€115,000	2

# Cost of non compliance

## Top ten largest fines imposed to date under GDPR



#practicalglobalprivacy

# Cost of non compliance



20 biggest

[Products](#) [Services](#) [Pricing](#) [Resources](#) [Partners](#) [About](#)

[Request a demo](#)



## 1. Meta GDPR fine- €1.2 billion

In May 2023, in a groundbreaking decision within the past five years of GDPR enforcement, the **Irish Data Protection Commission (DPC)** imposed a historic fine of **€1.2 billion** on US tech giant Meta.

This **record-breaking** fine was issued for the transfer of personal data of European users to the United States without adequate data protection mechanisms and serves as a significant milestone in data protection regulation.

Meta, the parent company of popular platforms like **Instagram and WhatsApp**, has been penalized for failing to comply with the European Union's General Data Protection Regulation (GDPR) before, but this fine highly surpasses all other fines.

As Meta plans to appeal the decision, the outcome of this legal battle will have far-reaching implications, **shaping the future of data transfers** and privacy rights in the digital age.

This fine serves as a clear warning to other companies that the **GDPR's requirements must be taken seriously**, and non-compliance can result in severe financial consequences





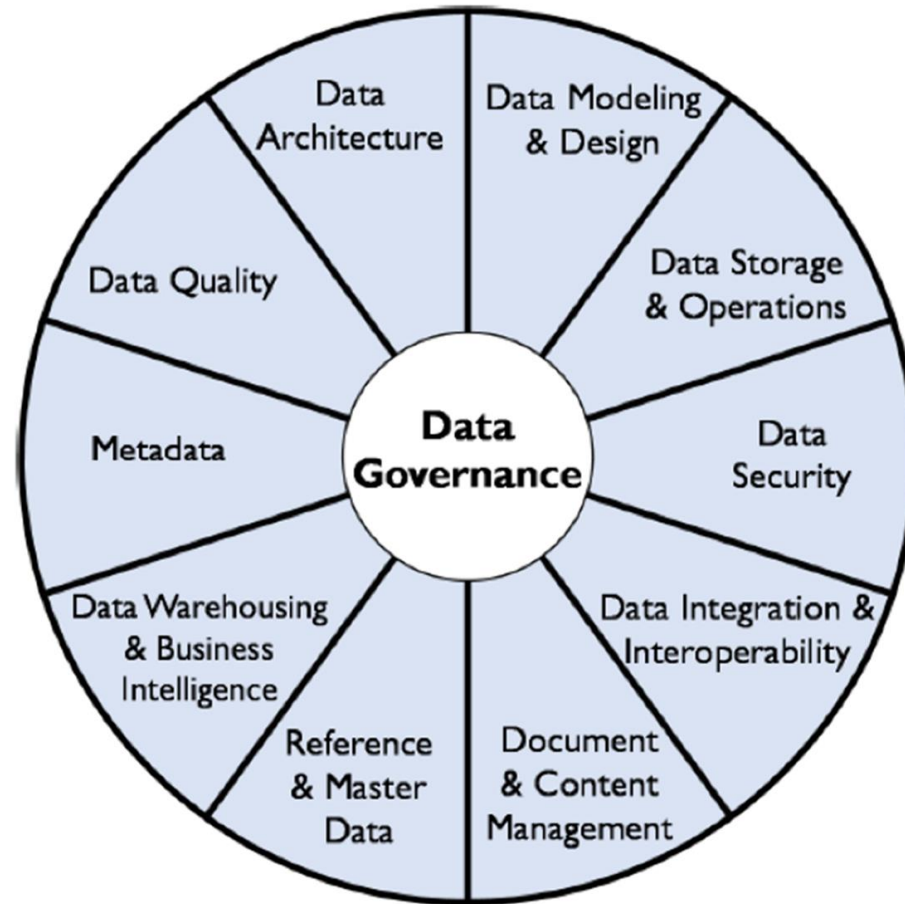
Shared Prosperity **Dignified Life**



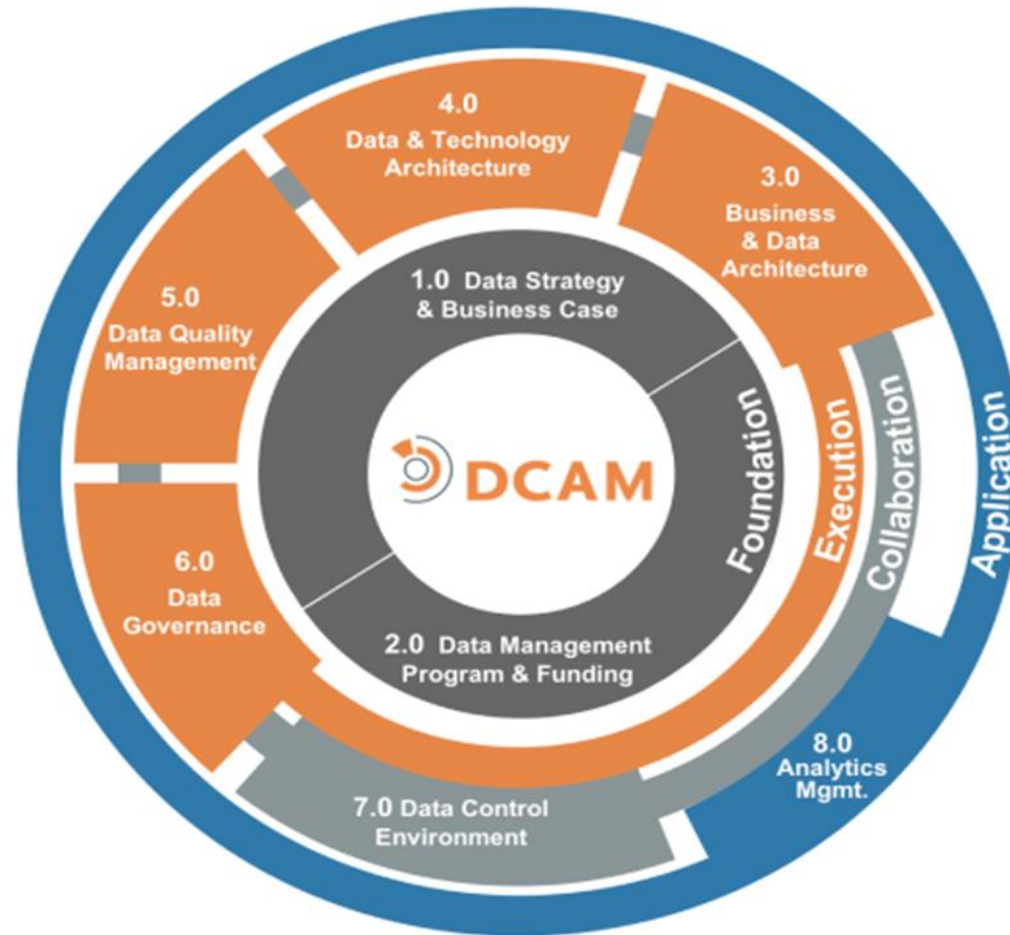
# Exploring Privacy Global best practices



# DAMA Data Management Framework



# DCAM- Data Management Capability Assessment Model



# NIST Privacy Framework

**IDENTIFY-P:** Develop the organizational understanding to manage privacy risks for individuals arising from data processing.

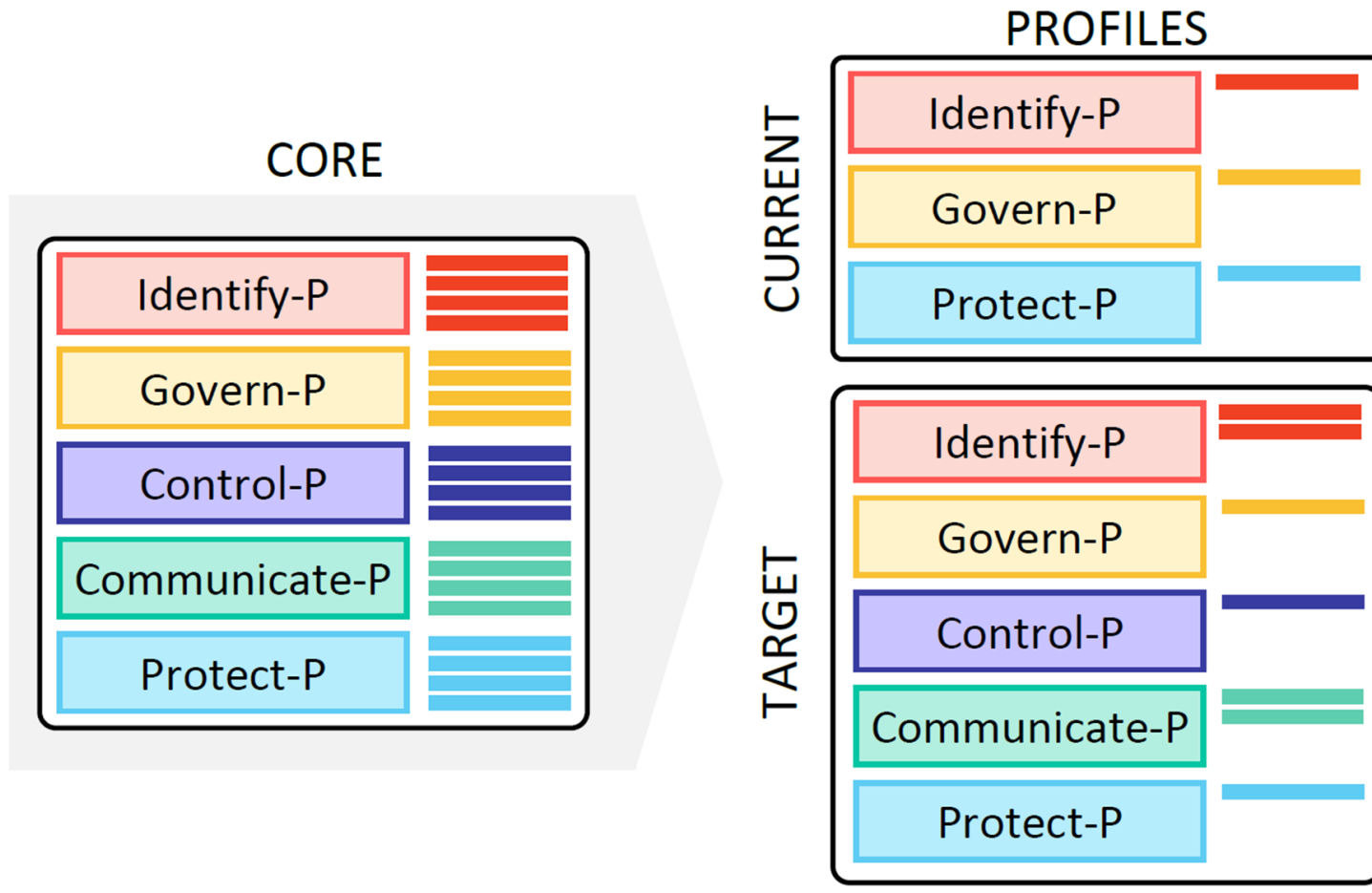
**GOVERN-P:** Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

