DATA PROTECTION

In a nutshell

DataConsulting

office@dataconsulting.ae

Presentation overview

01 | The Business Case 3

02 | What is Data Protection? 6

03 | Cost of Weak Data Protection 10

04 | Regulatory Consequences 14

05 | UAE Data Privacy Law 17

01

THE BUSINESS CASE

Data protection supports growth, earns trust and helps control costs.

Data protection supports growth and operations

Privacy helps the business expand, use its data and avoid preventable losses.



Enter new markets

Privacy compliance supports expansion into markets with stricter data protection requirements.

Launch data-based services

Customer and patient data can support new digital services and revenue opportunities under clear privacy rules.

Build reliable AI

Reliable AI needs accurate data. Privacy controls help keep personal data correct and up to date.

Lower operating costs

Clear ownership and standard workflows reduce repeated coordination when teams handle personal data.

Organisations report benefits beyond compliance

Survey evidence supports the business priorities and trust case.

Strengthen customer loyalty



95%

report stronger customer loyalty and trust from privacy investments.[1]

Cisco Data and Privacy Benchmark (2026)

Improve efficiency



95%

report operational efficiencies from privacy-related investments.[2]

Cisco Data and Privacy Benchmark (2026)

Reduce financial exposure



95%

report benefits in mitigating losses from data breaches.[2]

Cisco Data and Privacy Benchmark (2026)

Enable responsible innovation



96%

report greater agility and innovation from appropriate data controls.[2]

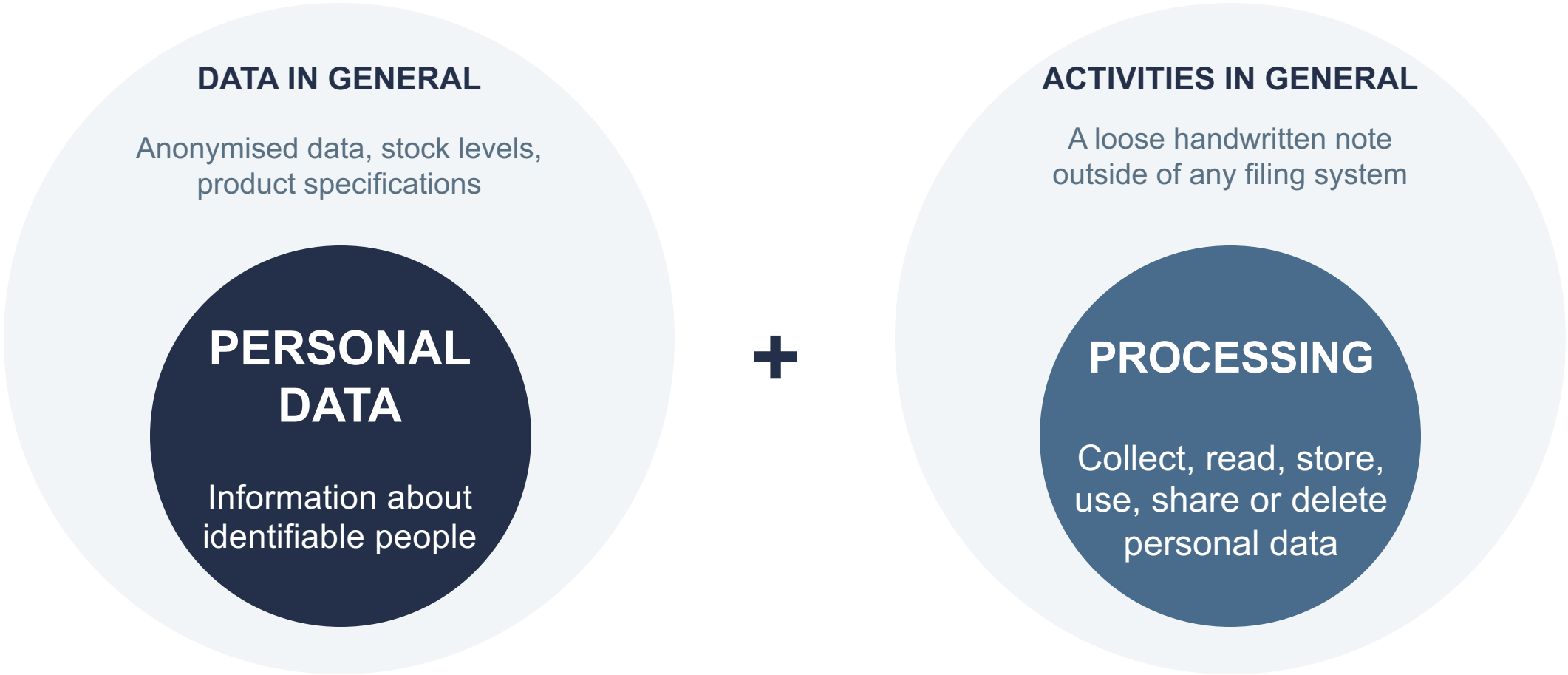
Cisco Data and Privacy Benchmark (2026)

02

WHAT IS DATA PROTECTION?

