

## Personal Data Protection Law

### *Suggested amendments*

#### Article 1

For the purpose of implementing this Law, the following terms shall have the meanings assigned thereto, unless the context requires otherwise:

- 1- **Law:** The Personal Data Protection Law.
- 2- **Regulations:** The Implementing Regulations of the Law.
- 3- **Competent Authority:** The authority to be determined by a resolution of the Council of Ministers.
- 4- **Personal Data:** Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, date of birth, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.
- 5- **Processing:** Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.
- 6- **Collection:** The collection of Personal Data by Controller in accordance with the provisions of this Law, either from the Personal Data Subject directly, a representative of the Personal Data Subject, any person has legal guardianship over the Personal Data Subject or any other party.
- 7- **Destruction:** Any act that leads to the removal of Personal Data, rendering the Personal Data inaccessible or irrecoverable.
- 8- **Disclosure:** Enabling any person, other than the Controller or Processor, to obtain, use or access Personal Data by any means or for any purpose.
- 9- **Transfer:** The transfer of Personal Data from one place to another for Processing.
- 10- **Publishing:** Transmitting or making available any Personal Data using any written, audio or visual means.
- 11- **Sensitive Personal Data:** Personal Data that includes a reference to an individual's racial or ethnic origin, or religious, intellectual or political belief, as well as criminal and security data, biometrics, Genetic Data, Credit Data, Health Data, and data that indicates that one or both of the individual's parents are unknown.
- 12- **Genetic Data:** Any Personal Data related to the hereditary or acquired characteristics of a natural person that uniquely identifies the physiological or health characteristics of that person, and derived from biological sample analysis of that person, such as DNA or any other testing that leads to generating genetic data.
- 13- **Health Data:** Any Personal Data related to an individual's health condition, whether their physical, mental or psychological condition, or related to Health Services received by that individual.
- 14- **Health Services:** Services related to the health of an individual, including preventive, curative, rehabilitative and hospitalizing services, as well as the provision of medications.
- 15- **Credit Data:** Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.
- 16- **Personal Data Subject:** The individual to whom Personal Data relates.
- 17- **Public Entity:** Any ministry, department, public institution or public authority, any independent public entity in the Kingdom, and any body affiliated therewith.
- 18- **Controller:** Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the Data is processed by that Controller or by the Processor.
- 19- **Processor:** Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.

#### Article 2

1- This Law shall apply to:

- a. Any Processing of Personal Data carried out in the Kingdom in any manner whatsoever.

## Personal Data Protection Law

### *Suggested amendments*

- b. Any Processing of Personal Data of individuals who are located in the Kingdom, carried out in any manner whatsoever by an entity located outside the Kingdom.
- 2- Paragraph 1 of this Article shall include Personal Data of the deceased if such Personal Data leads to identifying the deceased person or their family members specifically.
- 3- This Law shall not apply to the Processing of Personal Data by an individual for personal or family use, as long as the Personal Data is not published or disclosed to others. The Regulations shall specify the personal and family uses referred to in this paragraph.

#### **Article 3**

The provisions and procedures stated in this Law shall be without prejudice to any provision that grants a right to Personal Data Subject or confers better protection on Personal Data Subject pursuant to any other law or any international agreement to which the Kingdom is a party.

#### **Article 4**

Personal Data Subject shall have the following rights pursuant to this Law and as set out in the Regulations:

- 1- The right to be informed, which includes informing Personal Data Subject of the legal basis and the purpose of collecting their Personal Data.
- 2- The right to access their Personal Data held by the Controller, in accordance with the rules and procedures set out in the Regulations, and without prejudice to the provisions of Article 9 of this Law.
- 3- The right to request correcting, completing or updating their Personal Data held by the Controller.
- 4- The right to request the Destruction of their Personal Data held by the Controller, without prejudice to the provisions of Article 18 of this Law.
- 5- The right to obtain their Personal Data in a legible and clear format, including the right to request the Transfer of their Personal Data to another Controller if this is technically possible, in accordance with the rules and conditions set out in the Regulations.
- 6- Other rights provided for in this Law, as set out in the Regulations.

