SPARK
PROFESSIONAL SERVICES

EGYPT · LAW NO. 151 OF 2020

Egypt's PDPL, in force.

A practical guide to the Personal Data Protection Law for organizations that collect, use or share personal data in Egypt.

INSIDE THIS GUIDE

14
sections, each tied to the article it comes from

2
readiness tracks: governance and legal, technical and operational

7
licence and permit categories the PDPC can issue

Contents

PART A · UNDERSTAND THE PICTURE

01 Where we are now 03

02 Who the law applies to 04

03 Personal and sensitive data 05

PART B · CORE OBLIGATIONS

04 Lawful processing 06

05 Controller and processor duties 07

06 Licences, permits and accreditation 08

07 The Data Protection Officer 09

PART C · ACTIVITIES WITH SPECIAL RULES

08 Sensitive and children's data 10

09 Cross-border transfers 11

10 Electronic direct marketing 12

PART D · WHEN A REQUEST OR INCIDENT COMES

11 Data subject rights and requests 13

12 Breach notification 14

PART E · ENFORCEMENT AND NEXT STEPS

13 Penalties and enforcement 15

14 Your readiness roadmap 16

HOW TO READ THE REFERENCES

"Art. X" is an article of the Personal Data Protection Law attached to Law No. 151 of 2020; "IL Art. X" is an article of the issuing law; "ER Art. X" is an article of the Executive Regulations (Ministerial Decree No. 816 of 2025).

BEFORE YOU ACT

This guide gives general information drawn from the text of the law. It is not legal advice. Confirm procedures, fees and forms with the PDPC before relying on them.

SECTION 01 — Part A · Understand the picture

Where we are now

For five years the PDPL existed largely on paper. The Executive Regulations changed that: they set out how licensing, DPO registration, inspection and enforcement work. With the one-year adjustment window granted by the issuing law now behind us, the question is no longer whether the law applies, but whether an organization can show it complies.

The road to enforcement

15 July 2020

Law No. 151 of 2020 published in the Official Gazette.

October 2020

The law takes effect three months after the day following publication (IL Art. 7).

1 November 2025

Executive Regulations issued by Ministerial Decree No. 816 of 2025.

One year later

The adjustment window ends: organizations must have aligned with the law and its regulations (IL Art. 6).

The numbers to know

72 h
to report a breach to the PDPC
Art. 7

3 days
working days to inform affected individuals
Art. 7

6 days
working days to answer a rights request
Art. 32

90 days
for the PDPC to decide a licence application
Art. 27

3 yrs
licence validity; permits last up to 1 year
Art. 1

EGP 5M
highest fine (EGP), with prison for some offences
Arts. 41, 42, 45

WHAT CHANGED IN PRACTICE

Processing personal data without the right PDPC authorization, without a registered Data Protection Officer, or without adequate security is now a live compliance exposure, not a future project. The PDPC can inspect, warn, suspend or cancel licences, and the economic courts hear criminal cases (IL Art. 5).

SECTION 02 — Part A · Understand the picture

Who the law applies to

The PDPL protects the personal data of natural persons processed electronically, in whole or in part, by any holder, controller or processor (IL Art. 1). Its criminal provisions also reach Egyptians abroad, foreign residents, and foreigners outside Egypt where the act is an offence there too and the data belongs to Egyptians or residents of Egypt (IL Art. 2).

Three roles Art. 1

Controller
Has the right to obtain personal data and decides how, and to what standards, it is kept or processed.

Processor
Processes personal data for itself or for a controller, under an agreement and on its instructions.

Holder
Holds personal data in any form or on any storage medium, whether it created the data or received it.

Roles attach to each activity, not to the organization. A software company is usually the controller of its own staff and customer data, and a processor of the data its clients load into its platform.

Outside the scope, with examples IL Art. 3

Exclusion	Example
Personal use	Data individuals keep about others for personal use, such as contacts on an employee's own phone or a family photo album.
Official statistics or a legal provision	Census data collected by CAPMAS, or the specific data a company must report to the Tax Authority under tax law. Only that processing is excluded, not the rest of the company's HR data.
Media purposes	An accurate press report about a public official, where the data is used for nothing else.
Judicial records	Police reports, prosecution files and court case papers.
National security bodies	Data held by the Presidency, the Ministries of Defence and Interior, the General Intelligence Service or the Administrative Control Authority.
Central Bank and supervised entities	A bank's customer data is excluded. Money transfer and exchange companies are **in scope**, and so are insurers, which the Financial Regulatory Authority supervises.