How organisations use personal data

Data Protection Scope



Personal Data

A person can be identified directly (e.g. name, unique ID) or indirectly by combining information (e.g. job title, employer name).

Identity

Name, ID number, date of birth

Contact

Email, phone, home address

Work

Salary, performance, attendance



Digital activity

IP address, device ID, location

Transactions

Purchases, payments, account history

Personal life

Health information, family details

What is Data Processing?

Processing covers every operation on personal data, throughout its lifecycle.

PERSONAL DATA

One customer.
One record.

Name
Contact details
Customer ID
Purchase history

EACH OPERATION COUNTS

01 **Collection**
Receive customer details

02 **Organisation**
Structure the customer record

03 **Use**
Use details to provide a service

04 **Modification**
Update a contact address

05 **Disclosure**
Share data with an authorised recipient

06 **Storage**
Save data in an approved system

07 **Retention**
Keep data for the defined period

08 **Deletion**
Remove data when no longer needed

03

COST OF WEAK DATA PROTECTION

Weak controls create incidents. Incidents create business costs.

One small error can reach the whole business

One data-handling error can create four types of business impact.

Legal exposure

Notification duties, claims or penalties.



Financial loss

Investigation, legal advice and recovery costs.

Lost trust

Customer complaints and reputational harm.

Operational disruption

Teams divert time to contain and fix the incident.

What makes up the cost of one data breach?

IBM sample of corporate incidents, including phishing and supply-chain compromises.

$8m[1]

AVERAGE PER BREACH

Average in IBM's sample of breached organisations. Not a cost estimate for one misdirected letter.

Minimum size or severity: not stated in the public release. Middle East, not UAE-only.



Lost business

$3.57m [1]

Disruption, lost revenue and customers leaving.

Post-breach response

$2.17m [1]

Legal support, helpdesks and support for affected people.

Detection & escalation

$1.90m [1]

Forensics, incident assessment and escalation to decision-makers.

Notification

$0.36m [1]

Informing affected people and relevant authorities.

1 IBM Middle East, 3 Aug 2026. All amounts are USD millions per breach. Study period: Mar 2025–Feb 2026. URLs and limitations in notes.

Governance can help reduce breach costs

The clearest evidence concerns response preparation, supported by clear ownership.

$1.49m[1]

LOWER AVERAGE COST PER BREACH

Organisations with extensive incident-response planning and testing had lower costs.

IBM 2023 global study
553 breached organisations

1 IBM / Ponemon, Cost of a Data Breach 2023. Planning and testing comparison. Full source and interpretation in notes.

What governance puts in place

01 Clear incident ownership

A named lead can activate the response.

02 A tested response plan

Teams know the decisions and escalation route.

03 Regular exercises

Teams practise before a real incident.

Observed study association. It does not establish a guaranteed saving from data governance or a percentage of the $8m Middle East mean.

04

REGULATORY CONSEQUENCES

Fines can follow a breach, or a missed compliance duty.

Big failures. Extraordinary consequences

Serious failures bring larger penalties and corrective action.

EU / GDPR

Meta Platforms

Ireland / 2023

EUR 1.2bn

Unlawful EU-to-US data transfers. The regulator also ordered suspension and corrective action.

Irish DPC

EU / GDPR

Uber

Netherlands / 2026

EUR 824.99m

Automated driver deactivations without the required human assessment.

Dutch AP

EU / GDPR

TikTok

Ireland / 2025

EUR 530m

Transfers to China without adequate safeguards, and insufficient transparency.

Irish DPC

UAE / ADGM

Okadoc

Abu Dhabi / 2024

USD 20,000

Failures in handling an access request, privacy procedures and regulator cooperation.

ADGM

DIFC FINES

510 published fine decisions across 2023–2025. DIFC only.



2023	2024	2025
173	64	273

Missed compliance duties can trigger fines, even without a data breach.