**CONTROL-P:** Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

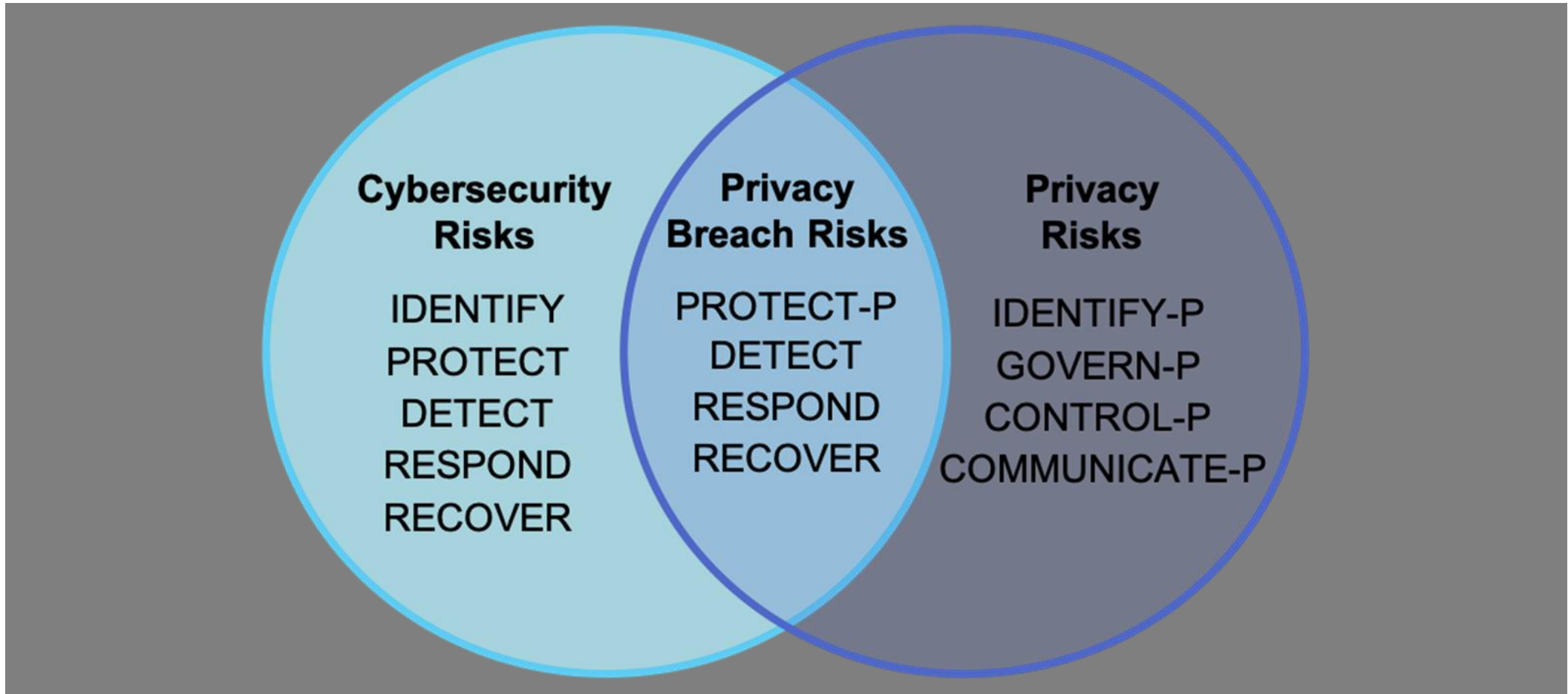
**COMMUNICATE-P:** Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