OFTEN MISSED

Controllers and processors outside Egypt must appoint a representative in Egypt (Art. 4(11), Art. 5(12)). Under the Executive Regulations, a foreign controller or processor with no branch in Egypt must have that local representative approved by the PDPC.

SECTION 03 — Part A · Understand the picture

Personal and sensitive data

Personal data Art. 1

Any data about an identified natural person, or one identifiable directly or indirectly by linking it with other data, such as a name, voice, picture, identification number or online identifier, or data revealing psychological, health, economic, cultural or social identity.

Sensitive personal data Art. 1

Data revealing mental, psychological, physical or genetic health, biometric data, financial data, religious beliefs, political opinions or security status. **In all cases, children's data is sensitive.**

Examples by sector

Sector	Personal data	Sensitive data
Insurance and non-bank finance	Name, phone, policy number, branch visits	Income and account data, medical reports in claims, biometric login
Healthcare	Patient name, appointment times	Diagnoses, lab results, genetic tests, mental health records
Retail and e-commerce	Delivery address, purchase history, device ID	Saved card details, any data on customers under 18
Education	Parents' contact details, staff records	All data on students under 18, parents' payment details
Telecom and technology	Phone numbers, IP addresses, location data	Fingerprint or face unlock data, payment data
Real estate and hospitality	Tenant and guest names, ID numbers, CCTV footage	Bank and payment details, data on guests' children

Other definitions that matter Art. 1

Term	Meaning under the law
Processing	Any electronic or technical operation on personal data: writing, collecting, recording, storing, combining, sending, receiving, publishing, erasing, changing, retrieving or analysing it.
Making data available	Any means that lets others learn of the data: viewing, sharing, publishing, transferring, using, displaying, sending or disclosing it.
Breach	Any unauthorized access, or unlawful copying, sending, sharing or transfer aimed at disclosing, destroying or altering personal data.
Cross-border movement	Transferring, making available, storing or processing personal data from inside Egypt to outside it, or the reverse.

SECTION 04 — Part B · Core obligations

Lawful processing

Everything starts from one rule: personal data may not be collected, processed, disclosed or revealed by any means without the explicit consent of the data subject, or in the cases the law permits (Art. 2).

Four lawful bases for electronic processing Art. 6

1

Consent

The data subject agrees to the processing for one or more specified purposes.

2

Contract or legal claims

Needed to perform or conclude a contract for the data subject, or to assert or defend their legal rights.

3

Legal obligation

Required by law, by an order of the competent investigation authorities, or by a court ruling.

4

Legitimate rights

Lets the controller meet its obligations, or a concerned party exercise legitimate rights, unless this conflicts with the data subject's fundamental rights.

Four conditions on every dataset Art. 3

01 Collected for legitimate, specified purposes declared to the data subject.

02 Accurate, sound and secured.

03 Processed lawfully and in a way that suits the purposes of collection.

04 Not kept longer than needed for that purpose.

CONSENT IN PRACTICE

Under ER Art. 2, providing data to receive a lawful service counts as consent to the processing that service needs, and nothing more; a new purpose needs fresh consent. Consent is also not the only basis: payroll rests on the employment contract.

HOW THE PDPC EXPECTS CONSENT TO LOOK

The PDPC's Data Subject Consent Guidelines ask for consent requests presented in Arabic as the primary language, kept separate from privacy notices and general terms and conditions, and given through a clear affirmative action, never presumed. For sensitive data, consent must be in writing, on paper or electronically.

SECTION 05 — Part B · Core obligations

Controller and processor duties

Articles 4 and 5 are the operational core of the PDPL. Most of what an inspector will ask to see comes from these two lists.

