COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Morocco

DATA PROTECTION & CYBER SECURITY LAW

Contributing firm

DLA Piper

Mehdi Kettani

Head of IPT – Morocco | mehdi.kettani@dlapiper.com

This country-specific Q&A provides an overview of data protection & cyber security law laws and regulations applicable in Morocco.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

MOROCCO
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

The fundamental right to privacy is contained in Article 24 of the Constitution of 2011, which provides:

"Everyone has the right to the protection of his or her private life. The home is inviolable.

Searches may only be carried out under the terms and in the ways provided by the law. Private communications, in all their forms, are secret. Only the courts may authorize, under the conditions and in the forms provided for by the law, access to their contents, their total or partial disclosure or their invocation at the expense of any person.

Freedom of circulation and establishment within the national territory, and freedom to leave and return to it, in accordance with the law, shall be ensured to all".

The Constitution affirms the principle of the right to protection of privacy and seeks to protect the rights of individuals with regard to their personal information.

Furthermore, the Constitution has established the supremacy of ratified international conventions and imposes the respect thereof at the national level.

The Moroccan legislature has established a system of legal protection for personal data by adopting the following laws:

- Law no. 09-08 on personal data protection and its implementing Decree no. 1-09-15);
- Law no. 31-08 on consumer protection (online advertising and spamming);
- Law No. 07-03 supplementing the penal code regarding the repression of offenses relating to automated data processing systems;
- Law no. 34-05 amending and supplementing Law 2-00 relating to copyright and neighboring rights;
- Law no. 05-20 on cybersecurity.

In Morocco, the collection and processing of personal data is governed by the Law no. 09-08 on personal data protection and its implementing Decree No. 1-09-15 (the "Data Protection Law").

Data Protection Law regulates automatic and some manual processing of personal data and sensitive personal data. Processing of personal data means any operation or set of operations performed by automatic or non-automatic means and that forms part of a filing system.

The Data Protection Law regulates the collection and processing of personal data of individuals in Morocco (referred as "data subjects" in the following Q&A) and does not protect legal persons such as limited liability companies and private limited companies.

The National Control Commission for the Protection of Personal Data (Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel) (the "CNDP") is responsible for enforcing the Data Protection Law and has also issued several binding decisions on personal data processing for different purposes.

No announced changes in the data protection and privacy law for now. This being said, it is possible that a reform of the data protection and privacy law takes place in the near future, to implement GDPR like regulations.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

The data controller should take a number of measures to comply with the requirements of Data Protection Law. To ensure compliance with these requirements, the data controller should inter alia declare or obtain authorisation from the CNDP, prior to the processing of the data.

Indeed, Data Protection Law requires controllers to obtain prior authorization from the CNDP before processing:

- sensitive personal data;
- data for purposes other than those for which it was collected;
- genetic data not used by health workers for medical purposes, whether for preventive medicine, diagnosis, or care;
- personal data involving offenses, convictions, or security measures not used by court officers;
- the identification card number of the data subject; or
- interconnected files belonging to legal persons with different main purposes or one or more legal persons managing public services with different public interest purposes.

In the circumstances not subject to a prior authorization and in particular which do not involve the processing of above-mentioned data, a declaration (notification) to the CNDP is required before processing personal data.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The Data Protection Law defines personal data as information of any kind relating to an identified or identifiable natural person, regardless of its form, including sound and images. An identifiable person is one that can be identified directly or indirectly, especially by reference to (i) an identification number and (ii) one or more specific elements of the person's physical, physiological, genetic, psychological, economic, cultural, or social identity.

Thus, sensitive personal data includes personal data revealing a natural person's (i) racial or ethnic origin, (ii) political opinions, (iii) religious and philosophical beliefs, (iv) trade union membership, and (v) health data, including genetic data.

4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The personal data must be treated fairly and lawfully by providing a list of information about the circumstances in which the data controller collects personal data, such as the categories of recipients of the personal data, whether providing the personal data is obligatory or voluntary, the possible consequences of the failure to provide personal data and the existence of the rights to access and rectify collected personal data.

Moreover, the personal data must be collected for specific, explicit and legitimate purposes which means that the controller must ensure to collect data for purposes determined by Data Protection Law (i.e to comply with a legal obligation, perform a contract with the data subject, etc.)

The retention of personal data is limited by the purposes of the processing. Once the purposes are reached, data may not kept by the controller.

