ItQan
Advocates & Legal Consultants

A Practical Guide for Companies

Companies' Guide to Compliance with the Egyptian Personal Data Protection Law

Practical reading of Law No. 151 of 2020 and its Executive Regulations No. 816 of 2025

Prepared by ItQan - Advocates & Legal Consultants

2026 Edition

About this Guide

ItQan prepared this guide to help companies understand the practical requirements for compliance with the Egyptian Personal Data Protection Law and its Executive Regulations, from a corporate perspective that connects law, governance, technology and day-to-day operations.

The guide provides a practical and direct explanation of the key obligations and risks, with tables, checklists and starter templates that can be adapted to each company's business model and data environment.

Contents

Chapter 01

Why Companies Need This Guide

> Personal data protection is no longer a technical issue for IT only. It is a corporate obligation shared by management, legal, HR, marketing, sales and customer service.

The Core Idea

Egyptian Personal Data Protection Law No. 151 of 2020 and the Executive Regulations issued by Ministerial Decree No. 816 of 2025 establish a framework for the collection, processing, storage, transfer, disclosure and use of personal data, including for direct electronic marketing.

This guide does not aim to reproduce legal provisions. It translates them into operational steps that companies can apply internally.

Practical principle:
Any company that stores customer, employee, supplier or website user data may be subject to data protection obligations if that data is processed electronically, wholly or partially.

What changed after the Executive Regulations?

The Executive Regulations converted many general legal obligations into operational requirements: secure electronic registers, consent mechanisms, licences and permits, requirements for Data Protection Officers, breach response procedures, and controls for direct electronic marketing and cross-border data transfers.

Governance

Define roles and responsibilities internally.

Documentation

Maintain secure records for processing, consent and retention.

Response

Create a clear plan for requests, complaints and incidents.

Who is this guide for?

- Executive management that needs a clear view of legal and operational risk.
- Legal teams responsible for policies, contracts and notices.
- HR teams that handle employee and candidate data every day.
- Marketing and sales teams using email, WhatsApp, SMS and targeted advertising.
- IT and cybersecurity teams responsible for systems and information security.

Chapter 02

Scope of Application: Is Your Company Covered?

> The first step in any compliance programme is to determine whether the law applies to your business, and which data and operations fall within its scope.

The General Rule

The law applies to personal data processed electronically, whether wholly or partially, by any holder, controller or processor, in relation to natural persons.

> **Practical application:** If a company keeps customer data on a CRM system, employee files on an HR system, or job applications by email or through an online platform, it is usually carrying out electronic processing of personal data.

Examples of companies commonly within scope

Business type	Examples of data	Risk point
E-commerce	Names, addresses, phone numbers and order history	Marketing and disclosure to shipping/ payment providers
Service companies	Customer data, complaints, contracts and correspondence	Indefinite retention or sharing without a lawful basis
Clinics and medical centres	Health data, bookings and reports	Health data is sensitive personal data
Schools and education platforms	Student and parent data, test results	Children's data is treated as sensitive data
Marketing agencies	Prospect lists and user behaviour	Special rules for direct electronic marketing

Important Exclusions

The law excludes certain situations, such as purely personal use, some statistical or legal processing, data held by national security authorities, and certain data held by the Central Bank of Egypt and entities subject to its supervision, within the limits set by law.

Quick Diagnostic Question

> **Warning:** Exclusions should not be interpreted broadly. Merely operating in a regulated sector does not automatically place a company outside the data protection regime.

Quick diagnostic questions

1. Does the company collect data relating to natural persons?
2. Does it store or process that data electronically, even partially?
3. Is the data used for commercial, administrative, marketing or service purposes?
4. Is the data disclosed to a third party such as a payment provider, shipping company or cloud vendor?

If the answer to any of these questions is yes, the next step is to prepare an internal data map.

Chapter 03

Key Terms in Business Language

> Understanding the terminology determines legal responsibility: is the company a controller, processor, holder, or more than one of these at the same time?

Term	Practical meaning	Company example
Personal data	Any data relating to an identified or identifiable natural person.	Name, phone, email, image, ID number, IP address, employment data.
Sensitive data	Data requiring higher protection due to its nature or impact on the person.	Health, biometric, financial data, beliefs, political opinions, children's data.
Data subject	The person to whom the data relates.	Customer, employee, candidate, website user, individual supplier.
Controller	The party that determines why and how data is collected and processed.	A company collecting customer data to manage services and marketing.
Processor	A party processing data on behalf of a controller and under its instructions.	Cloud hosting provider, payroll company, call centre.
Holder	A party that legally or physically holds or keeps data.	Electronic archive or document storage provider.
Processing	Any electronic operation on data: collection, recording, storage, modification, analysis, disclosure, transfer or deletion.	Entering customer data into a CRM or sending a marketing campaign.