Area	Controller · Art. 4	Processor · Art. 5
Basis for data	Obtain data with consent or where the law permits	Process only on written instructions
Purpose	Set how processing is done; keep it within the specified purpose	Do not exceed the purpose or duration; tell the controller how long processing takes
Accuracy	Check data is correct and adequate; fix errors as soon as known	Keep processing consistent with the purpose
Security	Apply technical and organizational measures and standards	Protect the processing, media and devices used
Retention	Erase when the purpose ends, or keep only in a form that cannot identify the person	Erase at the end of processing or hand data back to the controller
Records	Data record: categories, recipients, legal basis, retention, erasure, cross-border transfers, security measures	Processing record: activities per controller, contacts, DPO, retention, erasure, security measures
Disclosure	Make data available only where the law permits	Same, and no processing that conflicts with the controller's purpose
Accountability	Prove compliance and allow PDPC inspection	Prove compliance on request and allow PDPC inspection
Authorization	Hold a PDPC licence or permit	Hold a PDPC licence or permit
Abroad	Appoint a representative in Egypt	Appoint a representative in Egypt

MORE THAN ONE CONTROLLER

Each controller carries every obligation in the law, and the data subject may exercise rights against each separately (Art. 4).

MORE THAN ONE PROCESSOR

Each processor is bound by every obligation unless a contract clearly divides their duties (Art. 5). Put it in writing.

Breaching the duties in Arts. 4, 5 or 7 carries a fine of EGP 300,000–3,000,000 (Art. 38).

SECTION 06 — Part B · Core obligations

Licences, permits and accreditation

Processing without the right authorization is a violation in its own right, even if nothing goes wrong with the data (Art. 4(10), Art. 5(11)). For most organizations, this is the first practical step.

Licence

Issued to legal persons only. Valid for three years, renewable.

Art. 1

Permit

Natural or legal persons, possibly for a specific task. Up to one year, renewable more than once.

Art. 1

Accreditation

Certifies a person or entity is qualified to provide data protection consulting.

Art. 1

Categories the PDPC issues Art. 26

Category	Covers
Controller or processor	Keeping, handling and processing personal data
Electronic direct marketing	Sending marketing communications
Associations, unions and clubs	Processing members' data within their activities
Visual surveillance	CCTV and similar tools in public places
Sensitive data	Controlling and processing sensitive personal data
Data protection consulting	Permits and accreditation to advise on PDPL compliance
Cross-border transfer	Moving personal data outside Egypt

- **Fees:** up to EGP 2,000,000 for a licence and EGP 500,000 for a permit or accreditation (Art. 26).
- **Application:** on PDPC forms, with proof of financial and technical capacity (Art. 27).
- **Decision:** within 90 days of a complete file; no answer means rejection (Art. 27).
- **More than one:** an organization may hold several licences or permits depending on the data it handles (Art. 27).
- **Changes:** the PDPC may amend conditions, for example after a merger (Art. 28).
- **Cancellation:** breached conditions, unpaid renewal fees, repeated non-compliance, unapproved assignment or bankruptcy (Art. 29).

HOW FEES ARE SET · ER ARTS. 19, 20, 34

Licence fees scale with the number of personal data records held: the smallest tier is exempt and the maximum applies above five million records. A licence for one role only (controller or processor) costs 50% less. Permit fees depend on both duration and volume. Consulting accreditation costs EGP 5,000 a year and lasts three years. Breaching licence rules: EGP 500,000–5,000,000 (Art. 45).

SECTION 07 — Part B · Core obligations

The Data Protection Officer

The DPO is the person the PDPC deals with. The law makes the appointment a personal duty of the organization's legal representative, with its own penalty.

Appointment and registration Art. 8

- The PDPC keeps a register of DPOs; the Executive Regulations set the conditions and procedure for registration.
- The legal representative of any controller or processor that is a legal person must appoint a competent employee, inside its own legal entity and structure, as DPO; register them with the PDPC; and announce the appointment.
- Where the controller or processor is a natural person, that person is responsible for applying the law.

