Data Protection in Egypt: Overview

by Ahmed El Sharkawy and Menna AbouZekry, Sharkawy & Sarhan Law Firm, with Practical Law Data Privacy Advisor

Country Q&A | Law stated as of 30-Sep-2020 | Egypt

A Q&A guide to data protection in Egypt.

This Q&A guide gives a high-level overview of the data protection laws, regulations, and principles in Egypt, including the main obligations and processing requirements for controllers, processors, or other third parties. It also covers data subject rights, the supervisory authority's enforcement powers, and potential sanctions and remedies. It briefly covers rules applicable to cookies and spam.

To compare answers across multiple jurisdictions, visit the Data Protection Country Q&A Tool.

Regulation

Legislation

1. What national laws regulate the collection, use, and disclosure of personal data?

General Laws

On February 24, 2020, the Egyptian Parliament passed Egypt's first comprehensive data protection law. The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) will take effect on October 15, 2020, three months after its July 15, 2020 publication in the Official Gazette (Preamble, Article 6, PDPL).

Sectoral Laws

Egyptian sectoral laws that address data protection include:

- The Banking Law (No. 88/2003), which requires that all bank customer accounts, deposits, trusts, safes, and their related dealings remain confidential, except with the written permission of:
    - the owner of the account, deposit, trust, or safe;

- the account owner's successors, including anyone to whom all or some of such funds have been bequeathed; or
- a legal representative or authorized attorney or under a judicial ruling or an arbitral award.

(Article 97, Banking Law.)

- The executive regulations of the Mortgage Finance Law (No. 148/2001) (both in Arabic), which require client data of mortgage finance companies related to the relationship to remain confidential.
- The Egyptian Civil Status Law (No. 143/1994) (in Arabic), which addresses the confidentiality of citizens' civil status data.
- The Egypt Telecommunication Regulation Law (No. 10/2003), which provides for telecommunications privacy and imposes penalties for breach of its regulations.

This Q&A focuses on the PDPL.

Scope of Legislation

2. To whom do the laws apply?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) applies to:

- Controllers. A controller means any natural person or legal entity who has, because of their activities, the right to obtain personal data and specify the method and criteria for retaining, processing, or controlling the personal data.
- Processors. A processor is any natural person or legal entity that processes personal data on the controller's behalf, under an agreement with the controller according to the controller's instructions.
- **Recipient**. A recipient is any natural person, legally or factually holding and retaining personal data in any manner, or by any means of storage, regardless of whether that person created or received the personal data.
- Data Subjects**.** A data subject is any natural person to whom electronically processed personal data relates which can or does identify the individual from any other person.

(Chapter 1, Article 1, PDPL.)

For more on:

- The definition of personal data, see Question 3.

- The PDPL's regulated activities, see Question 4.
- The PDPL's jurisdictional scope, see Question 5
- The PDPL's exemptions, see Question 6.

3. What personal data does the law regulate?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) defines personal data as any data relating to an identified natural person or a natural person who is identifiable, directly or indirectly, by reference to other identifiers such as:

- Name.
- Voice.
- Picture.
- Identification number.
- Online identifier.
- Psychological, physical, economic, cultural, or social factors.

(Chapter 1, Article 1, PDPL.)

The PDPL also defines sensitive data, which is discussed in Question 11.

4. What acts are regulated?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) regulates the following acts:

- Processing personal data and sensitive personal data, which includes any electronic or technological operation to write, collect, register, keep, store, merge, send, receive, supply, publish, erase, amend or retrieve personal data partly or fully and using any electronic or technological means (Chapters 1 to 3 and 5 to 6, PDPL; see Question 8, Question 11, and Question 17).
- Cross-border movement of personal data, which means to transfer, make available, record, store, circulate, publish, use, display, send, receive or retrieve personal data or process such data from inside the geographic

borders of Egypt to outside of those borders or vice versa (Chapter 7, PDPL; see Question 20 and Question 22).

