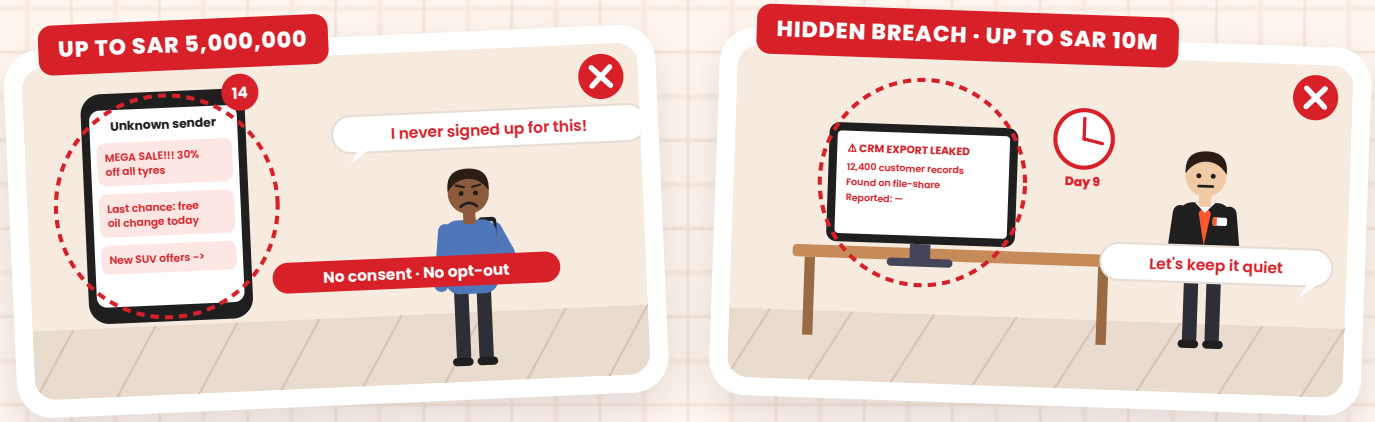
• CRITICAL EXPOSURE Automotive dealerships, workshops & distributors

PDPL Compliance Guidebook for Automotive Companies

The Personal Data Protection Law, standard by standard: what SDAIA checks, what good looks like, **and what each gap can cost your dealership.**



SAR 5M
maximum fine for **any single violation** of the PDPL or its regulations.

SAR 10M
ceiling when the **same violation is repeated**. The fine doubles.

2 years
in prison, plus up to SAR 3M, for **disclosing sensitive data** to cause harm or for gain.

12 standards · 29 checkpoints · Right way / wrong way · Real enforcement cases · Ideal fix time

14 Sep 2024 grace period ended → **16 Jan 2026** 48 violation decisions → **The next decision could carry your dealership's name.**

WHY THIS GUIDEBOOK EXISTS

Every customer you serve leaves personal data behind.

A dealership collects more personal data than most businesses: national IDs and licences for test drives, salaries for finance, phone numbers for every service booking. Since **14 September 2024**, when the PDPL grace period ended, every one of those records can be inspected by SDAIA, and every gap can be priced at **up to SAR 5 million**.

This guidebook turns the PDPL audit checklist into a **shared picture of what good looks like, and what failure costs**, so the people who audit and the people being audited work from the same page.

01

Know exactly what SDAIA checks

Each of the 12 PDPL standards is set out with the article of the law it comes from, so nobody can say they didn't know.

02

See the price of every gap

Every page shows the maximum fine, what else can happen, and a real enforcement case. Compliance becomes a business decision, not a nice-to-have.

03

Fix it before they find it

Each standard has an ideal fix time, so the riskiest gaps are closed first: some before the end of the shift.

04

Evidence you can show

Clear evidence rules mean that when SDAIA asks "prove it", the proof is already in the file.

WHERE PERSONAL DATA LIVES IN A DEALERSHIP, AND WHICH STANDARD PROTECTS IT

1	2	3	4	5	6	7	8
Website lead DAT-002 · 003	**Showroom** DAT-001 · 002	**Test drive** DAT-007 · 012	**Finance & insurance** DAT-003 · 010	**Service** DAT-002 · 012	**Marketing** DAT-004	**OEM & vendors** DAT-010 · 011	**Head office** DAT-005 · 006 · 008 · 009

FIVE TERMS YOU'LL SEE ON EVERY PAGE

Personal data
Anything that identifies a person: name, mobile, ID or Iqama number, plate linked to an owner, photo.

Sensitive data
Includes health, genetic, credit and financial data, and ethnic or religious origin. Explicit consent, higher risk.

Controller
The dealership: it decides why and how customer data is used, and carries the fine.

Processor
A vendor handling data for you: call centre, DMS, SMS gateway, payroll. Needs a contract.

Data subject
The customer or employee the data is about. Has rights to access, correct and delete.

WHO IT'S FOR

Dealer principals & GMs

Understand the exposure you carry and decide what gets fixed first.

DPOs & compliance teams

One checklist tied to the law, with evidence rules for every item.

Auditors

Consistent scoring, a clear method and the questions to ask on site.

ENFORCEMENT HAS STARTED

SDAIA isn't sending reminders. It's issuing decisions.

On 16 January 2026, SDAIA announced that its violation committees had issued **48 decisions** confirming PDPL violations. It named four recurring failures, and every one of them is in this guidebook:

Processing without a legal basis
In this guide: DAT-003 · 005 · 011

Disclosure without justification
In this guide: DAT-010 · 012

Weak security measures
In this guide: DAT-007 · 008 · 012

Marketing without consent
In this guide: DAT-004

THE PDPL PENALTY LADDER

LEVEL 1
Warning
The committee may start with a warning and a corrective order.

LEVEL 2
SAR 5M
Maximum fine for any violation of the law or its regulations (Art. 36).

LEVEL 3
SAR 10M
The same violation repeated: the ceiling doubles.

LEVEL 4
2 yrs + SAR 3M
Criminal: disclosing sensitive data to harm or for gain (Art. 35). Doubled on repeat.

On top of any level: **publication of the decision** with your name, **confiscation of proceeds** and corrective orders across every branch.