**PROTECT-P:** Develop and implement appropriate data processing safeguards

# NIST Privacy Framework

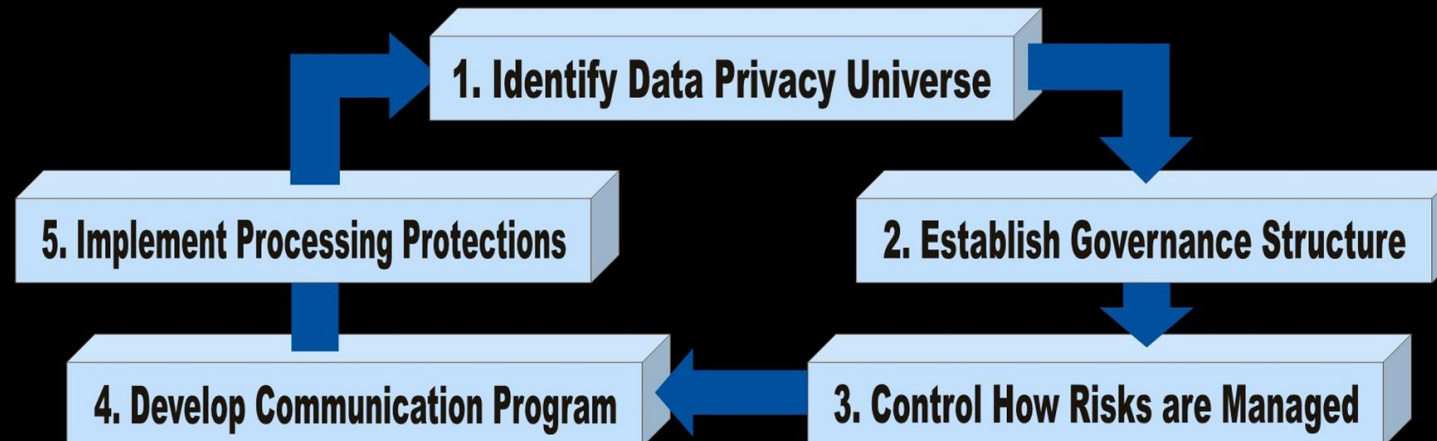


# NIST Privacy Framework



# NIST Privacy Framework

Use it to Manage your Organization's Privacy Risks

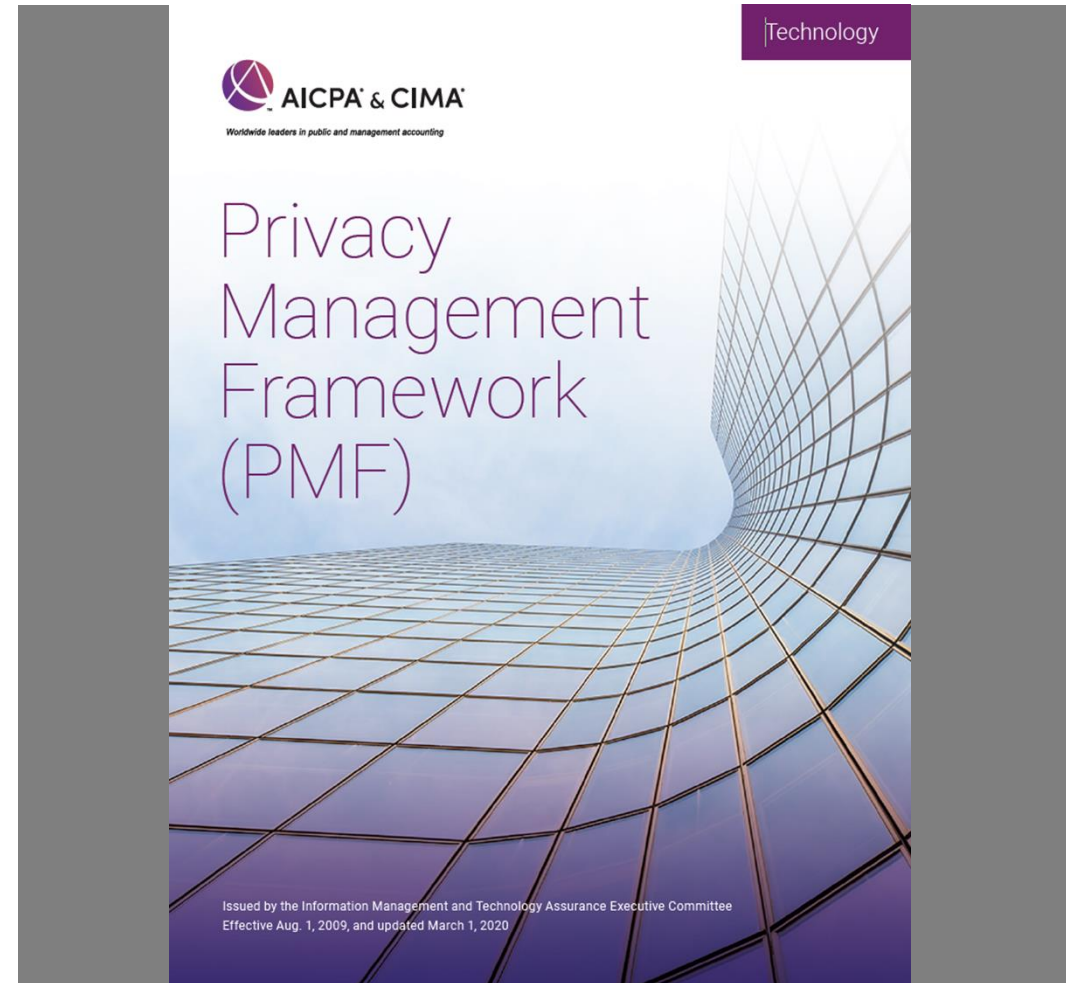


©2021 Praxiom Research Group Limited

<https://www.praxiom.com/nist-privacy.htm>



# Global Best Practices



# Global Best Practices



## NIST Special Publication NIST SP 800-50r1 ipd

### Building a Cybersecurity and Privacy Learning Program

Initial Public Draft

Marian Merritt  
*Applied Cybersecurity Division  
Information Technology Laboratory*

Susan Hansche  
*Cybersecurity and Infrastructure  
Security Agency  
Department of Homeland Security*

Brenda Ellis  
*National Aeronautics and Space  
Administration*

Kevin Sanchez-Cherry  
*Office of the Chief Information Officer  
Department of Transportation*

Julie Nethery Snyder  
*MITRE*

Donald Walden  
*Internal Revenue Service*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-50r1.ipd>

August 2023



U.S. Department of Commerce  
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology  
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*