- Electronic marketing, which means sending any message, statement, advertisement, or marketing content addressed to specific persons by any technological means to directly or indirectly promote goods, services, or commercial, political, social, or charitable petitions or requests (Chapter 8, PDPL; see Question 19).

5. What is the jurisdictional scope of the rules?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) applies to:

- Controllers, processors, and recipients that electronically process personal data regardless of where the processing takes place.
- Any person who commits a crime under the law, including:
  - Egyptians residing in Egypt or abroad;
  - non-Egyptians residing in Egypt; or
  - non-Egyptians residing abroad if the data relates to Egyptian citizens or foreign national residents and the crime is also punishable in the country where it occurred.

(Preamble, Article 1, PDPL.)

Controllers and processors outside of Egypt must appoint an Egyptian representative to communicate with the Personal Data Protection Center and data subjects on their behalf (Article 4(11), PDPL).

6. What are the main exemptions (if any)?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) does not apply to personal data:

- Processed by natural persons for personal use.
- Processed to obtain official statistical data or according to laws relevant to official statistical processing.

- Processed exclusively for media purposes when true and accurate and processed consistent with relevant laws.
- Relating to law enforcement records, investigations, and proceedings.
- Held by the National Security Authorities.
- Held by the Central Bank of Egypt and entities under its supervision.

(Preamble, Article 2, PDPL.)

Notification

7. Is notification or registration with a supervisory authority required before processing data?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) requires controllers and processors to obtain a license or permit from the Personal Data Protection Center (PDPC) before engaging in certain activities, for example:

- Processing, maintaining, storing, transferring, circulating, or making personal data available.
- Engaging in electronic marking activities.
- Processing personal data by associations, unions, or clubs.
- Processing sensitive personal data.
- Cross-border data transfers.

(Articles 26 and 27, PDPL.)

The PDPC will classify and determine the types of licenses and permits required and set the conditions for each under the PDPL's Executive Regulations. The Executive Regulations, which the PDPC has not yet issued, will set the procedures and fees for obtaining a license or permit. (Article 26, PDPL.)

For more information on the PDPC, see Question 25 and Regulator Details.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) requires controllers to:

- Only process personal data for specified and legitimate purposes notified to the data subject, and only after obtaining the data subject's consent unless an exception permits processing without consent (Articles 3(1), 4(1), and 6(1), PDPL; see Question 9).
- Only process personal data for the purposes for which it was collected (Articles 3(3) and 4(2), (3), PDPL).
- Only collect personal data relevant to the designated purpose (Article 4(4), PDPL).
- Ensure the accuracy of personal data and rectify any errors in the personal data (Articles 3(2) and 4(8), PDPL).
- Erase personal data when no longer necessary for the collection purpose. If a controller retains personal data for a legitimate reason after the collection purpose no longer applies, it must retain the personal data in a form that does not allow for data subject identification. (Articles 3(4) and 4(7), PDPL.)
- Implement technical and regulatory measures to protect and secure the personal data in their possession, maintain its confidentiality, and avoid a personal data breach or unauthorized erasure, alteration, or manipulation of the personal data (Article 4(6), PDPL).
- Be able to prove PDPL compliance and allow the Personal Data Protection Center (PDPC) to perform inspections and supervision to ensure compliance (Article 4(12), PDPL).
- Obtain a license or permit from the PDPC to handle personal data in certain circumstances (Article 4(10), PDPL; see Question 7).
- Create a personal data register that includes:
    - a description of the categories of personal data;
    - personal data recipients and the basis for disclosure;
    - the duration, restriction, and scope of disclosure;
    - the mechanism for erasing or editing the personal data;
    - information on cross-border transfers; and
    - a description of the technical and regulatory measures securing the personal data.

    (Article 4(9), PDPL.)
- Obtain the data subject's explicit written consent before processing sensitive personal data if the basis for the processing is the data subject's consent (Article 12, PDPL; see Question 11).