WHAT CAR COMPANIES ARE ACTUALLY PAYING FOR THE SAME FAILURES

COMPANY	FINE	WHAT THEY GOT WRONG	SAME AS
Volkswagen Germany · Jul 2022	**€1.1M** ≈ SAR 4.5M	Missing privacy signs on test vehicles, no processor contract, incomplete processing records	DAT-002 · 005 · 010
General Motors California · May 2026	**$12.75M** SAR 47.8M	Sold drivers' location and driving data to brokers without adequate notice or consent	DAT-003 · 007
Honda California · Mar 2025	**$632,500** SAR 2.4M	Demanded excessive information to process privacy requests; missing contracts with ad-tech firms	DAT-009 · 010
Ford California · Mar 2026	**$375,703** SAR 1.4M	Forced email verification before customers could opt out	DAT-009

SDAIA doesn't publish the amount of each decision, so these automotive cases under GDPR (EU) and CCPA (California) are the closest benchmarks: the same failures, priced by regulators abroad. Currency conversions are approximate.

AVERAGE OF THESE 4 AUTOMOTIVE FINES
≈ SAR 14M
Nearly **3× the PDPL ceiling** for a single violation. Regulators treat car companies as high-value data holders.

YOUR THEORETICAL CEILING
SAR 60M
12 standards × SAR 5M if each is found as a separate violation. **SAR 120M** if they're repeated.

HOW TO USE THIS GUIDE

One page per standard. One price per gap.

1. **Header**: code, area, owner and the maximum penalty
2. **The law**: the exact article SDAIA will cite
3. **The cost**: fine, what else can happen and a real case
4. **Right / wrong**: illustrated pass and fail, plus how to audit

THE 12 PDPL STANDARDS

DAT-001	PDPL Awareness Materials Displayed	LINKED	SAR 5M	7 days	5
DAT-002	Privacy Notice at Collection Points	CRITICAL	SAR 5M	72 hours	6
DAT-003	Lawful Basis & Consent Records ⛓ PRISON	CRITICAL	SAR 5M	7 days	7
DAT-004	Marketing SMS & Email Consent	CRITICAL	SAR 5M	24 hours	8
DAT-005	Records of Processing Activities	CRITICAL	SAR 5M	30 days	9
DAT-006	DPO Appointment & SDAIA Registration	CRITICAL	SAR 5M	30 days	10
DAT-007	Data Retention & Destruction	CRITICAL	SAR 5M	30 days	11
DAT-008	Personal Data Breach Notification	CRITICAL	SAR 5M	7 days	12
DAT-009	Data Subject Request Handling	CRITICAL	SAR 5M	7 days	13
DAT-010	Data Processor Contracts	CRITICAL	SAR 5M	30 days	14
DAT-011	Cross-Border Data Transfers	CRITICAL	SAR 5M	30 days	15
DAT-012	Physical Security of Customer Files ⛓ PRISON	CRITICAL	SAR 5M	Immediate	16

IDEAL FIX TIME · COUNTED FROM AUDIT SUBMISSION

Immediate	Fix before end of shift · data exposed right now	1 standard
24 hours	Fix within 1 working day · live unlawful processing	1 standard
72 hours	Fix within 3 working days · customers not informed	1 standard
7 days	Fix within 1 week · process and proof gaps	4 standards
30 days	Plan and close within 1 month · documents, contracts, governance	5 standards

SCORING EACH CHECKPOINT

PASS

Every criterion met at the time of audit, with evidence captured.

FAIL

Any criterion not met. Record it, attach evidence, create an action.

N/A

Only where "Applies when" rules it out (e.g. no transfers abroad). Record why.

DAT-001 PDPL · STANDARD 01 OF 12

PDPL Awareness Materials Displayed

Area **Reception · Staff areas** | Person in charge **Branch Manager · DPO** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

linked exposure: there is no fine for the poster itself

It's your **first proof of awareness** when SDAIA asks what you've done

• LINKED

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · No article requires a poster: it is company policy and the visible sign of an awareness programme · Penalty provisions: **PDPL Art. 35 & 36**

WHAT WE CHECK

PDPL awareness material, in the company's approved format, is displayed where every employee and visitor can see it.

CHECKPOINTS IN THE AUDIT

Q1 Are Personal Data Protection Law (PDPL) awareness materials, in the company's approved format, displayed in a visible area for employees and visitors?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

No fine for a missing poster. But it signals there's no awareness programme, and every violation it should have prevented carries **up to SAR 5 million**.

BEYOND THE FINE

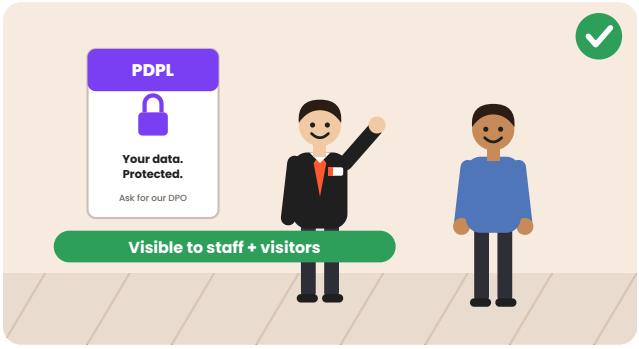
Untrained staff are the ones who forward customer lists on WhatsApp. Disclosing **sensitive data** to harm or for gain is a crime: **up to 2 years in prison and SAR 3M**.

REAL ENFORCEMENT

48 decisions

issued by SDAIA's violation committees by January 2026. The message: the grace period is over and **compliance is mandatory**.

✔ RIGHT WAY



Approved PDPL poster at reception, where every visitor and employee walks past it.

✖ WRONG WAY

LINKED · SAR 5M



Poster covered by a promotion banner. Staff can't say what PDPL is.

PURPOSE

Awareness is the cheapest control you have. Staff who know the rules stop the mistakes that lead to the SAR 5M findings in the rest of this guide.

FIX IT WITHIN

◷ 7 days

AUDIT CRITERIA · PASS WHEN

- Approved PDPL material displayed at reception and in staff areas
- Current version, not hidden, faded or covered
- Staff asked at random can explain what it means

IDEAL WAY OF AUDITING

1. Walk reception, showroom and staff room
2. Check the material matches the approved version
3. Ask 2 staff: "What does PDPL mean for you?"

Evidence: Photo of displayed material + notes of staff answers.

WORST CASE The poster costs nothing. The mistakes an untrained team makes (a forwarded customer list, an unconsented offer blast) cost **up to SAR 5 million each**.