> **Practical note:** The same company may be a controller for its customers' data, a processor for another company's data, and a holder of archived information. Each processing activity should be assessed separately.

How to identify your role

- If you decide why data is collected and how it is used, you are likely a controller.
- If you only use data to provide a service for another party under its instructions, you are likely a processor.
- If you simply retain data without deciding the purpose or method of processing, you may be a holder.

Chapter 04

Principles and Conditions for Data Collection and Processing

> The law does not prevent companies from using data. It requires the use to be lawful, specific, transparent, secure and proportionate to the purpose.

Core legal conditions

Specific purpose

Data must be collected for lawful, specific and disclosed purposes.

Accuracy

Data should be accurate, valid and updated when necessary.

Proportionality

Do not collect more data than needed for the stated purpose.

Security and confidentiality

Adopt technical and organisational measures to protect data.

Limited retention

Do not keep data longer than needed.

No change of purpose

Do not use data for a new purpose without a proper legal basis.

Consent is not a formality

The Executive Regulations emphasise that consent must be linked to the purpose, and that it should be recorded in a secure electronic register showing the date, form, purpose and scope of use.

> **Common mistake:** Using a broad sentence such as “I agree to the use of my data” without specifying the purpose, or later using customer data for marketing without clear consent or another lawful basis.

What Should Be Documented?

What should be documented?

Item	What to document
Purpose	Why is the data collected? Service delivery, contract performance, recruitment, marketing, support.
Data categories	Identification data, financial data, health data, children's data, digital behaviour data.
Consent	Date, method, wording, and how consent can be withdrawn.
Retention period	The period or criteria used to determine retention for each category.
Third-party disclosure	Who receives the data, why, and under what legal basis?
Security measures	Access rights, encryption, backup, access monitoring and response plan.

Data Subject Rights and How Companies Should Handle Them

> Data subject rights are not theoretical. Companies need a mechanism to receive requests, respond to them and document the outcome.

Main rights

Awareness and knowledge

Knowing what data was collected and why.

Access

Enabling the person to access their data within legal limits.

Correction

Correcting inaccurate data or completing missing data.

Erasure

Deleting data when the purpose ends or consent is withdrawn in appropriate cases.

Objection

Objecting to processing that affects fundamental rights and freedoms.

Withdrawal of consent

Withdrawing previous consent where legally available.

Response deadline

The party receiving a request relating to the exercise of rights must respond within six working days from the date the request is submitted, in accordance with the law.

> **Recommended procedure:** Create a dedicated email address or online form for data protection requests, assign a reference number to each request, and maintain a register showing receipt date, request type, owner, response date and outcome.

Practical Workflow for Data Subject Requests

1. **Verify identity:** without requesting excessive data.
2. **Classify the request:** access, correction, erasure, objection, withdrawal of consent.
3. **Check the legal basis:** is there a mandatory retention period or legal obligation preventing erasure?
4. **Implement the decision:** across the relevant systems and notify third parties where required.
5. **Respond and document:** within the statutory timeframe and record the decision.

Chapter 06

Controller and Processor Obligations

> The law distinguishes between controllers and processors, but imposes independent obligations on each. Contracts and internal policies should reflect this distinction.

Controller obligations

Obligation	Practical translation inside the company
Obtain data on the basis of consent or legal basis	Clear consent forms and privacy notices.
Ensure data accuracy and adequacy	Review input fields and avoid unnecessary data.
Determine the method and criteria of processing	Internal policy identifying who uses data and why.
Adopt technical and organisational protection	Permissions, encryption, backups, training and access monitoring.
Erase data after the purpose ends	Retention schedule and periodic deletion or anonymisation.
Maintain a special data register	Processing register covering categories, recipients, transfers and security.
Obtain licence or permit from the Centre	Assess whether the activity requires a licence or permit under the Regulations.

Processor obligations

A processor should not treat the data as if it owns it. Processing must be carried out under a written contract and specific instructions from the controller, with obligations of protection, confidentiality and purpose limitation.

> **A data processing agreement is essential:** cloud vendors, marketing providers, payroll companies, call centres, hosting providers and technical support vendors should be governed by a contract covering purpose, duration, data type, security measures, breach notice, and deletion or return of data after service termination.