#### **Article 5**

- 1- Except for the cases stated in this Law, neither Personal Data may be processed nor the purpose of Processing of Personal Data may be changed without the consent of the Personal Data Subject. The Regulations shall set out the conditions of the consent, the cases in which the consent must be express, and the terms and conditions related to obtaining the consent of the legal guardian if the Personal Data Subject fully or partially lacks legal capacity.
- 2- In all cases, Personal Data Subject may at any time withdraw the consent referred to in paragraph 1 of this Article. The Regulations shall set out the rules for such withdrawal.

#### **Article 6**

In the following cases, Processing of Personal Data shall not be subject to the consent referred to in paragraph 1 of Article 5 of this Law:

- 1- If the Processing serves actual interests of the Personal Data Subject, but communicating with the Personal Data Subject is impossible or difficult.
- 2- If the Processing is pursuant to another law or in implementation of a previous agreement to which the Personal Data Subject is a party.
- 3- If the Controller is a Public Entity and the Processing is required for security purposes or to fulfill judicial requirements.
- 4- If the Processing is necessary to achieve a lawful interest of the Controller or any other party, without prejudice to the rights and interests of the Personal Data Subject, and provided that the Personal Data is not Sensitive Personal Data, in accordance with the rules and provisions set out in the Regulations.

#### **Article 7**

## Personal Data Protection Law

### *Suggested amendments*

The consent referred to in paragraph 1 of Article 5 of this Law may not form a condition of providing a service or a benefit, unless such service or benefit is directly related to the Processing of Personal Data for which the consent is given.

#### **Article 8**

Subject to the provisions of this Law and the Regulations regarding the disclosure of Personal Data, when selecting the Processor, the Controller shall select one that provides the guarantees necessary to implement the provisions of this Law and the Regulations. The Controller shall verify the selected Processor's compliance with the provisions of this Law and the Regulations, without prejudice to its responsibilities towards the Personal Data Subject or the Competent Authority, as the case may be. The Regulations shall set out the provisions necessary in this regard, which shall include provisions concerning any subsequent contracts entered into by the Processor.

#### **Article 9**

- 1- The Controller may set timeframes for exercising the right to access Personal Data stated in paragraph 2 of Article 4, as set out in the Regulations. The Controller may restrict the said right in the following cases:
  - a. If this is necessary to protect the Personal Data Subject or others from any harm, as set out in the Regulations.
  - b. If the Controller is a Public Entity and the restriction is required for security purposes, to implement another law, or to fulfill judicial requirements.
- 2- The Controller shall prevent the Personal Data Subject from accessing Personal Data in any of the events stated in paragraphs 1, 2, 3, 4, 5 and 6 of Article 16 of this Law.

#### **Article 10**

Controller may collect Personal Data only from the Personal Data Subject. Such Personal Data may only be processed for the purpose for which the Personal Data is collected. However, in the following cases, Controller may collect Personal Data from a person other than the Personal Data Subject or process Personal Data for a purpose other than that for which the Personal Data is collected:

- 1- If the Personal Data Subject consents in accordance with the provisions of this Law.
- 2- If the Personal Data is publicly available, or collected from a publicly available source, without prejudice to the provisions of this Law.
- 3- If the Controller is a Public Entity and the Personal Data was not directly received from the Personal Data Subject, or was processed for a purpose other than that for which it was collected as required for security purposes or to implement another law or fulfill judicial requirements in accordance with the provisions set out in the Regulations.
- 4- If compliance with this restriction may cause harm to the Personal Data Subject or affect the vital interests of the Personal Data Subject, as set out in the Regulations.
- 5- If the Collection or Processing of Personal Data is necessary to protect the public health, public safety or public interest, or to protect the life or health of a specific individual. The Regulations shall set out the rules and procedures applicable in this regard.
- 6- If the Personal Data will not be recorded or stored in a form that makes it possible to directly or indirectly identify the Personal Data Subject. The Regulations set out the rules and procedures applicable in this regard.
- 7- If the Collection or Processing of the Personal Data is necessary to achieve lawful interests of the Controller or any other party, without prejudice to the rights or interests of the Personal Data Subject, and provided that the Personal Data is not Sensitive Personal Data, in accordance with the rules and provisions set out in the Regulations.