DAT-002 PDPL · STANDARD 02 OF 12

Privacy Notice at Collection Points

Area **Showroom · Service · Website**

Person in charge **DPO · Branch Manager**

Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 12** (privacy policy) and **Art. 13** (information at collection) · **Implementing Regulations Art. 4 & 18** · Penalty: **PDPL Art. 36**

WHAT WE CHECK

Customers are told why their data is collected, on what legal basis, who receives it and what their rights are: on every form, on the website and wherever CCTV records them.

CHECKPOINTS IN THE AUDIT

- **Q1** Is a privacy notice (purpose, legal basis, recipients, data subject rights) provided on customer forms at the branch?
- **Q2** Is a privacy policy published on the website/app where personal data is collected?
- **Q3** Is a visible notice displayed where CCTV records customers or visitors?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

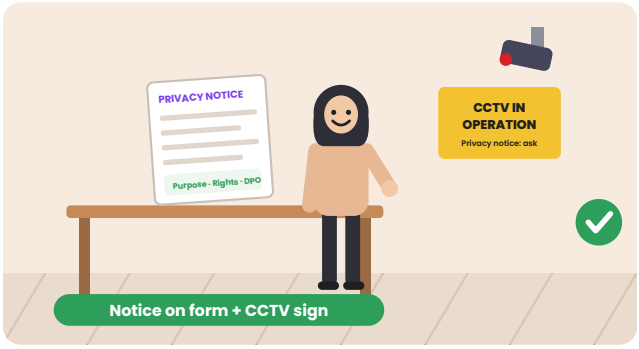
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

REAL ENFORCEMENT

€1.1M

Volkswagen fine in Germany (2022). One finding: **camera signs with privacy information were missing** on test vehicles. The regulator called it low severity.

✔ RIGHT WAY



Customer form carries a privacy notice, and a CCTV sign tells visitors they're being recorded.

✖ WRONG WAY

UP TO SAR 5M



Form asks for ID, mobile and salary with no explanation. The camera records with no sign.

PURPOSE

Dealers collect data at every step: lead forms, test drives, finance and service. A customer who isn't told what happens to their data hasn't been treated lawfully.

FIX IT WITHIN

◷ 72 hours

AUDIT CRITERIA · PASS WHEN

- Every customer form states purpose, legal basis, recipients and rights
- Privacy policy live on every website and app page that collects data
- A visible sign in every CCTV-covered area

IDEAL WAY OF AUDITING

1. Collect one of each form: lead, test drive, finance, service
2. Open the website lead form and check the policy link
3. Walk the site and match each camera to a sign

Evidence: Photos of forms + website screenshot + photo of each CCTV sign.

WORST CASE A missing camera sign was one of the findings behind **a €1.1 million fine** on Volkswagen. Under PDPL the same gap can cost **up to SAR 5 million**.

DAT-003 PDPL · STANDARD 03 OF 12

Lawful Basis & Consent Records

Area **CRM · F&I desk** | Person in charge **Data Protection Officer** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL **⛓ PRISON RISK**

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 5 & 6** (consent and its exceptions) · Implementing Regulations (consent provisions) · Penalties: **Art. 36**, criminal offence **Art. 35**

WHAT WE CHECK

Every use of customer data has a documented legal reason. Where that reason is consent, the dealership can produce it on demand. Sensitive and credit data needs explicit consent first.

CHECKPOINTS IN THE AUDIT

- **Q1** Is a lawful basis documented for each personal data processing activity?
- **Q2** Is customer consent, where relied on, captured and retrievable (signed form or system log)?
- **Q3** Is explicit consent obtained before processing sensitive or credit data?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

Disclosing **sensitive data** with intent to harm or for personal benefit is a criminal offence: **up to 2 years in prison and/or SAR 3M**, doubled on repeat.

REAL ENFORCEMENT

$12.75M

(≈ SAR 47.8M) paid by General Motors in May 2026 for selling drivers' data to brokers **without adequate notice or consent**. California's largest privacy penalty yet.

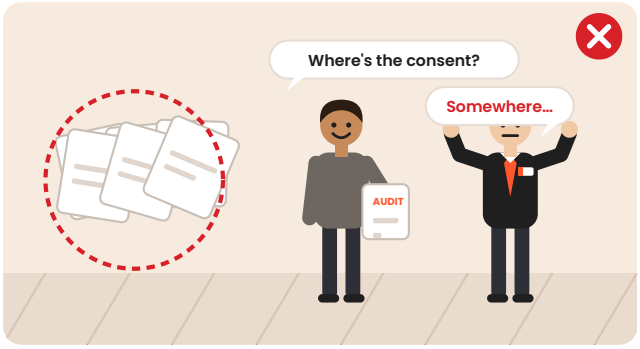
✔ RIGHT WAY



Customer record shows the legal basis, the consent, the date and where the signed proof is stored.

✖ WRONG WAY

SAR 5M + PRISON



Consent forms are loose in a drawer. When the auditor asks, nobody can find them.

PURPOSE

Consent you can't prove is consent you don't have. When a customer complains, SDAIA will ask for the record, not your word.

FIX IT WITHIN

◷ 7 days

AUDIT CRITERIA · PASS WHEN

- Legal basis recorded for each processing activity
- Consent retrievable for every sampled customer (form or system log)
- Explicit consent on file before credit or sensitive data is processed

IDEAL WAY OF AUDITING

1. Pick 10 customers across sales, F&I and service
2. Ask for the legal basis and consent proof for each
3. Check F&I files for explicit consent before credit checks

Evidence: CRM screenshots of consent fields + signed F&I consent forms.

WORST CASE A car maker paid **SAR 47.8 million** for using data without proper consent. Under PDPL, share sensitive data unlawfully and it's no longer only a fine: it's **up to 2 years in prison**.

DAT-004 PDPL · STANDARD 04 OF 12

Marketing SMS & Email Consent

Area **Sales & Service CRM** | Person in charge **DPO · Branch Manager** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 25** (marketing and awareness) · **Implementing Regulations Art. 28–29** (advertising and direct marketing) · Penalty: **PDPL Art. 36**

WHAT WE CHECK

Every promotional SMS, WhatsApp or email goes only to a customer who gave prior, recorded consent, and every message lets them stop it.