- Comply with requirements for disclosing personal data and transferring personal data cross border (Articles 4(5) and 14 to 16, PDPL; see Question 20).
- Appoint a representative in Egypt if located outside of Egypt (Article 4(11), PDPL).
- Appoint, announce, and register a data protection officer with the PDPC (Article 8, PDPL).
- Facilitate the exercise of data subjects' rights (Article 10, PDPL; see Question 13).
- Notify the PDPC and data subjects in the event of a personal data breach (Article 7, PDPL; see Question 16).
- Obtain the data subject's consent before sending electronic marketing communications and allow data subjects to easily withdraw consent (Article 17, PDPL; see Question 19).

9. Is the consent of data subjects required before processing personal data?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) sets out four lawful bases for processing personal data. One of those bases is obtaining the data subject's consent to process personal data for one or more designated purposes. (Article 6, PDPL). The PDPL requires consent to be explicit.

The PDPL also requires controllers to obtain:

- Data subject consent before:
  - transferring personal data to a country that does not offer the same level of personal data protection as the PDPL (Article 15, PDPL; see Question 20); and
  - sending electronic marketing communications (Article 17, PDPL; see Question 19).
- Explicit written consent from the data subject before processing sensitive personal data (Article 12, PDPL; see Question 11).

All personal data relating to children is considered sensitive personal data under the PDPL (Chapter 1, Article 1, PDPL). Before processing personal data of a child under 16, controllers must obtain explicit, written consent from the child's legal guardian (Article 12, PDPL; see Question 11).

For more on other legal bases for processing, see Question 10.

10. If consent is not given, on what other grounds (if any) can processing be justified?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) permits personal data processing without the data subject's consent if at least one of the following applies:

- The processing is necessary and essential to:
  - perform a contractual obligation;
  - take legal action;
  - execute an agreement for the data subject's benefit; or
  - undertake any procedure to assert or defend the data subject's legal rights.
- The processing is:
  - to perform an obligation regulated by law,
  - to comply with an order issued by competent investigation authorities; or
  - based on a court judgement.
- The processing enables the controller to perform its obligations or any relevant individuals to exercise their legitimate rights, unless the processing conflicts with the data subject's basic rights and freedoms.

(Article 6, PDPL.)

For information on:

- Controllers' other main obligations, see Question 8.
- Consent as a legal basis to process personal data, see Question 9.
- When controllers may execute cross-border transfers without a data subject's consent, see Question 20.

Special Rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) defines sensitive data as personal data that reveals the data subject's:

- Mental, psychological, or physical health.
- Genetic information.
- Biometric information.
- Financial information.
- Religious beliefs.
- Political opinions.
- Criminal records.
- Security status.

(Article 1, PDPL.)

The PDPL also includes all children's personal data in the definition of sensitive data (Article 1, PDPL).

The PDPL prohibits a controller or processor from collecting, transferring, storing, saving, processing, or making available sensitive data without first obtaining a license from the Personal Data Protection Center and satisfying one of the following:

- The controller or processor obtains the explicit written consent of:
    - the data subject; or
    - the data subject's legal guardian for data subjects under 16.
- The processing is necessary and essential to:
    - perform a contractual obligation;
    - take legal action;
    - execute an agreement for the data subject's benefit; or
    - undertake any procedure to assert or defend the data subject's legal rights.
- The processing is:
    - to perform an obligation regulated by law,
    - to comply with an order issued by competent investigation authorities; or
    - based on a court judgement.
- The processing enables the controller to perform its obligations or any relevant individuals to exercise their legitimate rights, unless the processing conflicts with the data subject's basic rights and freedoms.

(Articles 6 and 12, PDPL.)

An organization's data protection officer must supervise its controllers', processors', and affiliates' compliance with security policies and procedures to protect sensitive data (Article 13, PDPL.)

For more on the legal bases to process non-sensitive personal data, see Question 9 and Question 10.

Rights of Individuals

12. What information rights do data subjects have?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) requires controllers to provide data subjects with notice, at the time of collection, about the specific and legitimate purposes for personal data collection (Article 3(1), PDPL). Data subjects also have the right to know what personal data any controller, processor, or recipient holds about them (Article 2(1), PDPL; see Question 13).