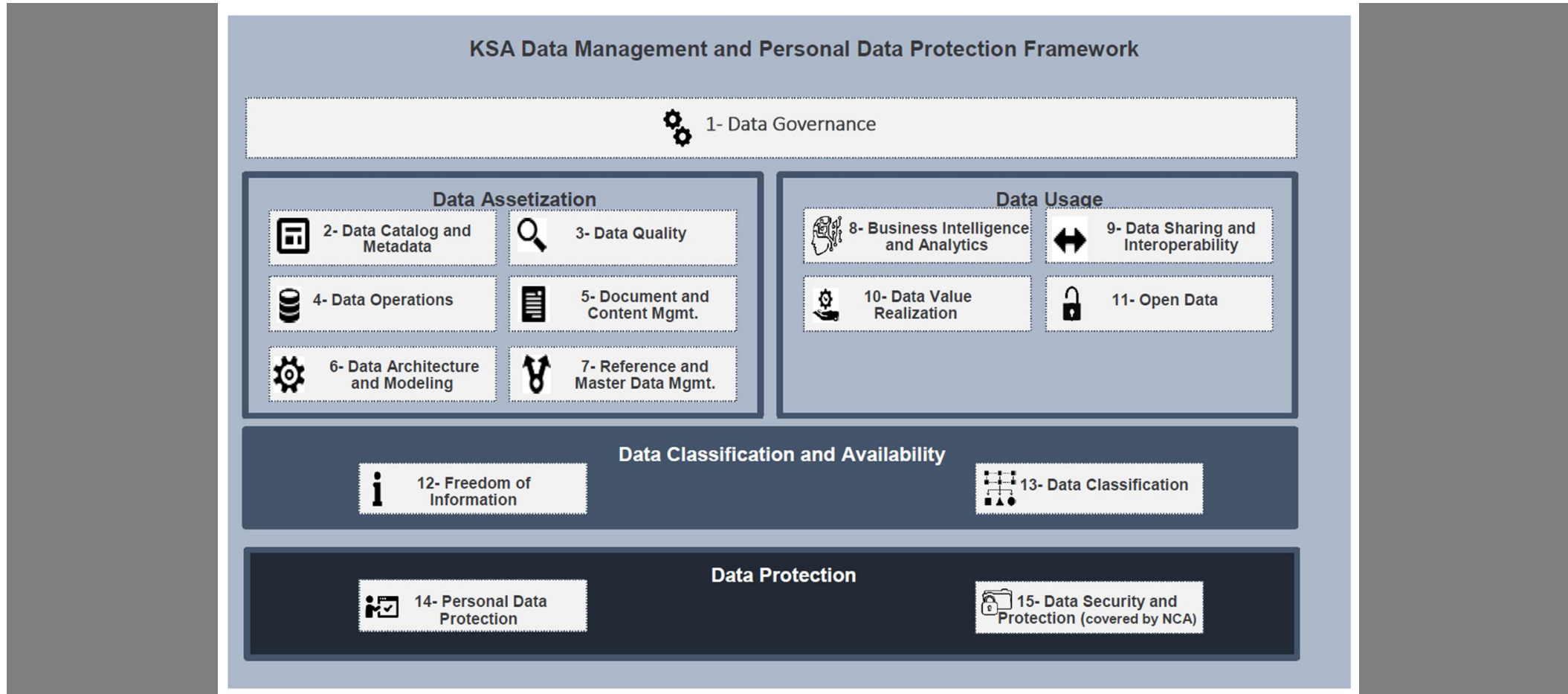


Shared Prosperity **Dignified Life**