#### **Article 11**

- 1- The purpose for which Personal Data is collected shall be directly related to the Controller's purposes, and shall not contravene any applicable legal provisions.

## Personal Data Protection Law

### *Suggested amendments*

- 2- The methods and means of collecting Personal Data shall not conflict with any legal provisions, shall be appropriate for the circumstances of the Personal Data Subject, shall be direct, clear and secure, and shall not involve any deception, misleading or extortion.
- 3- The Controller shall ensure that the content of the Personal Data is appropriate and limited to the minimum amount necessary to achieve the purpose of the Collection. The Regulations shall set out the rules applicable in this regard.
- 4- If the Personal Data collected is no longer necessary for the purpose for which it has been collected, the Controller shall, without undue delay, cease the Collection and destroy the previously collected Personal Data.

#### **Article 12**

The Controller shall adopt a privacy policy and make it available to Personal Data Subject for review prior to collecting Personal Data. The policy shall specify the purpose of Collection, the Personal Data to be collected, the method of Collection, the means of storage and Processing, the manner in which the Personal Data shall be destroyed, and the rights of the Personal Data Subject in relation to the Personal Data and how such rights shall be exercised.

#### **Article 13**

When collecting Personal Data directly from the Personal Data Subject, the Controller shall take appropriate measures to inform the Personal Data Subject of the following prior to or during the Collection:

- 1- The legal basis for collecting their Personal Data.
- 2- The purpose of the Collection, and shall specify the Personal Data whose Collection is mandatory and the Personal Data whose Collection is optional. The Personal Data Subject shall be informed that the Personal Data will not be subsequently processed in a manner inconsistent with the Collection purpose or in cases other than those stated in Article 10 of this Law.
- 3- Unless the Collection is for security purposes, the identity of the person collecting the Personal Data and the address of its representative, if necessary.
- 4- The entities to which the Personal Data will be disclosed, the capacity of such entities, and whether the Personal Data will be transferred, disclosed or processed outside the Kingdom.
- 5- The potential consequences and risks that may result from not collecting the Personal Data.
- 6- The rights of the Personal Data Subject pursuant to Article 4 of this Law.
- 7- Such other elements as set out in the Regulations based on the nature of the activity done by the Controller.

#### **Article 14**

The Controller may not process Personal Data without taking sufficient steps to verify the Personal Data accuracy, completeness, timeliness and relevance to the purpose for which it is collected in accordance with the provisions of the Law.

#### **Article 15**

The Controller may not disclose Personal Data except in the following cases:

- 1- If the Personal Data Subject consents to the disclosure in accordance with the provisions of the Law.
- 2- If the Personal Data is collected from a publicly available source, without prejudice to this Law.
- 3- If the entity requesting the disclosure is a Public Entity and the request is made for security purposes, to implement another law, or to fulfill judicial requirements in accordance with the provisions set out in the Regulations.
- 4- If the disclosure is necessary to protect the public health, public safety or public interest, or to protect the life or health of a specific individual. The Regulations shall set out the rules and procedures applicable in this regard.
- 5- If the disclosure is limited to subsequent Processing of Personal Data in a manner that does not lead to identifying the Personal Data Subject or any other individual specifically. The Regulations shall set out the rules and procedures applicable in this regard.

## Personal Data Protection Law

### *Suggested amendments*

- 6- If the Disclosure is necessary to achieve a lawful interest of the Controller or any other party, without prejudice to the rights or interests of the Personal Data Subject, and provided that the Personal Data is not Sensitive Personal Data, in accordance with the rules and provisions set out in the Regulations.

#### **Article 16**

The Controller may not disclose Personal Data in the cases stated in paragraphs 1, 2 and 5 of Article 15 if the disclosure:

- 1- Represents a threat to security, harms the reputation of the Kingdom, or conflicts with the interests of the Kingdom.
- 2- Affects the Kingdom's relations with any other state.
- 3- Prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal procedures.
- 4- Compromise the safety of an individual.
- 5- Results in violating the privacy of an individual other than the Personal Data Subject, as set out in the Regulations.
- 6- Conflicts with the interests of a person that fully or partially lacks legal capacity.
- 7- Breaches legally established professional obligations.
- 8- Involves a breach of an obligation, procedure, or judicial ruling.
- 9- Exposes the identity of a confidential source of information in a manner detrimental to the public interest.