CHECKPOINTS IN THE AUDIT

- **Q1** Is prior consent recorded for every customer receiving marketing SMS, WhatsApp or email?
- **Q2** Does each marketing message include a working opt-out mechanism?
- **Q3** Are opt-out requests actioned and suppressed in the marketing system?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

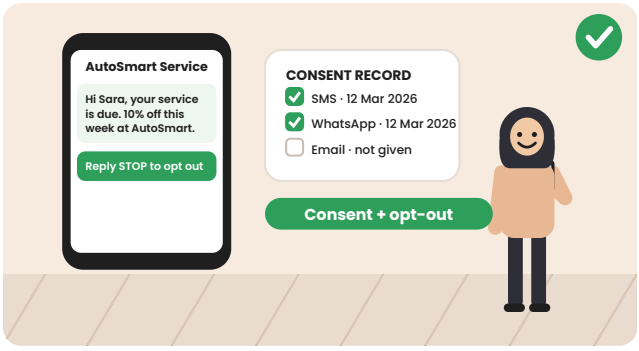
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

REAL ENFORCEMENT

48 decisions

issued by SDAIA committees by January 2026. **Marketing messages sent without consent** was one of the four recurring violations.

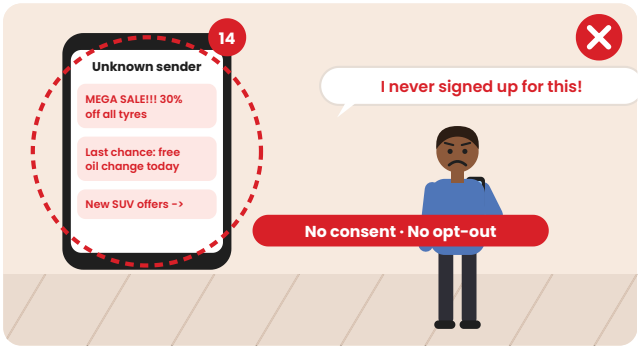
✔ RIGHT WAY



Service reminder goes only to customers with a dated consent record, and every message ends with a working opt-out.

✖ WRONG WAY

UP TO SAR 5M



The whole CRM list gets blasted with offers. No consent on file, no way to stop the messages.

PURPOSE

Dealerships hold thousands of phone numbers from sales, service and test drives. Using them for promotions without consent is unlawful processing, and every complaint is evidence.

FIX IT WITHIN

◷ 24 hours

AUDIT CRITERIA · PASS WHEN

- Dated consent record (channel + wording) for every sampled recipient
- Every sampled message carries a working opt-out (e.g. "Reply STOP")
- Opt-outs are suppressed and get no further marketing

IDEAL WAY OF AUDITING

1. Pull 10 recipients from the last SMS / WhatsApp campaign
2. Match each one to a consent record in the CRM
3. Opt out from a test number and confirm suppression

Evidence: CRM consent export + screenshot of message with opt-out + suppression list entry.

WORST CASE One offer blast to an unconsented list can bring an SDAIA decision of up to **SAR 5 million**, published with your name on it. Do it again after a warning: **SAR 10 million**.

DAT-005 PDPL · STANDARD 05 OF 12

Records of Processing Activities

Area **Head office · All branches** | Person in charge **Data Protection Officer**

Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 31** · **Implementing Regulations Art. 33** · Penalty: **PDPL Art. 36**

WHAT WE CHECK

A Record of Processing Activities (ROPA) lists every way the dealership uses personal data: why, what data, who receives it, how long it's kept and how it's protected.

Applies when: Keep the ROPA for the processing period plus 5 years. SDAIA can request it at any time.

CHECKPOINTS IN THE AUDIT

- **Q1** Is a Record of Processing Activities (ROPA) maintained covering all branch processes?
- **Q2** Does the ROPA state purposes, data categories, recipients, retention periods and security measures?
- **Q3** Has the ROPA been reviewed/updated within the last 12 months?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

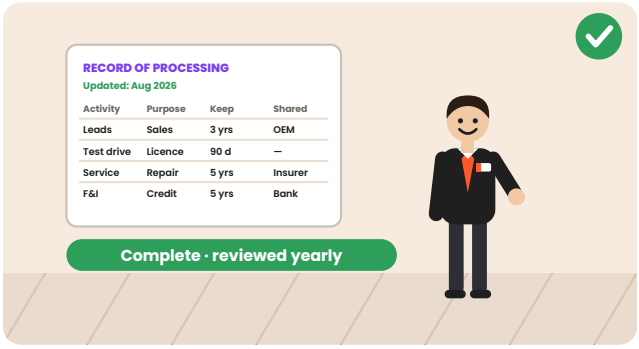
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

REAL ENFORCEMENT

€1.1M

Volkswagen (2022): **records of processing were incomplete**, with the security measures missing. One of four findings behind the fine.

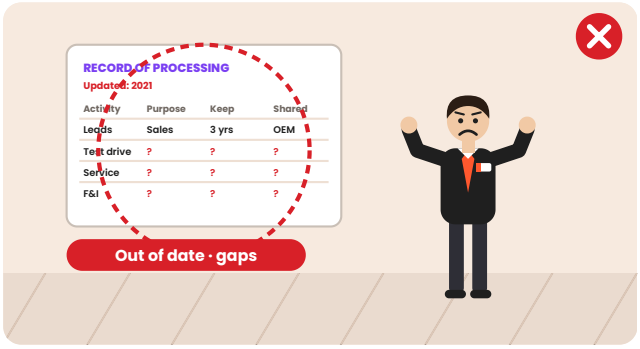
✔ RIGHT WAY



ROPA covers leads, test drives, service and F&I, with purpose, retention and recipients, reviewed this year.

✖ WRONG WAY

UP TO SAR 5M



Last updated in 2021. Most activities have no purpose, retention period or recipient.

PURPOSE

The ROPA is the first document SDAIA asks for. Without it you can't show you know what data you hold, so every other answer looks weak.

FIX IT WITHIN

30 days

AUDIT CRITERIA · PASS WHEN

- Covers every process: sales, test drive, F&I, service, marketing, HR
- Each entry states purpose, data, recipients, retention and security
- Reviewed or updated in the last 12 months

IDEAL WAY OF AUDITING

1. Request the ROPA and its last review date
2. Trace 3 real processes (e.g. test drive) to their entries
3. Check every entry has all five fields filled

Evidence: Copy of the ROPA with review date + 3 traced process samples.