For more on other data subject rights, see Question 13.

13. Other than information rights, what other specific rights are granted to data subjects?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) grants the following rights to data subjects:

- The right to access, review, and obtain their personal data from any controller, processor, or recipient (Article 2(1), PDPL).
- The right to withdraw consent for retaining or processing their personal data (Article 2(2), PDPL).
- The right to rectify, edit, erase, add to, or update their personal data (Article 2(3), PDPL).
- The right to limit the processing of their personal data (Article 2(4), PDPL).
- The right to be informed about any data breach involving their personal data (Article 2(5), PDPL).
- The right to object to personal data processing, or the results of processing, if it conflicts with their principal rights and liberties (Article 2(6), PDPL).
- The right to submit a complaint to the Personal Data Protection Center regarding a controller, processor, or recipient that impedes their rights (Article 33(2), PDPL).

The PDPL requires the following for data subject requests:

- The data subject must make the request in writing to the controller, processor, or recipient.
- The controller, processor, or recipient must verify and retain the documents submitted by the data subject.
- The controller, processor, or recipient must decide within six working days of the data subject's request, or the request is deemed rejected.
- If the controller, processor, or recipient rejects a data subject's request, it must justify its decision.

(Article 10, PDPL.)

For more on data subject information rights, see Question 12.

14. Do data subjects have a right to request the deletion of their data?

See Question 13.

Security Requirements

15. What security requirements are imposed in relation to personal data?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) requires controllers to take all technical and regulatory measures necessary to:

- Protect and secure personal data and maintain its confidentiality.
- Prevent a personal data breach.
- Prevent unauthorized data erasure, alteration, or manipulation.

(Article 4(6), PDPL.)

Processors must similarly protect and secure their processing activities, media, and devices, as well as the personal data processed (Article 5(7), PDPL).

An organization's data protection officer must supervise its controllers', processors', and affiliates' compliance with security policies and procedures to protect sensitive data (Article 13, PDPL).

For more on sensitive data, see Question 11.

16. Is there a requirement to notify data subjects or the supervisory authority about personal data security breaches?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) defines a data breach as any:

- Unauthorized or illegal access to personal data.
- Illegitimate operation to:
    - disclose or reveal personal data by reproducing, sending, distributing, exchanging, transferring, or circulating it; or
    - modify or damage personal data during storage, transfer, or processing.

(Chapter 1, Article 1, PDPL.)

The PDPL requires controllers and processors to inform the Personal Data Protection Center (PDPC) of a personal data breach within 72 hours of discovery, or immediately if the breach relates to national security, and provide the following information:

- The nature and form of the breach.
- The causes of the breach.
- The approximate number of affected data subjects.
- The categories of breached personal data.
- The data protection officer's information.
- The potential consequences of the breach.
- The proposed or completed remedial actions.
- Any additional information that the PDPC requests.

(Article 7, PDPL.)

Within three working days of notification to the PDPC, the controller or processor must notify the data subjects of the breach and its remedial measures (Article 7, PDPL).

For a chart of global data breach notification requirements, see Practice Note, Global Data Breach Notification Laws Chart: Overview.

Processing by Third Parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) requires processors to:

- Process personal data according to the PDPL, its Executive Regulations, and the controller's or the Personal Data Protection Center's (PDPC) written instructions on the processing's scope, subject, nature, and designated purpose.
- Process personal data in a legitimate manner, for a legitimate purpose, and consistent with public order and morals.
- Process personal data only for the designated purpose and necessary duration.
- Erase personal data on delivery to the controller or at the end of the processing's necessary duration.
- Obtain the controller's prior written approval before involving another processor.
- Process personal data only for the controller's designated purpose, unless the additional processing is for a statistical or educational purpose or is not for profit. Processing for these purposes must:
    - not impede the right to privacy; and
    - use encrypted personal data.
- Protect and secure processing activities, media, devices, and the related personal data.
- Refrain from directly or indirectly damaging the data subject.
- Maintain a processing record that includes the processing's categories, duration, restrictions, scope, erasing and editing mechanisms, security measures, and the processor's and data protection officer's contact details.
- Be able to demonstrate compliance with the PDPL on the controller's or PDPC's request and allow the PDPC to conduct inspections or supervision to ensure compliance.
- Obtain a license or permit from the PDPC to process personal data.
- Appoint a representative in Egypt if the processor is outside Egypt.