What the DPO is responsible for Art. 9

- **Assess:** Periodically assess and test data protection systems, document the results and issue recommendations
- **Liaise:** Act as the direct point of contact with the PDPC and carry out its decisions
- **Enable rights:** Make it possible for data subjects to exercise their rights
- **Report breaches:** Notify the PDPC of any breach
- **Respond:** Answer requests from data subjects and others, and respond to the PDPC on complaints
- **Records:** Follow up the data record or processing record so it stays accurate
- **Remediate:** Remove violations inside the organization and take corrective action
- **Train:** Organize training so staff can meet the law's requirements

What the Executive Regulations add ER Arts. 7–9, 12

- Academic qualifications or professional certifications, practical experience, a PDPC-approved test and good conduct.
- The PDPC decides on registration within 30 working days.
- Each DPO gets a code showing the volume and nature of data they may handle.
- An annual privacy report to the PDPC.
- A new DPO files a report within 15 days of taking over.
- No conflicting duties; a separate work system if one DPO serves several entities.

PENALTY FOR THE ORGANIZATION

A legal representative who fails the Art. 8 duties: EGP 200,000–2,000,000 (Art. 39).

PENALTY FOR THE DPO

A DPO who fails the Art. 9 duties: EGP 200,000–2,000,000, or EGP 50,000–500,000 if due to negligence (Art. 40).

SECTION 08 — Part C · Activities with special rules

Sensitive and children's data

Sensitive data carries the strictest rules in the law: a licence, written consent, extra security, and the possibility of prison.

What the law requires Art. 12

- **A PDPC licence is required** to collect, transfer, store, keep, process or make available sensitive data, whether you are a natural or legal person.
- **Written and explicit consent** from the data subject is required, except where the law permits otherwise.
- **Children:** any of these operations needs the guardian's consent.
- A child's participation in a game, competition or any other activity cannot depend on giving more personal data than it needs.

Children by age ER Art. 15

Under 15

The guardian's explicit written consent before any processing. It must state how long it lasts, can be withdrawn or changed, and is given through PDPC-approved mechanisms.

15 to 18

The guardian's consent is still required; the child or the guardian may submit it, through mechanisms the PDPC sets.

- No profiling, tracking or behavioural monitoring of children taking part in games or competitions (ER Art. 14).
- Keep secure electronic records of consents and of erasure, correction or stop requests, and of how they were handled (ER Art. 14).

Common situations to check

- **HR and payroll:** medical certificates, salary and bank details, and biometric attendance are sensitive.
- **Employee benefits:** adding employees' children to a medical plan means processing children's data.
- **Customer onboarding:** income, card and account data collected for credit or payment is financial data.
- **Apps, games and events:** anything open to under-18s needs guardian consent and data minimization.

WHAT IS AT STAKE

Collecting, processing, storing, transferring or disclosing sensitive data without consent or legal basis: at least three months' imprisonment and/or a fine of EGP 500,000–5,000,000 (Art. 41).

SECTION 09 — Part C · Activities with special rules

Cross-border transfers

Transferring, storing or sharing personal data in a foreign country is prohibited unless that country offers a level of protection no lower than the PDPL **and** the PDPC has granted a licence or permit (Art. 14). The definition is wide: making data accessible from abroad also counts (Art. 1).

Exceptions with explicit consent

Art. 15

Where the destination lacks adequate protection, transfer is still allowed with the explicit consent of the data subject or their representative, for:

- Saving the data subject's life or providing medical care
- Proving, exercising or defending a right before the courts
- Concluding or performing a contract in the data subject's interest
- International judicial cooperation
- A necessity or legal obligation to protect the public interest
- Money transfers to another country under its laws
- An international agreement Egypt is party to

Sharing with a party abroad

Art. 16

Making data available to a controller or processor outside Egypt requires **a PDPC licence** and all three conditions:

01 The parties do similar work, or obtain the data for the same purpose.

02 Each party, or the data subject, has a legitimate interest.

03 The foreign party's legal and technical protection is no lower than in Egypt.

COMMON PITFALL

Email, CRM, HR, backup and analytics platforms hosted outside Egypt move personal data across the border every day. Most organizations need a cross-border licence or permit even if they never think of themselves as "transferring" data. Under ER Art. 16, transfers are limited to the countries named in the licence, which must be updated before adding a new one.

Questions to ask about every system

- Where is the data stored and backed up?
- Who can access it from abroad, including vendor support teams?
- Which countries are involved, and what protection do they offer?
- Is the transfer covered by a PDPC licence or permit?

WHAT IS AT STAKE

Breaching Arts. 14, 15 or 16: at least three months' imprisonment and/or EGP 500,000–5,000,000 (Art. 42).