WORST CASE It's the first document SDAIA will ask for. Missing or out of date, you've failed before the inspection starts, with a ceiling of **SAR 5 million**.

autosmart

DAT-006 PDPL · STANDARD 06 OF 12

DPO Appointment & SDAIA Registration

Area **Head office** | Person in charge **Legal & Compliance · DPO** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 30(2)** · **Implementing Regulations Art. 32** (DPO) & **Art. 34** (registration) · SDAIA Rules for Appointing a DPO · SDAIA Registration Rules

WHAT WE CHECK

Where the rules require it, a Data Protection Officer is formally appointed and the entity is registered on SDAIA's National Data Governance Platform with a valid certificate.

Applies when: Only where required: e.g. core processing of sensitive data or large-scale systematic monitoring. A registration certificate is valid for a maximum of 5 years.

CHECKPOINTS IN THE AUDIT

- **Q1** Is a Data Protection Officer formally appointed where required?
- **Q2** Is the entity registered on SDAIA's National Data Governance Platform with a valid certificate, where required?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

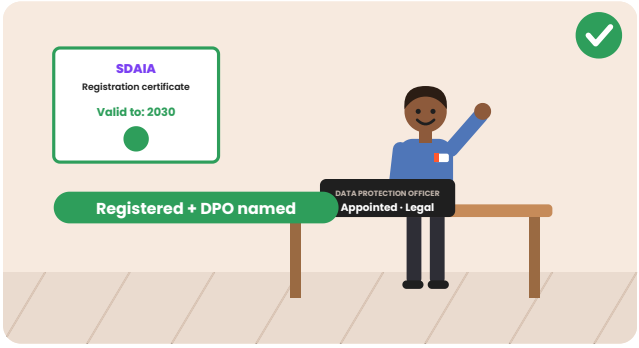
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

REAL ENFORCEMENT

48 decisions

by SDAIA committees. **Failure to put organisational measures in place** was one of four recurring violations. No accountable owner is the most basic gap.

✔ RIGHT WAY



Registration is valid to 2030 and a named DPO owns data protection.

✖ WRONG WAY

UP TO SAR 5M



Certificate expired in 2024. The DPO desk is empty, so nobody owns the problem.

PURPOSE

Someone has to own data protection. Without a DPO, breach reports, customer requests and SDAIA questions fall between departments.

FIX IT WITHIN

30 days

AUDIT CRITERIA · PASS WHEN

- Assessment on file showing whether a DPO and registration are required
- Where required: DPO formally appointed in writing
- Where required: registration certificate valid and current

IDEAL WAY OF AUDITING

1. Ask for the DPO / registration assessment
2. See the appointment letter and DPO contact
3. Check the certificate's expiry date on the platform

Evidence: Appointment letter + registration certificate + assessment memo.

WORST CASE With no DPO, nobody reports a breach in 72 hours or answers a customer in 30 days. Every missed deadline is **another violation of up to SAR 5 million**.

DAT-007 PDPL · STANDARD 07 OF 12

Data Retention & Destruction

Area **Archive · Showroom · Service** | Person in charge **DPO · Branch Manager**

Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 18** (destruction when no longer necessary) · Penalty: **PDPL Art. 36**

WHAT WE CHECK

Personal data is kept only as long as it's needed. An approved schedule says how long, and data past that date is securely destroyed and logged.

CHECKPOINTS IN THE AUDIT

- **Q1** Is an approved retention schedule in place for personal data held by the branch?
- **Q2** Is personal data past its retention period destroyed (shredding/secure deletion) with a destruction log?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

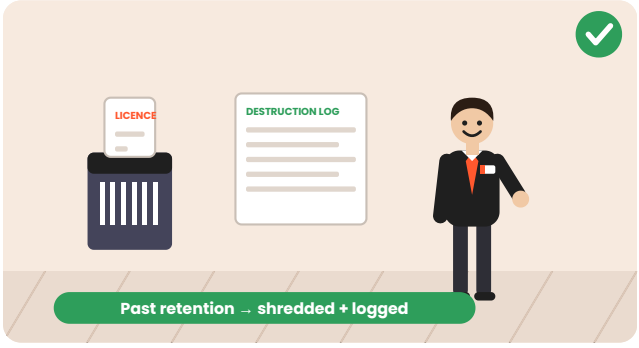
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

WHY IT MATTERS

$12.75M

GM's 2026 penalty was California's first for **data minimisation and purpose limitation**: holding and using data beyond what customers agreed to.

✔ RIGHT WAY



Licence copies past retention go through the shredder, and every batch is logged.

✖ WRONG WAY

UP TO SAR 5M



Ten years of licences, Iqama copies and old leads in boxes. Nobody can say why they're still here.

PURPOSE

Every old file is risk with no value. If it leaks, you'll have to explain why you still had a 2016 licence copy, and there's no good answer.

FIX IT WITHIN

◷ 30 days

AUDIT CRITERIA · PASS WHEN

- Approved retention schedule for each data type
- Nothing in sampled storage is past its retention date
- Destruction log records what, when, how and by whom

IDEAL WAY OF AUDITING

1. Get the retention schedule
2. Open 3 archive boxes and 1 CRM report; check the dates
3. Match destroyed batches to the destruction log

Evidence: Retention schedule + photos of archive + destruction log extract.

WORST CASE A leak of data you should have deleted years ago can be **two violations, not one**: keeping it, and failing to protect it. Up to **SAR 5 million each**.

autosmart

DAT-008 PDPL · STANDARD 08 OF 12

Personal Data Breach Notification

Area **IT · Head office** | Person in charge **DPO · Legal & Compliance** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 20** · **Implementing Regulations Art. 24** (notify within 72 hours via the SDAIA platform) · Penalty: **PDPL Art. 36**

WHAT WE CHECK

When personal data leaks, SDAIA is notified within 72 hours and affected customers are told where needed. A written procedure and an incident register make that possible.