Essential Clauses in a Data Processing Agreement

Essential clauses in a processing agreement

- Description of the data and purpose of processing.
- Controller instructions and the processor's authority.
- Confidentiality obligations and access restrictions.
- Technical and organisational security measures.
- Immediate notification of any breach or suspected breach.
- Regulation of sub-processors.
- Return or deletion of data after the relationship ends.
- Audit, oversight and cooperation with the Personal Data Protection Centre.

Chapter 07

Personal Data Protection Officer

> The Data Protection Officer is the meeting point between law and operations: monitoring compliance, handling requests and complaints, and liaising with the Centre where required.

Legal and practical role

The law provides that the Data Protection Officer is responsible for implementing the law, its Executive Regulations and the decisions of the Centre, monitoring procedures within the entity, and receiving requests relating to personal data.

Compliance monitoring

Periodic review of policies, systems and procedures.

Contact point

Dealing with the Centre and responding to requests and reports.

Request management

Following up access, correction, erasure and objection requests.

Training

Raising employee awareness of data protection requirements.

Registration with the Centre

The Executive Regulations establish an electronic register for Data Protection Officers at the Centre. Each officer receives an identification code, subject to requirements such as qualifications or certificates, experience, approved testing, and absence of convictions for dishonesty or breach of trust offences.

Independence of the DPO

The DPO should not be a nominal appointment. The role requires sufficient authority to access information, review policies, issue recommendations and escalate risks to management.

> **Common mistake:** appointing an IT employee alone without legal or managerial empowerment, or assigning the role to a person whose duties conflict with independent oversight of data use.

Chapter 08

Sensitive Data and Children's Data

> Sensitive data requires heightened care and, in relevant cases, licence or permit requirements and explicit consent. It should not be handled like ordinary data.

What is sensitive data?

Sensitive data includes data revealing mental, psychological, physical or genetic health; biometric data; financial data; religious beliefs; political opinions; and security status. Children's data is treated as sensitive personal data in all cases.

Data	Why sensitive?	What the company should do
Employee medical reports	Relates to health	Restrict access to authorised HR and keep only for the necessary period.
Attendance fingerprint	Biometric data	Assess necessity and apply stronger technical protection.
Student or child data	Children's data	Obtain guardian consent and avoid excessive data collection.
Detailed financial data	Reveals financial status	Encrypt, restrict access and define the purpose precisely.

> **Golden rule:** Before collecting sensitive data, ask: is it necessary? Can the purpose be achieved with less data? Is there clear consent and a lawful basis? Do we need a licence or permit?

Children's data

Where children's data is processed, guardian consent may be required. A child's participation in a game, competition or activity should not be conditional on providing more data than necessary for participation.

Chapter 09

Direct Electronic Marketing

> Marketing is one of the highest-risk areas in data protection, especially when companies use phone, email or WhatsApp lists without documenting the data source and consent.

When are we dealing with direct electronic marketing?

When a company uses an electronic communication method to promote its own products or services or those of others, such as email, SMS, WhatsApp, notifications or similar digital channels.

Core obligations

- Obtain the required licence from the Centre for direct electronic marketing activities within the categories identified by the Executive Regulations.
- Obtain the data subject's explicit consent to receive the marketing communication.
- Do not use the data for another purpose or share it for other purposes without explicit consent.
- Maintain electronic records showing how and when consent was obtained and for what purpose.
- Provide a clear and easy opt-out or withdrawal mechanism.
- Erase the data upon withdrawal of consent, expiry of the retention period or loss of the marketing purpose.

Common risks: purchasing phone number databases, sending promotional messages to previous customers without separate marketing consent, or failing to provide a clear unsubscribe method.

Marketing Campaign Checklist

Checklist before any marketing campaign

☐ Do we know the source of the contact data?

☐ Is there clear consent to receive marketing communications?

☐ Is the campaign purpose consistent with the consent obtained?

☐ Is there a simple opt-out method?

☐ Are opt-outs automatically recorded?

☐ Are third-party agencies contractually bound as processors where applicable?

> **Recommended practice:** Keep a campaign compliance file for each campaign, including audience source, consent evidence, message copy, opt-out mechanism, vendor list and approval record.

Chapter 10

Cross-Border Data Transfers

> Cross-border transfer is not just a technical hosting issue. It includes sending, making available or storing personal data outside Egypt.

Why does it matter?

Many companies use foreign cloud providers, multinational HR platforms, overseas parent companies, outsourced support centres or global marketing tools. Each of these may involve an international transfer or access to personal data.