#### **Article 17**

- 1- If Personal Data is corrected, completed or updated, the Controller shall notify such amendment to all the other entities to which such Personal Data has been transferred and make the amendment available to such entities.
- 2- The Regulations shall set out the timeframes for correction and updating of Personal Data, types of correction, and the procedures required to avoid the consequences of Processing incorrect, inaccurate or outdated Personal Data.

#### **Article 18**

- 1- The Controller shall, without undue delay, destroy the Personal Data when the purpose of the Collection ceases to exist. However, the Controller may retain Personal Data after the Collection purpose ceases to exist if all that may lead to identifying the Data Subject is removed in accordance with the rules set out in the Regulations
- 2- In the following cases, the Controller shall retain the Personal Data after the purpose of the Collection ceases to exist:
  - a. If there is a legal justification for retaining the Personal Data for a specific period, in which case the Personal Data shall be destroyed upon the lapse of that period.
  - b. If the Personal Data is closely related to a case under consideration before a judicial authority and its retention of the Personal Data is required for that purpose, in which case the Personal Data shall be destroyed once the judicial procedures are concluded.

#### **Article 19**

The Controller shall take all the necessary organizational, administrative and technical measures to safeguard Personal Data, including during the Transfer of Personal Data, in accordance with the provisions and rules set out in the Regulations.

#### **Article 20**

If the Controller becomes aware that the Personal Data has been leaked, damaged or illegally accessed, and such leakage, damage or access is capable of causing harm to the Personal Data Subject or is detrimental to the rights or interests of the Personal Data Subject, the Controller shall carry out the notification requirements relating to the leakage of Personal Data, in accordance with the rules and provisions set out in the Regulations, and the provisions set by the Competent Authority.

## Personal Data Protection Law

### *Suggested amendments*

#### **Article 21**

The Controller shall respond to the requests of the Personal Data Subject pertaining to the rights of the Personal Data Subject under this Law within such period and in such method as set out in the Regulations.

#### **Article 22**

If the Controller provides a product or service that depends on or is related to the Processing of Personal Data, the Controller shall evaluate the effects of the Processing of the Personal Data in relation to such product or service, based on the nature of the activity done by the Controller and the nature of the product or service, in accordance with the related provisions of the Regulations.

#### **Article 23**

Without prejudice to this Law, the Regulations shall set out additional rules and procedures for the Processing of Health Data in a manner that ensures the privacy of the Personal Data Subject and protects the rights of the Personal Data Subject as set out in this Law. Such additional rules and procedures shall include the following:

- 1- Restricting the right to access Health Data, including medical files, to the minimum number of employees or workers whose roles require such access to Health Data, and only to the extent necessary to provide the required Health Services.
- 2- Restricting Health Data Processing operations to the minimum number of employees and workers as necessary to provide Health Services or offer health insurance programs.
- 3- The cases where the Personal Data Subject must be notified of any request for Disclosure of their Health Data.

#### **Article 24**

Without prejudice to this Law, the Regulations shall set out additional rules and procedures for the Processing of Credit Data in a manner that ensures the privacy of the Personal Data Subject and protects the rights of the Personal Data Subject as set out in this Law and the Credit Information Law. Such rules and procedures shall include the following:

- 1- Taking appropriate measures to verify that the Personal Data Subject has given their express consent to the Collection of the Personal Data, changing the purpose of the Collection, or Disclosure or Publishing of the Personal Data in accordance with the provisions of this Law and the Credit Information Law.
- 2- Requiring that the Personal Data Subject be notified when a request for disclosure of their Credit Data is received from any party.

#### **Article 25**

With the exception of the informational materials sent by Public Entities, Controller may not use personal means of communication, including the post and email, of the Personal Data Subject to send advertising or informational materials, except in accordance with the following:

- 1- Obtaining the prior consent of the recipient.
- 2- The sender of the material shall provide a clear mechanism, as set out in the Regulations, that enables the intended recipient to request stopping sending such materials.