The collection of the personal data must also be adequate, relevant and not excessive. The controller has to ensure to collect the personal data required for the purpose of the processing in question.

The personal data must be accurate and necessary and kept up to date. All necessary measures must be ensured that data which are inaccurate or incomplete, with regard to the purposes of their collection and further processing, are erased or rectified.

Where the data controller is established outside of Moroccan territory, it must designate a local reprersentative.

Finally, the personal data must be kept in a form enabling the person concerned to be identified and for a specified period, which means that the personal data must be encrypted and anonymized.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

As a principle, the Data Protection Law requires data controller to obtain the consent of the data subjects before processing their personal data unless an exception applies (as mentioned below).

The data subject must give his consent for the processing of his personal data, freely, specifically and in an informed manner.

However, controllers are allowed to process personal data without data subject consent in the following circumstances:

- To comply with legal obligation to which the data subject or controller is subject.
- To perform a contract with the data subject or pre-contractual measures at the request of the data subject.
- To protect the vital interests of the data subject, if the data subject is physically or legally incapable of giving consent.
- To perform a task carried out in the public interest, or in the exercise of the official authority vested in the data controller or a third party to whom the personal data is disclosed.
- To pursue the data controller's or a third party's legitimate interests, unless the interest of the data subject or fundamental rights and freedom prevail.

6. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The Data Protection Law does not specify rules relating to the form of the consent, but it must leave no doubt regarding the data subject's intent to consent (i.e : in the case of the obtention of data subject's electronically, the consent may be sufficient if it meets all the requirements set by Data Protection Law).

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

The data controller must obtain the express consent of the data subjects before processing their sensitive personal data.

Moreover, the controller is required to obtain a prior authorization before processing sensitive personal data.

Finally, the controller is required to ensure the respect of special security requirements when processing sensitive or health-related data.

8. How do the laws in your jurisdiction address children's personal data or PII?

Moroccan law does not impose any special requirements for the processing of children's personal data.

9. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

Data Protection Law includes derogations to its scope, exclusions to the information obligation and the necessary obtention of the data subjects' consent requirements and the limitation to data subjects right to object. Firstly, the Data Protection Law established the personal data processing that fall outside its scope including:

- Processing by a natural person for exclusively personal or domestic activities; Processing concerning public security, defence, and state security;
- Processing authorized under another law;
- Collection and processing to prevent crime in accordance with applicable legal conditions. However, the controller must notify to the CNDP his identity, the basis for processing, the purpose for processing, the category or categories of data subjects and the categories of personal data relating to the data subjects, the origin of the collected personal data, third parties to whom the data may be communicated, and the measures taken to ensure the security of the processing.

In addition to the exclusions mentioned in the question 5 above, the controllers are not required to provide

information about the personal data processing to data subjects when :

1. the processing is necessary for national defence, internal or external state security, or crime prevention;
2. it is impossible for the controller to provide information, particularly in cases of personal data processing for statistical, historical, or scientific purposes. The controller must notify the CNDP about the impossibility to provide information and the reasons why it is impossible;
3. The Moroccan law expressly authorizes the personal data recording or disclosure.
4. The processing is solely for journalistic, artistic, or literary purposes.

Finally, the Data Protection Law provides limitations regarding the data subjects right to object, particularly to the processing is based on a legal requirement or in case that the right to object cannot be exercised because of the Data Protection Law allowing for the processing and also for unjustified objections. Indeed, to exercise their right to object, the data subjects should justify that they have legitimate reasons to object to the processing.

In practice, the CNDP usually requires the data controller to justify the data subjects consent even for the situations excluded by the Data Protection Law.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

The Data Protection Law does not mention any of the privacy by design and privacy by default. However, on 26 March 2020, the CNDP published a press release alerting actors concerned by the Data Protection Law's compliance to the principles of "Privacy by Design" in order to ensure compliance at the earliest possible stage rather than waiting for the final phases of their projects.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

The controller is not required to establish an internal register, as required in Europe by the General Data Protection Regulation (GDPR). However, it is recommended that the controller maintain a record of the carried data processing and establish an internal data processing policies to enable its employees to monitor the use and processing of personal data as well as to inform them about their obligations with regard to the data subjects' personal data processing that the company hold.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

The data controller is not required to put in place data retention and disposal policies and procedures. This being said, it is recommended to put in place such policies to set unified standards in terms of how long may the data be retained (e.g. after an employee leaves the company) and how may the data be disposed.