CHECKPOINTS IN THE AUDIT

- **Q1** Is a documented breach response procedure in place requiring notification to SDAIA within 72 hours?
- **Q2** Is a breach/incident register maintained, including notifications made to SDAIA and affected individuals?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

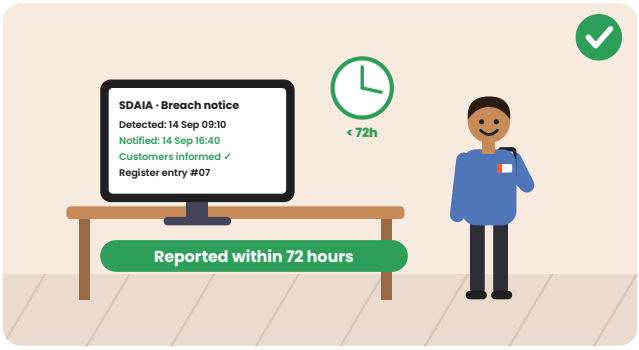
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

THE DEADLINE

72 hours

from becoming aware of a breach to notifying SDAIA through its platform. The clock **doesn't wait for your investigation** to finish.

✔ RIGHT WAY



Leak detected in the morning, reported to SDAIA the same day and logged in the incident register.

✖ WRONG WAY

UP TO SAR 5M



A CRM export leaked 9 days ago. Management decided to keep quiet.

PURPOSE

Breaches happen: a stolen laptop, a wrong email, a leaked export. Hiding one turns an incident into a violation.

FIX IT WITHIN

◷ 7 days

AUDIT CRITERIA · PASS WHEN

- Written procedure with the 72-hour SDAIA step and a named owner
- Incident register kept, including near-misses
- Past notifications to SDAIA and customers recorded

IDEAL WAY OF AUDITING

1. Read the procedure: who, how and by when
2. Review the incident register for the last 12 months
3. Ask the owner to walk through a mock breach

Evidence: Procedure + register extract + any SDAIA notification receipts.

WORST CASE The breach is one problem. Hiding it is another: a missed 72-hour deadline is a separate violation, **up to SAR 5 million**, and **SAR 10 million** if it happens again.

DAT-009 PDPL · STANDARD 09 OF 12

Data Subject Request Handling

Area **Customer care · Website** | Person in charge **DPO · Branch Manager** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 4** (data subject rights) · Implementing Regulations (30-day response, extendable once) · Penalty: **PDPL Art. 36**

WHAT WE CHECK

Customers have an easy, published way to ask for access to, correction of or deletion of their data, and every request is answered within 30 days.

CHECKPOINTS IN THE AUDIT

Q1 Is there a published channel for customers to request access, correction or deletion of their data?

Q2 Is a request log maintained showing responses issued within 30 days (or justified 30-day extension)?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

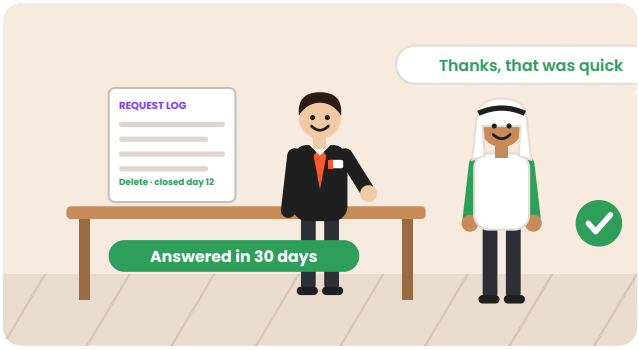
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

REAL ENFORCEMENT

SAR 3.8M

paid by Honda (2025) and Ford (2026) combined in California for making customers **jump through hoops to use their privacy rights**.

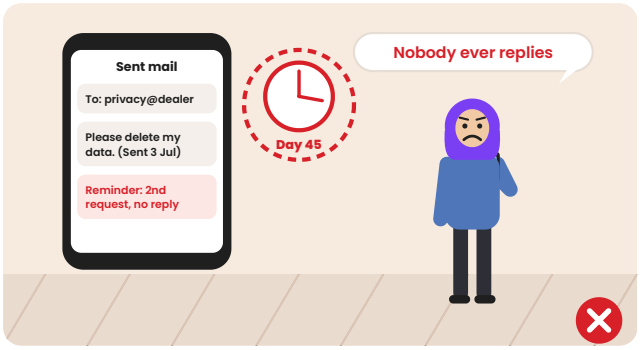
✔ RIGHT WAY



Deletion request logged and closed on day 12, well inside 30 days.

✖ WRONG WAY

UP TO SAR 5M



Customer emailed twice. 45 days later, still no reply.

PURPOSE

Customers who can't reach you go to SDAIA. A clear channel and a 30-day answer stop a request from becoming a complaint.

FIX IT WITHIN

◷ 7 days

AUDIT CRITERIA · PASS WHEN

- A published channel (email, form, desk) for data requests
- Request log with dates received and answered
- Every response within 30 days, or one justified extension

IDEAL WAY OF AUDITING

1. Find the channel on the website and at the branch
2. Review the request log for the last 6 months
3. Send a test request and time the response

Evidence: Screenshot of channel + request log extract + test request result.

WORST CASE Two car makers paid **SAR 3.8 million combined** for making privacy requests hard. Ignoring them entirely under PDPL: **up to SAR 5 million**.

DAT-010 PDPL · STANDARD 10 OF 12

Data Processor Contracts

Area **Procurement · IT** | Person in charge **Legal & Compliance Officer** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 8** (selection of processors) · Implementing Regulations (processor agreements) · Penalty: **PDPL Art. 36**

WHAT WE CHECK

Every vendor that handles customer or employee data (call centre, CRM, DMS, payroll, marketing agency) works under a written agreement covering purpose, security and PDPL.

Applies when: Wherever a third party processes personal data for you: IT, call centre, CRM, payroll, courier.

CHECKPOINTS IN THE AUDIT

Q1 Are written data processing agreements in place with all vendors handling customer or employee personal data?

Q2 Do the agreements specify processing purpose, security obligations and compliance with the PDPL?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

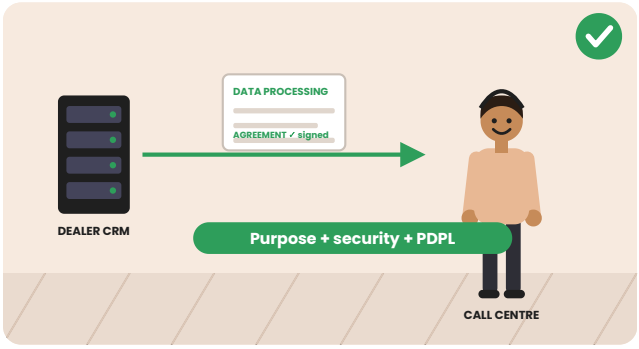
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

REAL ENFORCEMENT

€1.1M

Volkswagen (2022): **no data processing contract** with the service provider handling the data. One of four findings behind the fine.