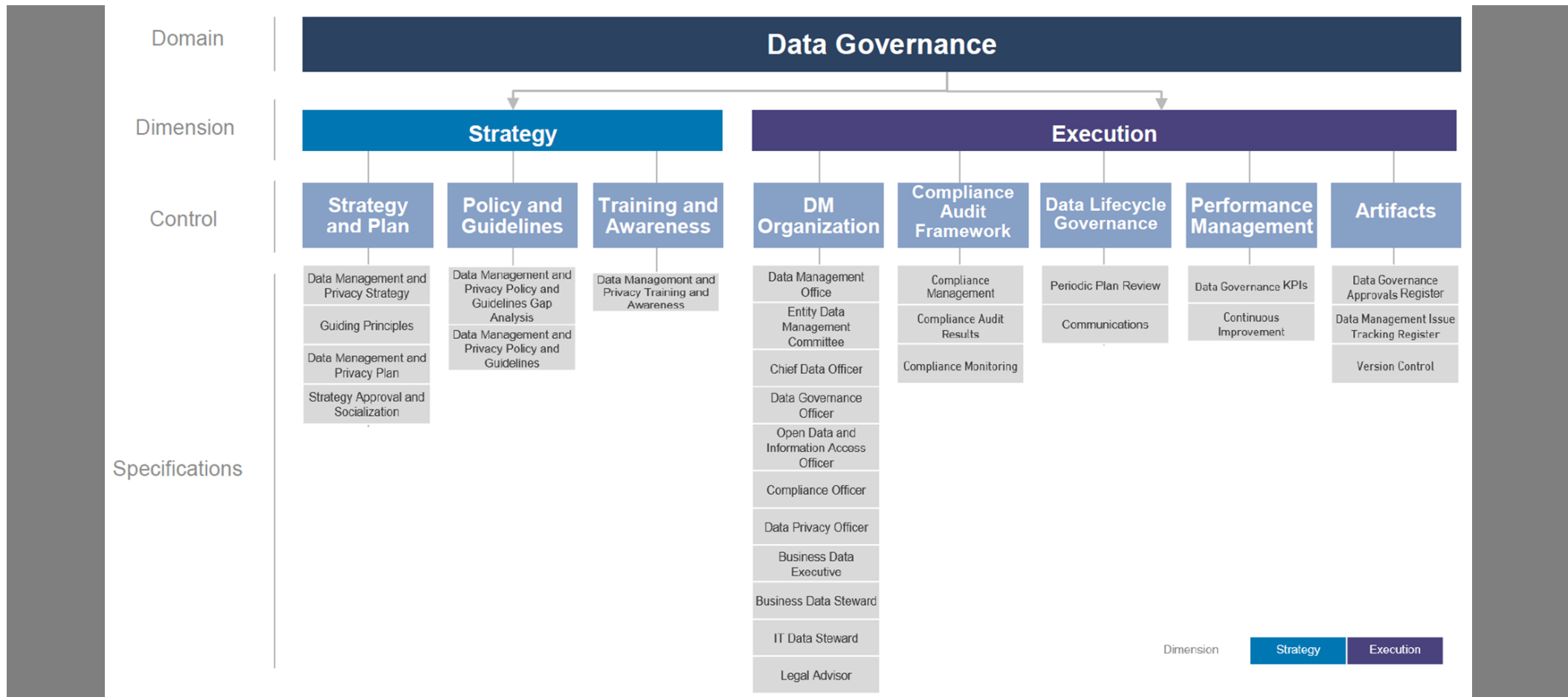


# Global best practices Samples from Arab world

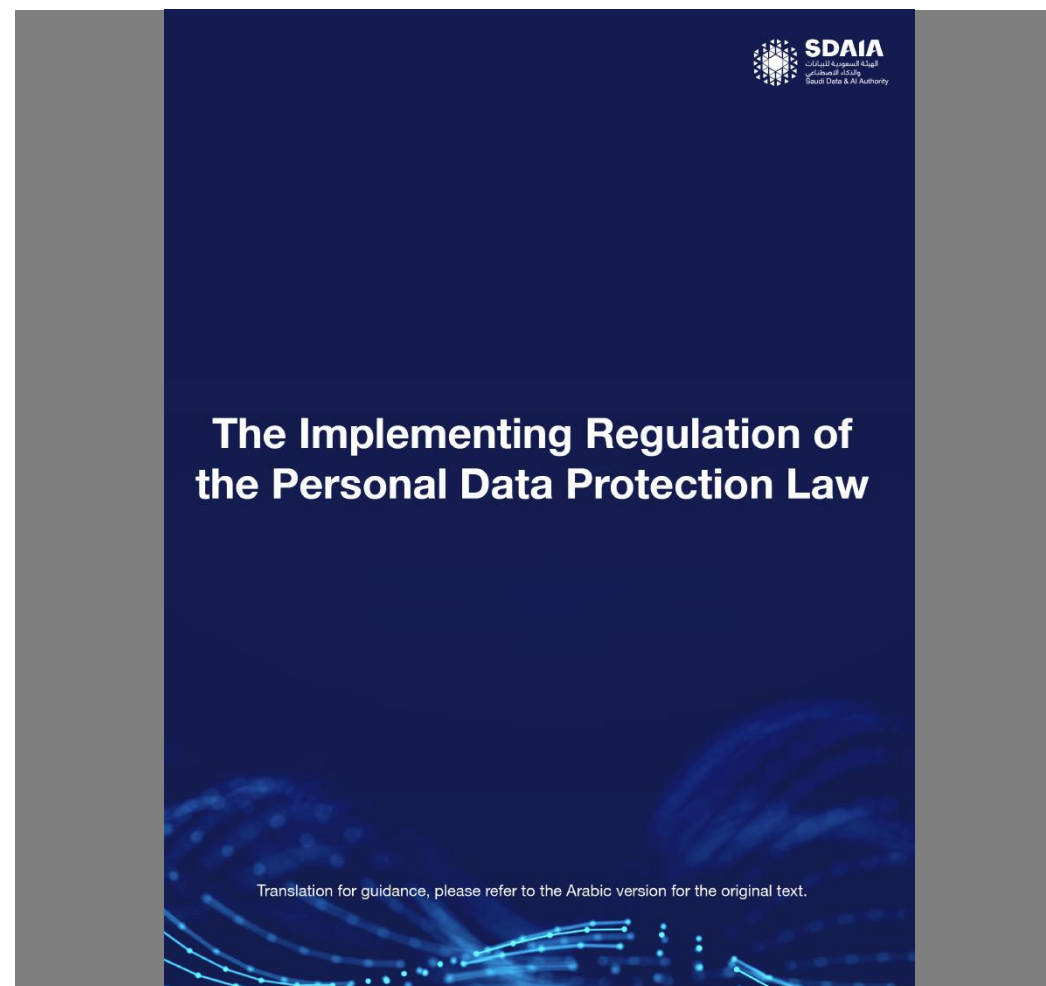