SECTION 10 — Part C · Activities with special rules

Electronic direct marketing

The law defines electronic marketing broadly: any message or advertising content sent by any technical means to specific people to promote goods, services or commercial, political, social or charitable requests (Art. 1).

Before you send Art. 17

- Obtain the data subject's consent.
- Show who created and sent the message.
- Give a valid address where the sender can be reached.
- Say clearly that the message is direct marketing.
- Offer a clear, easy way to refuse or withdraw consent.

Sender obligations Art. 18

- Use the data for a specified marketing purpose.
- Do not disclose the recipient's contact details.
- Keep electronic records of consent, its changes or non-objection, for **three years** from the last message sent.
- Erase the data when consent is withdrawn or the purpose ends; marketing intermediaries must check the original sender holds consents and record the data's source (ER Art. 18).

You also need a licence Art. 26

Electronic direct marketing is its own licence or permit category. Marketing your own services and sending campaigns for others both fall under it, so agencies and platforms need to check their position as well as the brands they work for.

What a good consent record shows

Who and when

The person, the date and the channel where consent was given.

For what

The specific marketing purpose the person agreed to.

What changed

Every update, opt-out or objection, kept for three years.

WHAT IS AT STAKE

Breaching the marketing rules in Arts. 17 and 18: EGP 200,000–2,000,000 (Art. 43).

SECTION 11 — Part D · When a request or incident comes

Data subject rights and requests

The law gives every data subject six rights, and puts the work of honouring them on the organizations that hold the data.

The six rights Art. 2

Know and access
Know what personal data any holder, controller or processor has, and view, access or obtain it.

Withdraw consent
Withdraw prior consent to retention or processing.

Correct and erase
Correct, amend, erase, add to or update personal data.

Restrict
Limit processing to a specific scope.

Be told of breaches
Know about any breach of their personal data.

Object
Object to processing or its results where it conflicts with their fundamental rights.

How requests and complaints run

Step	What the law requires	Article
Request	Any holder, controller or processor must answer a rights request within six working days.	Art. 32
Fees	A charge set by the PDPC may apply, capped at EGP 20,000. Being told of a breach is always free.	Art. 2
Disclosure requests	Must be written and decided within six working days. A refusal needs reasons; silence counts as refusal.	Art. 10
Complaint	A data subject can complain to the PDPC about a violation, a refusal to honour rights, or a DPO decision.	Art. 33
PDPC decision	Issued within 30 working days; the organization must comply within 7 working days of notice.	Art. 33

Six working days is short: a request that travels from a branch, call centre or vendor to the DPO and back needs a defined intake channel, an identity check and a tracking log.

SECTION 12 — Part D · When a request or incident comes

Breach notification

Article 7 sets one of the tightest clocks in the law. Both controllers and processors carry the duty, and the PDPC informs the national security bodies in every case.

The timeline Art. 7

0
Become aware
The clock starts when the controller or processor learns of the breach.

72 h
Report to the PDPC
Report and send the required details. Immediately if national security is involved.

+3 days
Inform individuals
Notify affected data subjects within three working days of reporting, with the measures taken.

What the PDPC report must contain Art. 7

- The nature, form and causes of the breach, and the approximate number of records affected
- The DPO's details
- The likely consequences of the breach
- Measures taken and proposed to contain it and reduce harm
- Documentation of the breach and corrective actions
- Any documents or data the PDPC requests

Getting ready before it happens

A named owner
The DPO is the PDPC's contact and must notify it of breaches (Art. 9).

Detection that works
72 hours only helps if monitoring can spot a breach quickly.

Processors in the loop
Contracts should require vendors to tell you at once, since they carry the same duty.

A breach register
ER Art. 5 requires a secure electronic register of every breach, and notice to individuals through a channel agreed in advance.

WHAT IS AT STAKE

Failing the Art. 7 duties: EGP 300,000–3,000,000 (Art. 38).