The Regulations shall set out the provisions concerning the aforementioned advertising and informational materials, as well as the conditions and circumstances concerning the consent of the recipient.

#### **Article 26**

- 1- Processing of Personal Data for marketing purposes shall be conditional on setting a clear mechanism that allows the target recipient to request the cessation of the Processing whenever the target recipient so wishes. The Regulations shall set out the rules applicable in this regard.
- 2- Sensitive Personal Data may not be processed for marketing purposes unless it is collected directly from the Personal Data Subject and the Personal Data Subject expressly consents to the Processing of their Sensitive Personal Data for marketing purposes. The Regulations shall set out the rules and conditions applicable in this regard.

#### **Article 27**

## Personal Data Protection Law

### *Suggested amendments*

In the following cases, Personal Data may be collected or processed for scientific, research or statistical purposes without the consent of the Personal Data Subject:

- 1- If the Personal Data does not contain information that specifically identifies the Personal Data Subject.
- 2- If the information that specifically identifies the Personal Data Subject is to be destroyed during the Processing of such Personal Data prior to the Disclosure of such Personal Data to any other entity, and provided such Personal Data is not Sensitive Personal Data.
- 3- If the Collection or Processing of Personal Data for the said purposes is required under any other law, or in implementation of a prior agreement to which the Personal Data Subject is a party.

The Regulations shall set out the rules necessary in relation to this Article.

### **Article 28**

- 1- Controller may transfer Personal Data outside the Kingdom or disclose Personal Data to an entity outside the Kingdom in accordance with the following:
  - a. If the country to which the Personal Data is to be transferred has regulations that ensure appropriate protection of Personal Data and protection of the rights of Personal Data Subjects, and has a supervisory entity that imposes appropriate procedures and measures on Controllers to protect Personal Data, so that the standards of Personal Data protection in that country are not less than the standards provided for under this Law and the Regulations.
  - b. The Competent Authority adopts evaluation criteria for the requirements set out in paragraph (1.a) of this Article.
- 2- Notwithstanding paragraph 1 of this Article, in the following cases, Controller may transfer Personal Data to outside the Kingdom or disclose Personal Data to an entity outside the Kingdom in a manner other than as stated in paragraph (1.b) of this Article:
  - a. If this is for preserving the public interest, public health, public safety, or protecting the life or health of a specific individual or individuals.
  - b. If the transfer is relating to performing an obligation under an international agreement to which the Kingdom is a party.
  - c. If this is done in performance of an obligation of the Personal Data Subject, in accordance with the applicable provisions set out in the Regulations.
- 3- When transferring Personal Data outside the Kingdom or disclosing Personal Data to an entity outside the Kingdom, the Controller shall observe the following:
  - a. Such transfer shall not adversely affect the national security or vital interests of the Kingdom.
  - b. The Transfer or Disclosure of Personal Data shall be limited to the minimum amount of Personal Data required.

### **Article 29**

- 1- Without prejudice to the provisions of this Law and the powers of the Saudi Central Bank pursuant to applicable legal provisions, the Competent Authority shall be the entity in charge of overseeing the implementation of this Law and the Regulations.
- 2- The Regulations shall identify the cases where the Controller shall appoint one or more persons as Personal Data protection officer(s), and shall set the responsibilities of any such person in accordance with the provisions of this Law.

## Personal Data Protection Law

### *Suggested amendments*

- 3- The Controller shall cooperate with the Competent Authority in performing its duty to supervise the implementation of the provisions of this Law and the Regulations, and shall take such steps as necessary in connection with the related matters referred to the Controller by the Competent Authority. The Competent Authority may request documents and information from the Controller to ensure its compliance with this Law and the Regulations.
- 4- The Competent Authority may, at its sole discretion, authorize other entities to perform part of its responsibilities in connection with overseeing the implementation of the provisions of this Law and the Regulations.