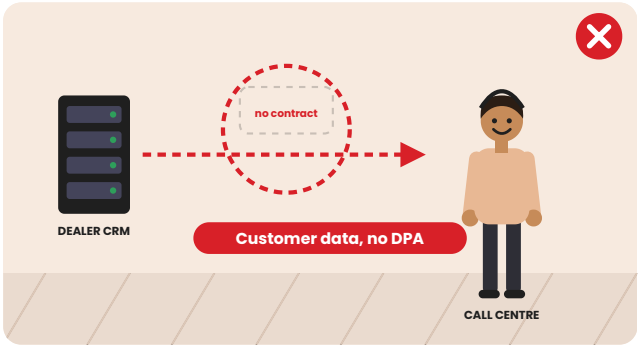
✔ RIGHT WAY



Call centre gets customer data under a signed agreement covering purpose, security and PDPL.

✖ WRONG WAY

UP TO SAR 5M



Customer lists go to the call centre with no contract. If they leak it, it's your violation.

PURPOSE

You stay responsible for data your vendors handle. A processor agreement proves you chose them carefully and bound them to the law.

FIX IT WITHIN

30 days

AUDIT CRITERIA · PASS WHEN

- Vendor list shows everyone who touches personal data
- A signed processing agreement for each one
- Each agreement covers purpose, security and PDPL

IDEAL WAY OF AUDITING

1. List vendors: DMS, CRM, call centre, SMS, payroll, agencies
2. Request the agreement for 3 of them
3. Check for purpose, security and PDPL clauses

Evidence: Vendor list + 3 agreement copies with the clauses marked.

WORST CASE Your vendor's leak is **your violation**. With no contract, you can't show you did anything to prevent it, and the ceiling is **SAR 5 million**.

autosmart

DAT-011 PDPL · STANDARD 11 OF 12

Cross-Border Data Transfers

Area **IT · OEM systems** | Person in charge **Legal & Compliance · DPO** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 29** · **Regulations on Personal Data Transfer outside the Kingdom** (SDAIA) · Penalty: **PDPL Art. 36**

WHAT WE CHECK

Every flow of personal data out of Saudi Arabia is known, each one has an approved safeguard, and a risk assessment is on file where the rules require one.

Applies when: Only where personal data is transferred or accessed outside the Kingdom, e.g. OEM global systems or foreign cloud.

CHECKPOINTS IN THE AUDIT

- **Q1** Are all transfers of personal data outside Saudi Arabia identified (e.g. foreign cloud, parent company systems)?
- **Q2** Is an approved safeguard (SDAIA SCCs, binding common rules or certificate) in place for each transfer?
- **Q3** Is a transfer risk assessment documented where required (sensitive data or non-adequate country)?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

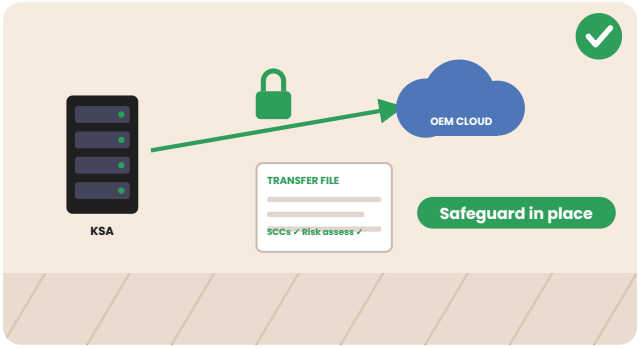
The committee can order its decision **published** (your dealership named), **proceeds confiscated** and corrective action across every branch.

WHY IT MATTERS

1 upload

to an OEM's global warranty, CRM or telematics platform **is a cross-border transfer**. It's easy to do every day without realising it.

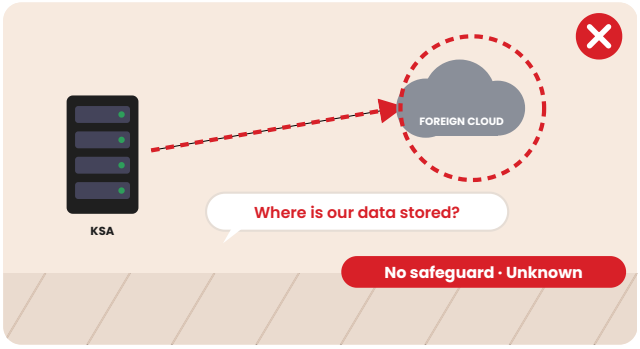
✔ RIGHT WAY



Data sent to the OEM cloud abroad is covered by SDAIA standard clauses and a documented risk assessment.

✖ WRONG WAY

UP TO SAR 5M



Nobody knows where the vendor stores the data. No safeguard, no assessment.

PURPOSE

Dealers share data with OEM systems, global DMS vendors and foreign cloud services every day. Each transfer abroad needs a lawful route.

FIX IT WITHIN

30 days

AUDIT CRITERIA · PASS WHEN

- Transfer map lists every system storing or accessing data abroad
- An approved safeguard (SCCs, binding rules or certificate) for each
- Risk assessment on file for sensitive data or non-adequate countries

IDEAL WAY OF AUDITING

1. Ask IT where DMS, CRM, email and OEM portals are hosted
2. Match each foreign location to its safeguard
3. Check the risk assessment for sensitive data flows

Evidence: Transfer map + safeguard documents + risk assessment.

WORST CASE Every customer file sent abroad without a safeguard is **unlawful processing**: a ceiling of **SAR 5 million**, doubling to **SAR 10 million** on repeat.

DAT-012 PDPL · STANDARD 12 OF 12

Physical Security of Customer Files

Area **Showroom · F&I · Service** | Person in charge **Branch / Site Manager** | Regulator **SDAIA**

MAXIMUM PENALTY

SAR 5,000,000

per violation, set by the SDAIA violations committee

Repeat violation: **up to SAR 10,000,000**

• CRITICAL **⛓ PRISON RISK**

THE LAW

PDPL

Personal Data Protection Law (Royal Decree M/19 of 1443H, amended by M/148 of 1444H) and its Implementing Regulations · **Art. 19** (security measures) and **Art. 28** (copying official identification documents) · Penalties: **Art. 36**, criminal offence **Art. 35**

WHAT WE CHECK

Paper files are locked away, desks and printers are clear, and ID, Iqama or passport copies are only taken where a law or competent authority requires it.