(Article 5, PDPL.)

The PDPL holds processors directly responsible for violations and subjects them to fines and penalties (see Question 26).

For more on controllers' main obligations, Question 8.

Electronic Communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) does not directly address the storage of cookies or equivalent devices on a data subject's terminal equipment. However, the PDPL applies to cookies if they can be used to directly or indirectly identify a data subject, in which case they are considered personal data under the PDPL (Article 1, PDPL).

19. What rules regulate sending commercial or direct marketing communications?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) prohibits direct electronic marketing to data subjects unless the sender:

- Obtains the data subject's consent.
- Includes the creator's and sender's identities in the communication.
- Maintains a valid contact address.
- Indicates the communication's direct marketing purpose.
- Offers a clear and simple mechanism for the data subject to opt out or withdraw consent.

(Article 17, PDPL.)

Under the PDPL, senders of electronic marketing communication must also:

- Specify a defined marketing purpose.
- Keep data subjects' contact details confidential.

- Maintain electronic registers of data subjects' consent or non-objection to receiving electronic marketing communications for three years after the last communication.

(Article 18, PDPL.)

International Transfer of Data

Transfer of Data Outside the Jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) prohibits transferring, storing, or sharing personal data outside of Egypt unless the controller or processor obtains a license from the Personal Data Protection Center (PDPC) and the destination country guarantees at least the same level of data protection as the PDPL or another exception applies (Articles 14 and 16, PDPL).

For example, the PDPL permits controllers and processors to transfer personal data to countries that do not provide the same level of data protection as Egypt if they obtain the data subject's explicit consent and the transfer, storage, or sharing fulfills one of the following purposes:

- To protect the data subject’s life, or to provide medical care, treatment, or the administration of medical services to the data subject.
- To prove, exercise, or defend a judicial right.
- To execute or perform a contract between the controller or processor and a third party for the data subject's benefit.
- To perform a procedure relating to international judicial cooperation.
- To protect the public interest as necessary or required by law.
- To complete a banking transfer.
- To comply with a bilateral or multilateral agreement to which Egypt is a party.

(Article 15, PDPL.)

The controller or processor must also obtain a license from the PDPC, after which time they can transfer, store, or share personal data outside of Egypt if:

- The nature of processing by each controller or processor is consistent with the purposes of use.

- Each controller or processor, or the data subject, has a legitimate interest in the personal data processing.
- The foreign controller or processor uses legal and technical protections that provide the same level of protection required in Egypt.

(Article 16, PDPL.)

21. Is there a requirement to store any type of personal data inside the jurisdiction?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) does not require organizations to store personal data inside Egypt. Sectoral laws may have data localization requirements, but they are beyond the scope of this Q&A.

For more information on rules regulating data transfers, see Question 20.

Data Transfer Agreements

22. Are data transfer agreements contemplated or in use? Has the supervisory authority approved any standard forms or precedents for cross-border transfers?

The Personal Data Protection Law (No. 151/2020) (in Arabic) does not require using a data transfer agreement for cross-border transfers, and the Personal Data Protection Center is not yet established.

23. For cross-border transfers, is a data transfer agreement sufficient, by itself, to legitimize transfer?

See Question 20 and Question 22.

24. Must the relevant supervisory authority approve the data transfer agreement for cross-border transfers?

See Question 22.