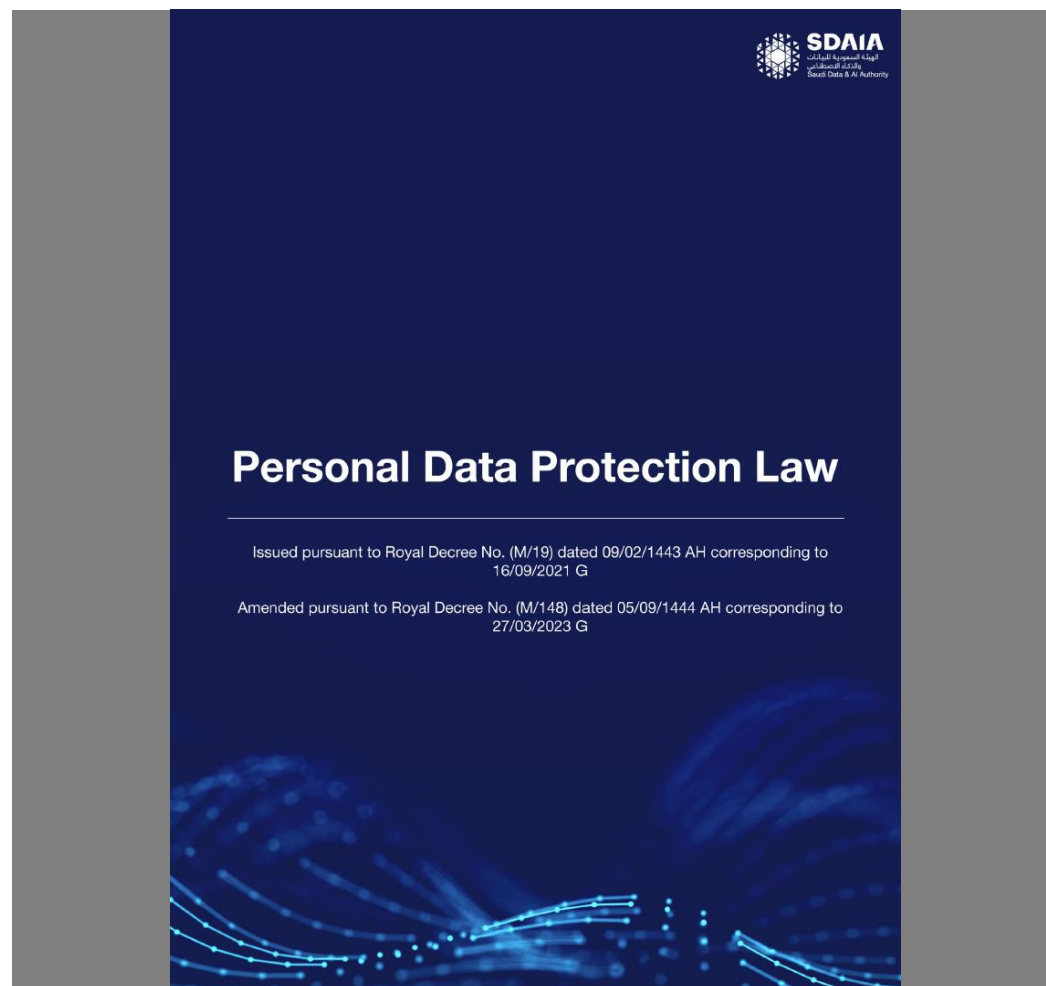
# KSA SDAIA Data Management & PDP Framework