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

The Data Protection Law does not provide any requirements to consult the CNDP, but it is recommended when the controller meet difficulties to ensure his compliance with the legal requirements. However, the CNDP could be consulted by the data subjects and by any institution directly or indirectly concerned by the Data Protection Law.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The CNDP released on 14 December 2020 a Deliberation No. D-188-2020 relating to the risk assessment regarding data processing activities. According to the Deliberation No. D-188-2020 the following data processing activities are concerned by the risk assessment:

- Data processing activities which allow the decision-making on the basis of automated processing of personal data;
- Data processing activities involving large-scale processing of sensitive data;
- Data processing activities which allow systematic monitoring of data subjects;
- Data processing activities carried out in the context of the use of technological solutions or innovative organizational solution;
- Data processing activities carried out in compliance with legal obligations;
- Data processing activities carried out in the context of performing a public interest mission; and
- Data processing activities carried out on the basis of legal provisions.

An impact analysis must be carried out before the implementation of the contemplated data protection activity and must be regularly reviewed in order to ensure that the level of risk remains acceptable.

The risk assessment may relate to one (1) data processing activity or to a set of similar data processing activities and must contain at least:

- a detailed description of the data processing activities and their purposes, including both technical and operational aspects;
- a legal assessment on the necessity and proportionality of the data processing activities with regard to fundamental principles and rights (purpose, collected data and retention periods, rights of data subjects, etc.) that are set by law and must be observed whatever the risks are;
- a technical assessment of data security risks (confidentiality, integrity and availability), and their possible impacts on privacy, in order to specify the necessary technical and organizational measures to ensure the protection of personal data;
- a description of the contemplated measures to deal with the risks (legal measures, organizational measures, logical security and physical security measures), including the guarantees and mechanisms aiming to ensure the protection of personal data and compliance with laws requirements.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

No DPO appointment is required.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

No training is required or recommended. This being said, employees act under the company's responsibility, making the training very much recommended.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

The Data Protection Law requires businesses (controllers) to provide data subjects with a notice including the following information in the documents serving the collection of personal data:

- The identity of the controller or the controller's representative;
- The purpose of the processing;
- Any additional information, such as:
    - The recipients or categories of the data processed;
    - If providing the data is obligatory or voluntary;
    - The possible consequences of a failure to provide the data;
- The existence of the right of access and the right to rectify the data;
- Information about the receipt delivered by the CNDP after the declaration or request for authorization for personal data processing.

It should be noted that the notice must be delivered before collecting the data subject's personal data.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically

only apply through flow-down contractual requirements from the owners/controller?)

The Data Protection Law drew a distinction between the controllers and the processors of personal data, in particular in terms of their obligations. The controller is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by laws or regulations, the controller must be indicated in the law governing the organization and operation or in the statute of the entity legally or statutorily competent to process the personal data in question. However, the processor is defined as the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller, which means that the processor should only act under the instructions of the controller. The processor is bound by the obligations of confidentiality and security of the data processing activities pursuant to the contract governing the relationship between the controller and the processor.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

When data processing is conducted by a processor on behalf of the controller, the controller must choose a processor providing sufficient guarantees in respect of the technical and organizational security measures relating to the processing activities. The controller must ensure the compliance with those measures by the processor.

Furthermore, the Data Protection Law requires that the performance of the processing by a processor must be governed by a contract or legal act legally binding the processor to the controller. The contract must provide in particularly that the processor shall act solely on the instructions of the controller and that the obligations of security and confidentiality laid down by the applicable law as described below and by which the controller is bound shall be incumbent on the processor.

The Data Protection Law requires controllers to implement technical and organizational measures to protect personal data against (1) the accidental or unlawful destruction, (2) the accidental loss, alteration, disclosure, or unauthorized access and (3) all the other unlawful forms of processing, especially when the processing involves data transmission in a network. Such requirements must be duplicated in the contract the processor in order to have the processor to comply with these obligations. Moreover, sensitive or health-related data processing are subject to additional security measures. In particular, the controller has to:

- Deny unauthorized persons to access to the facilities used for data processing (facilities access control) ;
- Prevent unauthorized reading, copying, modification, or removal of data media (data media control);
- Prevent unauthorized input of the data and unauthorized inspection, modification, or deletion of stored data (storage control);
- Prevent the use of automated data processing systems by unauthorized persons using data communication equipment (user control);
- Ensure that persons authorized to use an automated data processing system have access only to the data covered by their access authorization by means of individual and unique user identities and confidential access modes (data access control);
- Verify the entities to which they transfer data using data transmission facilities (transmission control);
- Ensure it is possible to verify afterward, within an appropriate timeframe based on the sector, what data was introduced, when it was introduced, and by whom (introduction control);
- Prevent unauthorized reading, copying, modification, or deletion of the data during transfer or transport (transport control).