Enforcement and Sanctions

25. What are the enforcement powers of the supervisory authority?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) establishes the Personal Data Protection Center (PDPC) as the authority responsible for personal data protection and processing in Egypt (Article 19, PDPL). The PDPC's rights and responsibilities include, among others:

- Setting, developing, and executing policies, programs, and strategic plans to protect personal data.
- Unifying policies and plans to secure and process personal data.
- Setting and applying decisions, regulations, precautions, procedures, and criteria related to personal data protection.
- Setting a guidance framework for codes of conduct for personal data protection and approving entities' codes of conduct.
- Organizing, cooperating, and communicating with government and non-government entities on personal data protection initiatives.
- Issuing licenses, permits, and certifications under the PDPL.
- Establishing and regulating a data protection officer register.
- Receiving and investigating complaints and reports related to the PDPL and issuing decisions.
- Commenting on various draft laws and international agreements that regulate or relate to personal data.
- Verifying and rendering decisions on cross-border personal data transfers.
- Providing expertise and advice on personal data protection, particularly to investigative authorities and the judiciary.
- Entering into agreements and memorandums of understanding and coordinating, cooperating, and exchanging knowledge with similar international entities.
- Preparing and issuing an annual status report on personal data protection in Egypt.

(Article 19, PDPL.)

The PDPL gives the PDPC's board of directors the power to take any action necessary to further the purposes of the PDPC, the PDPL, and its regulations, including:

- Adopting policies, strategic plans, and programs for personal data protection.
- Approving the regulations, controls, measures, and standards for personal data protection.
- Activating diverse international cooperation plans, treaties, and protocols and exchanging knowledge with international entities and organizations.

(Article 21, PDPL.)

26. What are the sanctions and remedies for non-compliance with data protection laws?

The Personal Data Protection Law (No. 151/2020) (in Arabic) (PDPL) permits the Personal Data Protection Center (PDPC) to issue the following administrative sanctions for non-compliance:

- Warnings with a grace period to remedy any violations.
- Warnings regarding partial or total suspension of a license, permit, or certification.
- Partial or total suspension or cancellation of a license, permit, or certification.
- Publication of the violations in one or more major media outlets at the violator's expense.
- Technical supervision by the PDPC at the controller or processor's cost.

(Article 30, PDPL.)

The PDPL provides for additional criminal sanctions for non-compliance, including:

- Fines from EGP50,000 to EGP5 million.
- Imprisonment for at least three or six months to three years.

(Articles 37, 42, 43, and 47, PDPL.)

Data subjects and other relevant persons may submit a complaint to the PDPC for rights violations under the PDPL (Article 33, PDPL). They also may pursue their rights under the general rules of tort liability.

Regulator Details

W https://www.itida.gov.eg/English/

Description. The Personal Data Protection Center (PDPC), once established, will be the regulator for the Data Protection in Egypt. The PDPC will be under the jurisdiction of the Ministry of Information Technology.

Online Resources

W www.cc.gov.eg

Description. The official website for the Egyptian Court of Cassation, which sometimes provides updates on the laws and regulations in Egypt. Any English versions of the laws and regulations are nonbinding.

W https://www.itida.gov.eg/English/

Description. The official website of the Information Technology Industry Development Agency, the executive IT arm of the Ministry of Communications and Information Technology.

W http://www.mcit.gov.eg/

Description. The official website of the Ministry of Communications and Information Technology, which proposed the Personal Data Protection Law.

Contributor Profiles

Ahmed El Sharkawy, Partner

Sharkawy & Sarhan Law Firm
T +(202) 23 22 54 00 Ext. 101

E: a.sharkawy@sharkawylaw.com

W www.sharkawylaw.com

Professional qualifications. Egypt, Attorney, 1999

Areas of practice. Technology, data protection & cybersecurity, PPPs, public tenders, corporate & commercial.

Menna AbouZekry, Attorney at law

Sharkawy & Sarhan Law Firm
T +(202) 23 22 54 00

E m.abouzekry@sharkawylaw.com

W www.sharkawylaw.com

Professional qualifications. Egypt, Attorney, 2019

Areas of practice. Data protection & cybersecurity, corporate & commercial.

END OF DOCUMENT