# KSA SDAIA Data Management & PDP Framework



# KSA Personal Data Protection law & Implementation Regulation



# Egyptian Personal Data Protection law & Cyber Crime Law

الجريدة الرسمية - العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨ ٣

## قانون رقم ١٧٥ لسنة ٢٠١٨

في شأن مكافحة جرائم تقنية المعلومات

باسم الشعب

رئيس الجمهورية

قرر مجلس النواب القانون الآتي نصه ، وقد أصدرناه :

الباب الأول

الأحكام العامة

تعريفات

مادة (١)

في تطبيق أحكام هذا القانون ، يُقصد بالكلمات والعبارات التالية المعنى المبين

قرين كل منهما :

الجهاز : الجهاز القومى لتنظيم الاتصالات .

الوزير المختص : الوزير المعنى بشئون الاتصالات وتكنولوجيا المعلومات .

البيانات والمعلومات الإلكترونية : كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه ، بواسطة تقنية المعلومات ، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات ، وما فى حكمها .

بيانات شخصية : أى بيانات متعلقة بشخص طبيعى محدد أو يمكن تحديده ، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى .

بيانات حكومية : بيانات متعلقة بالدولة أو إحدى سلطاتها ، أو أجهزتها أو وحداتها ، أو الهيئات العامة ، أو الهيئات المستقلة أو الأجهزة الرقابية ، أو غيرها من الأشخاص الاعتبارية العامة وما فى حكمها ، والمتاحة على الشبكة المعلوماتية أو على أى نظام معلوماتى أو على حاسب أو ما فى حكمها .

الجريدة الرسمية - العدد ٢٨ مكرر (هـ) فى ١٥ يولية سنة ٢٠٢٠ ٢

## قانون رقم ١٥١ لسنة ٢٠٢٠

بإصدار قانون حماية البيانات الشخصية

باسم الشعب

رئيس الجمهورية

قرر مجلس النواب القانون الآتى نصه ، وقد أصدرناه :

( المادة الأولى )

يُعمل بأحكام هذا القانون والقانون المرافق فى شأن حماية البيانات الشخصية المعالجة إلكترونياً جزئياً أو كلياً لدى أى حائز أو متحكم أو معالج لها ، وذلك بالنسبة للأشخاص الطبيعيين .

( المادة الثانية )

تسرى أحكام هذا القانون والقانون المرافق له على كل من ارتكب إحدى الجرائم المنصوص عليها فى القانون المرافق متى كان الجانى من المصريين داخل الجمهورية أو خارجها ، أو كان من غير المصريين المقيمين داخل الجمهورية ، أو كان من غير المصريين خارج الجمهورية إذا كان الفعل معاقباً عليه فى الدولة التى وقع فيها تحت أى وصف قانونى وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية .

( المادة الثالثة )

لا تسرى أحكام القانون المرافق على ما يأتى :

١ - البيانات الشخصية التى يحتفظ بها الأشخاص الطبيعيين للغير ، ويتم معالجتها للاستخدام الشخصى .

٢ - البيانات الشخصية التى تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقاً لنص قانونى .

٣ - البيانات الشخصية التى تتم معالجتها حصراً للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة ، وألا تستخدم فى أى أغراض أخرى ، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام .



Shared Prosperity **Dignified Life**



## Workshop on Building Trust in Digital Government Services, Beirut, 11-12 September 2023