When entering into a contract with a processor, the controller must make sure that the contract contains provisions triggering the processor’s responsibility in case the above obligations are not respected

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

The Data Protection Law has not provided any specific definition of the monitoring or profiling of the data subjects.

However, an opt-in consent is required for both monitoring or profiling and the use of tracking technologies such as cookies.

Data Protection Law provides that the data subjects are entitled to access and knowledge of the logic behind any automated processing of personal data concerning them, which could consequently result in a profiling.

Furthermore, in its guidelines on the compliance with the Data Protection Law of Web sites, the CNDP requires controllers collecting personal data by means of cookies to collect the consent of the Internet user, and that the controller are required to provide information about the purposes of the use of cookies and the means of opposing to their collection.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

Cross-contextual behavioral advertising is not regulated per se by the Data Protection regulations. This being said, since it involves sharing and cross-processing of personal data, it would be subject to the authorization of the CNDP, which would automatically refuse to provide the requested authorization. Therefore, it would practically not be possible to be compliant with data protection regulations.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is "sale" or related terms defined and what restrictions are imposed, if any?

The sale of personal data would be considered as a purpose of the processing. Such processing would be subject to the prior authorization of the CNDP, which would automatically refuse to provide the requested authorization.

Therefore, while it is not regulated per se, it would practically not be possible to sell personal data and be compliant with data protection regulations at the same time.

23. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Provided that the prior consent of the data subject to receive marketing messages is given and that this processing has been previously declared to the CNDP, the data controller is allowed to send direct prospecting messages.

However, prior consent is not required for direct prospecting through the various forms of electronic messages (i) if the contact details were collected directly from the person concerned on the basis of a previous sale of products or services related to the products or services included in the prospecting message and (ii) if the recipient has the possibility of opposing, at no cost, to receive direct prospecting e-mail, is not included the cost of transmitting the refusal to use his contact details.

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

The Data Protection Law defined biometric data as personal data and distinguishes between genetic data and biometric data. Genetic data is defined as sensitive data subject to the rules listed in the previous questions.

The processing of biometric data is subject to the provisions of CNDP Decision no. 478-2013 of 1 November 2013 on the conditions necessary for the use of biometric devices for access control. This decision lays down the rules for the use of biometric data and makes the installation of a biometric device subject to prior authorization by the CNDP.

However, the CNDP may authorize the use of biometric data for access control to sensitive premises and facilities under the following conditions:

- The controller must justify that alternative methods of access control are not sufficiently reliable to secure the site;
- the biometric data of a limited number of persons who are regularly or temporarily present on the site for the performance of their mission must be processed;
- Biometric data cannot be used in its original form. For example, for fingerprinting, a limited number of features have to be extracted;
- The controller shall not establish a database for the storage of the collected biometric data. However, in certain specific cases, the

establishment of a database could be authorized by the CNDP;
- As a general rule, the data must be recorded on a support exclusively held by the data subject, such as a smart card or magnetic card;
- The use of biometric devices must be for authentication purposes and not for identification purposes.

Facial recognition is subject to the provisions of CNDP Decision no. 195-2020, under which the use of facial recognition technologies is subject to the following requirements:

- Obtain the CNDP authorization for the processing;
- Ensure the authentication phases using the services provided, immediately after its establishment, by the trusted national third party system managing an official identity;
- Organize the architecture of the information system, based on the appropriate principles enabling the authentication phases to be easily switched to the trusted third party system (API-type architectures or others).

25. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

The Data Protection Law allows the transfer of personal data to countries providing a sufficient level of protection of privacy and fundamental rights and freedoms of individuals.

By the deliberation n° 236-2015 of 18 December 2015 modifying deliberation n° 465-2013 of 6 September 2013, the CNDP established the list of countries providing sufficient protection of privacy and fundamental rights and freedoms of individuals with regard to the processing of personal data.