Typical situations

Scenario	Possible transfer issue
Hosting customer databases on a foreign cloud platform	Storage or access outside Egypt
Using a global HR system managed by the parent company	Employee data shared with a foreign group entity
Outsourcing customer support to a regional call centre	Disclosure of customer data abroad
Using global analytics and marketing tools	User behaviour data processed outside Egypt

Core point

Companies must assess whether the transfer is permitted under the law and the Executive Regulations, and whether a licence, permit, approval or specific safeguards are required.

Cross-Border Transfer Controls

Before transferring personal data outside Egypt

- Identify the data categories to be transferred.
- Identify the receiving country and recipient entity.
- Assess whether the recipient provides an adequate level of protection.
- Document the purpose and legal basis of transfer.
- Review whether the transfer requires a licence, permit or approval from the Centre.
- Sign a contract addressing confidentiality, security, onward transfers, breach notification, deletion and audit rights.

Common mistake: assuming that using a well-known cloud provider automatically makes the transfer compliant. The company remains responsible for assessing and documenting its compliance position.

Chapter 11

Personal Data Breaches

> A personal data breach should be treated as a legal, technical and management incident at the same time. Delay or poor documentation may increase liability.

What is a breach?

A breach may include unlawful or accidental destruction, loss, alteration, disclosure of, access to, or unavailability of personal data. It may result from cyber incidents, human error, misdirected emails, lost devices or unauthorised access.

Examples

Incident	Why it matters
Ransomware encrypting customer files	Loss of availability and possible unauthorised access
Emailing payroll data to the wrong recipient	Unauthorised disclosure of employee data
Loss of an unencrypted laptop	Possible access to personal data
Unauthorised CRM account access	Potential unlawful access and disclosure

Immediate response

- Contain the incident technically.
- Preserve evidence and logs.
- Assess the affected data categories and individuals.
- Evaluate the risk to data subjects.
- Prepare the required notifications and internal report.
- Document decisions and remedial action.

Breach Notification and Response Timeline

Notification logic

Companies should have a documented incident response plan that identifies who receives breach reports internally, who assesses legal notification requirements, and who communicates with the Centre and affected individuals where required.

Hour 0

Incident detected

First hours

Containment and evidence preservation

Within 72 hours

Assessment and notification to the Centre where legally required

Within 3 working days

Notify affected data subjects where required

Recommended incident file: incident description, discovery time, affected systems, affected data categories, number of individuals, containment measures, notification analysis, remedial actions and management approvals.

Chapter 12

Employee Data and Human Resources

> HR departments process some of the most sensitive and long-lived personal data in any company: recruitment, contracts, payroll, medical documents, attendance and investigations.

Common HR data

HR area	Examples	Compliance point
Recruitment	CVs, interviews, tests	Delete or archive according to a defined retention period.
Employment file	ID, contract, address, emergency contacts	Limit access and avoid unnecessary copies.
Payroll	Salary, bank data, deductions	Restrict access and use secure transmission.
Attendance	Time records, fingerprints	Assess necessity and apply security controls.
Disciplinary matters	Investigations and complaints	Confidentiality and need-to-know access.

HR checklist

- Review all employee data fields and remove unnecessary data.
- Set retention periods for candidates, employees and former employees.
- Restrict access to sensitive files.
- Document the legal basis for processing.
- Use written agreements with payroll, insurance, medical or outsourcing providers.

Chapter 13

Penalties and Risk Exposure

> The risk is not only financial. Non-compliance may create regulatory, contractual, reputational and operational exposure.

Main risk categories

Regulatory risk

Inspection, requests, licences, permits, corrective measures and penalties.

Contractual risk

Breach of client, vendor or group data protection obligations.

Reputational risk

Loss of customer trust following misuse or breach of data.

Operational risk

Business disruption, system shutdowns and remediation costs.

Management risk

Lack of governance may expose directors and senior management to criticism.

Litigation risk

Claims, complaints and evidence disputes following incidents.

Practical message

Compliance should not be viewed as a one-off policy. It is a governance programme involving mapping, policies, contracts, technology controls, training and periodic review.

Chapter 14

30-Day Compliance Roadmap

> A company does not need to solve everything in one day. A structured 30-day roadmap can create a clear starting point for management.

WEEK 1

Discover

Identify systems, data categories, purposes, departments and third parties.

WEEK 2

Assess

Classify roles, sensitive data, children's data, transfers, marketing and processors.

WEEK 3

Document

Prepare privacy notices, consent records, processing register, retention schedule and vendor clauses.