CHECKPOINTS IN THE AUDIT

- **Q1** Are customer files and documents containing personal data kept in locked cabinets or restricted rooms?
- **Q2** Are desks, counters and printers free of unattended customer documents (clean desk)?
- **Q3** Are copies of national ID/Iqama/passport taken only where required by law or a competent authority?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

A warning or a fine of **up to SAR 5 million for any violation** of the law or its regulations. For a repeat, the ceiling **doubles to SAR 10 million**.

BEYOND THE FINE

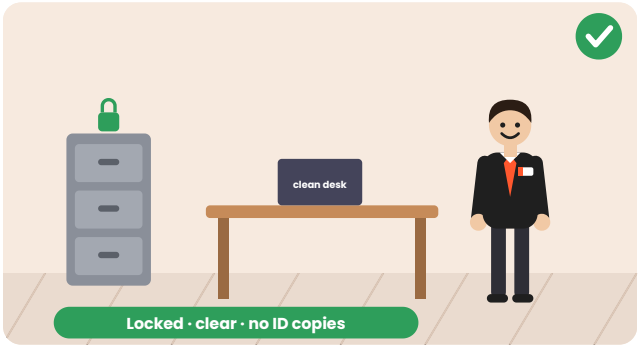
Disclosing **sensitive data** with intent to harm or for personal benefit is a criminal offence: **up to 2 years in prison and/or SAR 3M**, doubled on repeat.

REAL ENFORCEMENT

48 decisions

by SDAIA committees. **Failure to put security measures in place** was named among the four most common violations.

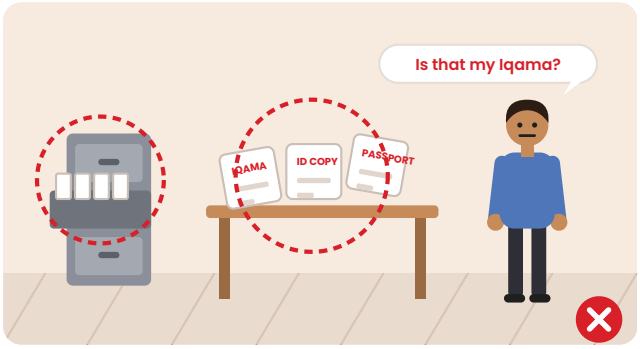
✔ RIGHT WAY



Files locked, desk clear, no unnecessary ID copies taken.

✖ WRONG WAY

SAR 5M + PRISON



Iqama and passport copies left on the desk, cabinet open. A customer spots his own ID.

PURPOSE

The simplest leak is a piece of paper. An Iqama copy on a counter is personal data exposed to every visitor.

FIX IT WITHIN

◷ Immediate

AUDIT CRITERIA · PASS WHEN

- Customer files in locked cabinets or restricted rooms
- Desks, counters and printer trays clear of customer documents
- ID / Iqama / passport copies only where legally required

IDEAL WAY OF AUDITING

1. Walk F&I, sales and service desks unannounced
2. Check cabinets and the printer tray
3. Ask why each ID copy on file was taken

Evidence: Photos of desks, cabinets and printer trays + sample file check.

WORST CASE An ID copy on a counter looks harmless until it's misused. The fine ceiling is **SAR 5 million**, and deliberate disclosure of sensitive data can mean **2 years in prison**.

CLOSE THE GAPS BEFORE SDAIA FINDS THEM

Your 30-day PDPL action plan.

Work top to bottom. The left column is where data is exposed or unlawfully used **right now**. Tick each standard off only when the evidence is on file.

Today

- ☐ **DAT-012** Physical Security of Customer Files
  ◷ **Immediate**
- ☐ **DAT-004** Marketing SMS & Email Consent
  ◷ **24 hours**

This week

- ☐ **DAT-002** Privacy Notice at Collection Points
  ◷ **72 hours**
- ☐ **DAT-001** PDPL Awareness Materials Displayed
  ◷ **7 days**
- ☐ **DAT-003** Lawful Basis & Consent Records
  ◷ **7 days**
- ☐ **DAT-008** Personal Data Breach Notification
  ◷ **7 days**
- ☐ **DAT-009** Data Subject Request Handling
  ◷ **7 days**

This month

- ☐ **DAT-005** Records of Processing Activities
  ◷ **30 days**
- ☐ **DAT-006** DPO Appointment & SDAIA Registration
  ◷ **30 days**
- ☐ **DAT-007** Data Retention & Destruction
  ◷ **30 days**
- ☐ **DAT-010** Data Processor Contracts
  ◷ **30 days**
- ☐ **DAT-011** Cross-Border Data Transfers
  ◷ **30 days**

?/12 Count your passes. **Every fail is a separate exposure of up to SAR 5 million**, and the fines that matter most are the ones for problems you already knew about.

SOURCES

- SPA: PDPL committees impose penalties on confirmed violations (16 Jan 2026) · spa.gov.sa/en/N2489505
- IAPP: Saudi Arabia's data protection authority steps up enforcement · iapp.org
- Orrick: Volkswagen fined €1.1M for GDPR violations during test drives (Aug 2022) · orrick.com
- Hunton: California AG record $12.75M CCPA settlement with GM (May 2026) · hunton.com
- Hunton: CPPA fines Honda $632,500 (Mar 2025) · hunton.com
- State of Surveillance: CPPA connected-car sweep, Ford settlement (Mar 2026) · stateofsurveillance.org
- Personal Data Protection Law, Implementing Regulations and Transfer Regulations · sdaia.gov.sa

Disclaimer. For compliance-audit guidance only; not legal advice. Penalty amounts are statutory maximums; SDAIA has not published a per-violation fine schedule. Draft amendments to the Implementing Regulations (consulted Apr–May 2025) may change specific obligations. Confirm against the latest official publications.

AUDIT SIGN-OFF

DEALERSHIP / BRANCH	AUDITOR	DATE	SCORE __ / 12

BRANCH MANAGER SIGNATURE	DPO SIGNATURE