The controller must notify the CNDP before transferring personal data to a country providing a sufficient level of protection regarding the established list.

Data controllers may also transfer personal data to a country not included on the list provided by the CNDP only if one of the following conditions applies:

- The data subject expressly consents to the transfer
- The transfer is necessary to safeguard the life of the person concerned, to preserve the public interest, to establish, exercise, or defend a right in court, perform a contract between the controller and data subject, to perform a contract between the controller and a third party in the data subject's interest, to execute an international mutual legal assistance measure, or to prevent, diagnose, or treat medical conditions.
- The transfer is covered under a bilateral or multilateral agreement to which Morocco is a party.
- The CNDP expressly authorizes a transfer that provides a sufficient level of protection of the data subject's privacy and fundamental rights and freedoms, particularly because of contractual clauses, such as a data transfer agreement, or binding corporate rules.

In these situations, the controller must submit a request to the CNDP to obtain an authorization that will allow the abroad data transfer.

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The Data Protection Law requires controllers to implement technical and organizational measures to protect personal data against (i) the accidental or unlawful destruction, (ii) the accidental loss, alteration, disclosure, or unauthorized access, and (iii) all other unlawful forms of processing especially when the processing involves data transmission in a network.

In addition, the security measures should ensure, considering the current state of the art and the implementation costs, an appropriate level of security for the risks of processing and the nature of the data to be protected.

The Data Protection Law also requires processors, or any person acting under their authority, to process personal data in accordance with both the instructions of the controllers and the legal requirements.

27. Do the laws in your jurisdiction address

security breaches and, if so, how does the law define “security breach”?

The Data Protection Law does not define the “security breach” and does not require the controller to report the security breach.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

Cybersecurity regulations provide for entities in sectors of vital importance in particular administrations, establishments and public enterprises and organisms disposing of a state agreement or license to perform a regulated activity (i.e those relating to public security, the financial sector, industry, transport networks, energy production and distribution and mining, the supply and distribution of water, telecommunications and postal services, audiovisual and communications, health and justice) are required to establish special measures for the protection of sensitive data in the critical infrastructure sector.

The compliance to cybersecurity regulations must be established with regards to the following principles:

- Organizational Structure;
- Information Systems Cartography;
- Establishing a budget for the information systems security;
- Control of the administrators of the entities’ information systems;
- Protection of data by following the security rules specified by the DNSSI;
- Training and awareness of system and network administrators and IT users about their rights and obligations ;
- Hosting on the national territory the sensitive data of the entities.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

The report of security breaches is only required for entities in sectors of vital importance and their services providers, in accordance with Law no. 05-20 on cybersecurity.

The report must be made to the the Information Systems Security Department (la Direction Générale de la Sécurité des Système d’Information) (DGSSI).

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

The legal requirements regarding dealing with cybercrime are provided by the Law no. 07-03 supplementing the criminal code with regards to infractions relating to automated data processing systems.

The following offences are covered by the provisions of the Law no. 07-03 completing the criminal code:

- The intrusion or fraudulent maintaining in an automated data processing system;
- Violations of the operation of an automated data processing system;
- Voluntary data breaches; and
- The association of cyber criminals.

31. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

In September 2011, Morocco created the Directorate General for Information Systems Security (DGSSI) under the Ministry of National Defense.

The DGSSI adopted a national cybersecurity strategy aiming to provide Moroccan information systems with a defence and a capacity of resilience, in order to create the conditions of trust environment and security.

In addition, a Computer Alert and Incident Management Centre (MA-CERT) attached to the DGSSI has been created and acting as a monitoring, detection and response centre for computer attacks. Thus, when a Critical Infrastructure is victim of an attack, it must communicate, within 48 hours, to the ma-CERT information relating to major incidents affecting the security or functioning of its sensitive information systems.

Finally, the National Telecommunications Regulatory Agency (ANRT) have important regulatory functions, which regulate Internet service providers and international organizations concerned with

cybersecurity.

32. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

Data Protection Law provides data subjects with a number of rights listed hereafter, that may be exercised by submitting a request to the controller who is obliged to respond according to the data subjects' request.

(i) the right to be informed with regards to the collection and processing of their personal data:

The data controller or his representative must expressly, precisely and unequivocally inform any person directly requested to collect their personal data prior to the collection of such data.