Examples cited by the DIFC regulator

- Privacy notification not renewed
- Annual assessment not completed*
- Investigation request unanswered

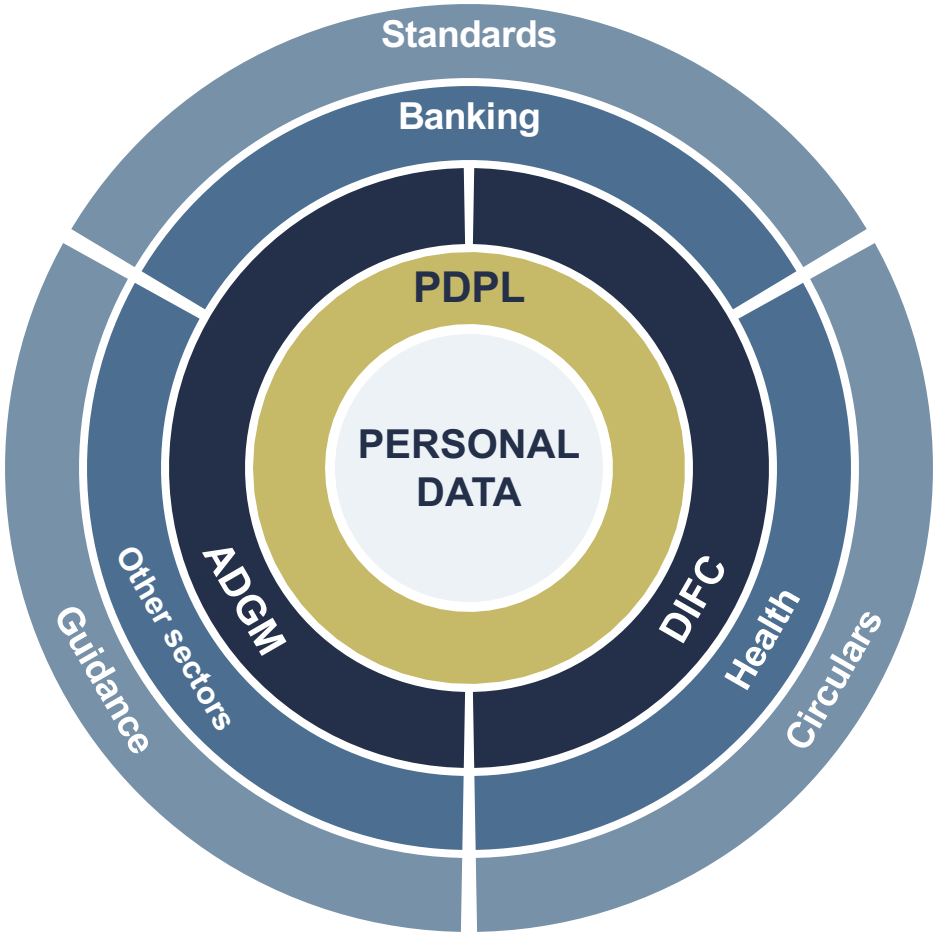
05

UAE DATA PRIVACY LAW

Local requirements and European standards

UAE privacy obligations come in several layers

The programme needs to bring the applicable UAE rules together.



Rings organise the assessment, not legal rank.

01 **Federal privacy law**

PDPL is the general UAE regime,
with exclusions for certain entities and data.

02 **Special Free Zone regimes***

DIFC and ADGM apply separate privacy laws
where federal PDPL excludes those companies.

03 **Industry rules**

Banking consumer data rules.
Health information and other sector laws.

04 **Regulatory detail**

CBUAE Consumer Protection Standards: binding
ADGM Circular 1/2025: keep the register current
ADGM DPIA Guidance Part 4: explanatory

GDPR is already a reference for UAE privacy

GDPR methods offer a starting point. The applicable UAE law still determines the duties.

01 Legal design

ADGM: closely based on GDPR (2021).
DIFC: consistent with EU rules (2020).
PDPL: similar principles and rights.

02 European guidance

ADGM uses European guidance to explain its own law in practice, for example how to assess privacy risks.

03 Regulator cooperation

Global Privacy Enforcement Network.
ADGM (Abu Dhabi): joined March 2018.
Also includes DIFC, Ireland and France.

04 Reusable transfer tools

ADGM’s EU contract-clause addendum has been available since November 2023.
It reduces duplicated transfer paperwork.

06

WHO WE ARE

Join our DataClub

DataConsulting

office@dataconsulting.ae