SECTION 13 — Part E · Enforcement and next steps

Penalties and enforcement

Offence	Art.	Penalty (EGP)
Collecting, processing or disclosing data without consent or legal basis	36	EGP 100k–1M. For gain or to harm: 6+ months' prison and/or EGP 200k–2M
Refusing to let a data subject exercise their rights	37	EGP 100k–1M
Collecting data without the Art. 3 conditions	37	EGP 200k–2M
Controller or processor breaching Arts. 4, 5 or 7	38	EGP 300k–3M
Legal representative breaching Art. 8 (DPO)	39	EGP 200k–2M
DPO breaching Art. 9	40	EGP 200k–2M; negligence EGP 50k–500k
Sensitive data without consent or legal basis	41	3+ months' prison and/or EGP 500k–5M
Breaching cross-border rules (Arts. 14–16)	42	3+ months' prison and/or EGP 500k–5M
Breaching marketing rules (Arts. 17–18)	43	EGP 200k–2M
Breaching licence, permit or accreditation rules	45	EGP 500k–5M
Obstructing PDPC officers with judicial powers	46	6+ months' prison and/or EGP 200k–2M

ADMINISTRATIVE SANCTIONS · ART. 30

After a warning to remedy, the PDPC board can suspend or withdraw a licence, publish the violations at the violator's cost, or impose technical supervision at its expense.

WHAT MAKES IT WORSE · ARTS. 47–48

The de facto manager faces the same penalties if they knew and their failure contributed. Convictions are published in the press and online. Repeat offences double the range; attempts carry half.

RECONCILIATION AND SETTLEMENT · ART. 49

Offences under Arts. 36–41 and 43 can be resolved by reconciliation with the victim, with PDPC approval, before a final judgment. Offences under Arts. 42, 44 and 45 can be settled with the PDPC at any stage. Either way the criminal case ends, but the injured party keeps the right to compensation.

SECTION 14 — Part E · Enforcement and next steps

Your readiness roadmap

Readiness runs on two tracks at once. The law requires “technical and organizational measures” (Art. 4(6), Art. 5(7)) and leaves the detailed standards to the Executive Regulations, so paperwork alone will not satisfy an inspector.

Governance and legal

What you must decide, document and register

01 Confirm scope and roles
Which activities fall under the PDPL, and your role in each.

02 Build your records
The data record (Art. 4) or processing record (Art. 5).

03 Fix lawful bases and consent
Match each activity to an Art. 6 basis; refresh consent where needed.

04 Secure authorizations
Every licence or permit you need, including transfers, marketing, CCTV and sensitive data.

05 Appoint and register the DPO
With authority, resources and a direct line to management.

06 Paper your third parties
Written instructions and clear duties for every processor, at home and abroad.

Technical and operational

What protects the data and proves it

01 Discover and classify
Find where personal and sensitive data lives across systems and vendors.

02 Control access
Least privilege, strong authentication and regular reviews.

03 Encrypt and protect
Protect data in transit and at rest, sensitive data first.

04 Monitor and detect
Logging and alerting that can spot a breach in time to meet 72 hours.

05 Retain and erase
Retention rules, secure deletion and anonymization (Art. 4(7)).

06 Respond and prove
A tested breach plan, a rights workflow, and evidence ready for inspection.

ALREADY ON AN ISO/IEC 27001 JOURNEY?

Much of the technical track overlaps with controls you may already run. Mapping PDPL obligations onto an existing ISMS lets you reuse evidence rather than build a second programme.

From reading the law to proving compliance.

Spark works with organizations across privacy, data protection and cybersecurity, turning regulatory text into programmes that hold up under inspection.

PDPL gap assessment
Where you stand against the law and its regulations, and what to fix first.

Data mapping and records
Data inventories, flows, and the Art. 4 / Art. 5 records.

Licensing support
Identifying the authorizations you need and preparing the file.

Policies and notices
Privacy policies, consent wording, retention and breach procedures.

DPIA and risk
Assessing high-risk processing, sensitive data and transfers.

Awareness and training
Preparing staff and the DPO for day-to-day compliance.

BOOK A FREE CONSULTATION SESSION

Email us and our team will get back to you.

info@sparkps.com

www.sparkps.com

About this guide: general information based on the text of Law No. 151 of 2020 on the Protection of Personal Data. It is not legal advice and is not an official PDPC publication. Detailed procedures, fees and forms are set by the Executive Regulations (Ministerial Decree No. 816 of 2025) and PDPC decisions; confirm them with the PDPC and qualified counsel before acting.