The controllers are required to give a number of information to the data subjects (see question 14) unless:

- the processing is necessary for national defence, internal or external state security, or crime prevention.
- Providing the information proves impossible, particularly in cases of processing personal data for statistical, historical, or scientific purposes if the data controller notifies the CNDP that providing notice is impossible and about the reason for the impossibility.
- Moroccan law expressly authorizes the personal data recording or disclosure.
- The processing is solely for journalistic, artistic, or literary purposes.

(ii) the right of access which allows data subject to access their personal data to ensure its accuracy:

Data subjects have the right to obtain from the controller, free of charge and without delay, whether or not their data are being processed. They may also request the characteristics of the processing carried out, such as its purposes, the categories and origin of the data processed and the recipients to whom the data are transmitted.

(iii) the right to request the rectification and erasure of personal data processing which do not comply with the Data Protection Law:

The data subjects have the right to request that the controller rectify, erase, or block personal data processing that does not comply with the Data Protection Law, especially if the data subject knew that the data and the processing are incomplete or inaccurate.

Data subjects may exercise their right by contacting the controller. in the case of a request for rectification, the controller is required to reply, within a clear period of ten days, to the requests of data subjects.

In the event of refusal or non-response within the abovementioned deadline, the data subject may submit a request for rectification to the CNDP, which will instruct one of its members to carry out all necessary investigations and ensures that rectifications are made.

(iv) the right to object to processing of their personal data:

Based on their legitimate interests, the data subjects may exercise their right to object unless the processing is based on a legal requirement or in case the right to object cannot be exercised because of the Data Protection Law allowing for the processing.

The data subjects also have the right to object to data processing for direct marketing purposes.

33. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

The data subjects' privacy rights are enforceable by means of:

1. the CNDP, which is the authority competent to receive complaints from data subjects who consider that they have been harmed by using and processing their personal data or when they notice a violation of the Data Protection Law dispositions. The CNDP is competent to examine and follow the controller up by ordering the publication of corrective measures. The CNDP may also, when deemed necessary, bring the case before the Public Prosecutor for the purpose of legal proceedings.
2. Judicial recourse by referring to the public prosecutor.

34. Does the law in your jurisdiction provide for a private right of action and, if

so, in what circumstances?

Please refer to our answer above.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

The data subject may bring a civil action apart from criminal proceedings and may claim compensation for the damage caused by the controller's breaches of its legal requirements, provided that the data subject establishes the damage, harm and causal link.

36. How are the laws governing privacy and data protection enforced?

The application of laws relating privacy and the protection of personal data are subject to administrative and criminal proceedings.

When a violation is established, the data subject could file a complaint before the police or the prosecutor in order to institute the criminal proceedings. The data subject may also make a complaint to the CNDP, which would investigate and provide its report to the prosecution in order to launch criminal proceedings.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

The law has established a list of violations subject to sanctions. These can be summarized as follows:

- any processing violating the public order, the safety, morality and good manners;
- the performance of a processing without authorization or the required declaration;
- the refusal of the right of access, rectification or opposition; any incompatibility with the purpose declared;
- failure to comply with the data storage period – failure to comply with the security measures for processing;
- failure to comply with the consent of the data subject, in particular in the case of direct marketing for commercial purposes, with aggravation of the sanctions in the case of sensitive data;
- any transfer of personal data to a country not recognized as providing adequate protection;
- any obstacle to the exercise of the control missions of the CNDP;
- any refusal to implement the decisions of the CNDP.

Violations of Data Protection Law are punishable as an administrative or criminal offense. The Data Protection Law provides for several sanctions, such as fines and/or imprisonment and/or withdrawal of CNDP authorization.

The sanctions vary according to the degree of the offence against the natural persons responsible for processing the personal data, and without prejudice to their civil liability towards the persons who have been harmed due to the offence, shall be liable to imprisonment for three months to two years and fines between 10,000 and 300,000 dirhams. These sanctions may be doubled in the event of a recidivism.

The penalties for an offence committed by a legal person, without prejudice to the sanctions that may be applied to its directors, shall be doubled. The legal person may be liable to confiscation of its property and the closure of the institutions thereof.

38. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

N/A.

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Yes, appeal can be made before the competent Court.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

No proposals for now.

Contributors

Mehdi Kettani
Head of IPT – Morocco

mehdi.kettani@dlapiper.com