WEEK 4

Implement

Train teams, activate request channels, approve incident procedure and assign ownership.

Expected deliverables after 30 days

- Initial data map.
- Register of processing activities.
- Privacy notice and consent approach.
- Data subject request workflow.
- Breach response procedure.
- Initial vendor and processor review.
- Departmental compliance action list.

30-Day Roadmap - Management View

Management questions at the end of the first month

☐ Do we know what personal data we process and why?

☐ Do we know where data is stored and who can access it?

☐ Do we know which third parties receive or process data for us?

☐ Do we have a process for data subject requests?

☐ Do we have an incident response owner and timeline?

☐ Do we know whether any processing activity requires a licence, permit or approval?

Key point: The first month should create control and visibility. Full maturity comes through continuing reviews, audits, training and system improvements.

Chapter 15

Departmental Checklists

> Data protection works only when each department understands its role. The legal team cannot implement compliance alone.

Executive Management

- Approve data protection governance and owners.
- Allocate budget for legal, IT and training requirements.
- Review high-risk processing and breach reports.

Legal Department

- Review privacy notices, consent wording and policies.
- Prepare data processing agreements and vendor clauses.
- Assess licences, permits, cross-border transfers and marketing requirements.
- Maintain a legal register of key obligations.

Human Resources

- Review recruitment forms and employee files.
- Set retention periods for candidate and employee data.
- Restrict access to sensitive and medical information.
- Coordinate with payroll, insurance and medical providers.

Departmental Checklists - Continued

IT and Cybersecurity

- Map systems containing personal data.
- Implement access controls, logging, backups and encryption where appropriate.
- Support incident response and evidence preservation.
- Review cloud providers and technical vendors.

Marketing and Sales

- Document the source of marketing databases.
- Use separate consent for marketing where required.
- Maintain opt-out and suppression lists.
- Avoid sharing marketing data without proper basis and contract.

Customer Service

- Recognise data subject requests and route them internally.
- Avoid excessive identity verification.
- Record complaints and requests consistently.

Chapter 16

Starter Templates

> The following model clauses and registers are starting points only. They should be adapted to each company's actual processing activities.

Privacy Notice - basic structure

- Who we are and how to contact us.
- What personal data we collect.
- Why we process the data.
- Legal basis or consent approach.
- Who receives the data.
- Whether data is transferred outside Egypt.
- How long we retain data.
- Data subject rights and how to exercise them.
- How complaints and questions are handled.

Consent record - minimum fields

Field	Example
Data subject identifier	Customer ID or email
Consent text/version	Version 1.2 - marketing email consent
Purpose	Receiving marketing communications
Date and time	Timestamp
Method	Website form, email, signed form
Withdrawal method	Unsubscribe link or request email

Starter Templates - Continued

Processing register - suggested columns

Column	Purpose
Department	Owner of processing activity
Purpose	Why the data is used
Data categories	Customer, employee, supplier, user data
Sensitive data?	Yes/No and category
Recipients	Internal/external recipients
Transfer outside Egypt?	Country and recipient
Retention period	Period or retention criterion
Security measures	Access, encryption, backup, logging
Legal basis / consent	Applicable basis and evidence

Breach report - minimum content

- Incident description and discovery time.
- Systems and data categories affected.
- Estimated number of data subjects.
- Immediate containment steps.
- Risk assessment.
- Notification assessment and actions taken.
- Remediation plan and responsible owners.

Chapter 17

Legal Sources and Methodology

This guide is intended as a practical corporate compliance guide. It summarises key obligations and converts them into business actions.

Main legal sources

- Egyptian Personal Data Protection Law No. 151 of 2020.
- Executive Regulations issued by Ministerial Decree No. 816 of 2025.
- Relevant decisions, forms and guidance issued by the Personal Data Protection Centre once published and updated.

Methodology

The guide focuses on the practical impact of the law on companies, including governance, HR, marketing, IT, vendor management, breach response and cross-border data transfer issues. It is not intended to replace legal advice tailored to a specific case.

Important notice: Data protection compliance requires periodic updates. Companies should review their policies and procedures whenever new executive decisions, regulatory guidance or business changes occur.

ItQan
Advocates & Legal Consultants

Contact Us

For more professional legal guides and updates

www.itqanlaw.com

Facebook
Official ItQan Page

LinkedIn
Itqan Law Firm

X
@itqanlawfirm

WhatsApp
+20 105 050 3390

This guide is prepared for general awareness purposes and does not substitute tailored legal advice for any specific matter.