#### **Article 30**

- 1- Without prejudice to the provisions of Article 18 of this Law, the Controller shall keep records, for such a period as required under the Regulations, of the Personal Data Processing activities, based on the nature of the activity done by the Controller, so that such records are available whenever requested by the Competent Authority. The records shall contain the following information at a minimum:
  - a. Contact details of the Controller.
  - b. The purpose of the Processing.
  - c. Description of the categories of Personal Data Subjects.
  - d. Any other entity to which Personal Data has been or will be disclosed.
  - e. Whether the Personal Data has been or will be transferred outside the Kingdom or disclosed to an entity outside the Kingdom.
  - f. The expected period for which Personal Data shall be retained.
- 2- Controller shall keep records of the operations performed on Personal Data and shall set rules to restrict access to Personal Data. The Regulations shall set out the rules and procedures concerning those records.

#### **Article 31**

In order to perform its obligations and supervise the implementation of this Law and the Regulations, the Competent Authority may issue decisions, instructions and circulars to enable the Competent Authority to monitor the Controllers' compliance with this Law and the Regulations. The Competent Authority shall have the following powers in particular:

- 1- Monitor compliance with this Law and the Regulations.
- 2- Issue guidelines, instructions and decisions relating to the enforcement of this Law and the Regulations, including decisions of precautionary measures and remedial actions to rectify any violation of this Law.
- 3- Seek assistance from other competent authorities to supervise the implementation of this Law and the Regulations.
- 4- Cooperate with its international counterparts entities in the cases that require supervising the implementation of this Law, without prejudice to the Kingdom's obligations under any international agreements, and in a manner that is not adverse to the Kingdom's international relations.
- 5- Take the necessary procedures to establish the violations of this Law, including carrying out detection and inspection activities.
- 6- Identify suitable tools and mechanisms to monitor the compliance of Controllers, including creating a national record for Controllers and providing services related to the protection of Personal Data. The Competent Authority may collect fees for the services it provides, in coordination with Ministry of Finance and the Non-Oil Revenues Development Center.
- 7- Identify suitable tools and mechanisms to monitor the compliance of the entities outside the Kingdom that process Personal Data of individuals residing in the Kingdom, and identify suitable procedures to implement this Law outside the Kingdom.



## Personal Data Protection Law

### *Suggested amendments*

#### **Article 32**

- 1- The Competent Authority shall set the conditions for engaging in the commercial, professional and non-profit activities relating to the protection of Personal Data in the Kingdom, as set out in the Regulations, and in coordination with the entities concerned.
- 2- The Competent Authority may license other entities to issue accreditation certificates for Controllers and Processors, so as to certify that those entities process Personal Data in accordance with this Law, provided that the Competent Authority shall establish the rules regulating the issuance of those certificates.
- 3- The Competent Authority may license other entities to audit the Personal Data Processing activities, as set out in the Regulations, and may establish rules, conditions and requirements for those licenses.

#### **Article 33**

A Personal Data Subject may submit to the Competent Authority or the Controller any complaint that may arise out of the implementation of this Law and the Regulations. The Regulations shall set out the rules for handing the complaints that may arise from implementing this Law and the Regulations.

#### **Article 34**

- 1- Without prejudice to any severer penalty stated in any other law, any person that discloses or publishes Sensitive Personal Data in violation of this Law shall be punished by imprisonment for not more than two years and/or a fine of not more than three million Saudi Riyals if the violation is committed with the intention of causing damage to the Personal Data Subject or achieving a personal benefit.
- 2- The Public Prosecution shall be in charge of investigating the violations stated in this Article and prosecuting the cases of such violations before competent courts.
- 3- A competent court shall hear the cases arising from the application of this Article and impose the stated penalties.
- 4- A competent court may double the fine if the violation is repeated, even if that results in exceeding the maximum limit of fine, provided however that in no circumstances may the fine exceed double the maximum limit.

#### **Article 35**

- 1- With respect to any matters not addressed by Article 34 of this Law, and without prejudice to any severer penalty stated in any other law, any natural or private legal person that violates this Law shall be punished as follows:
  - a. Warning.
  - b. A fine of not more than five million Saudi Riyals.
- 2- A penalty shall be proportionate to the nature and seriousness of the violation and the resulting damage.
- 3- The fine may be doubled if the violation is repeated, even if that results in exceeding the maximum limit of the fine, provided however that in no event may the fine exceed double the maximum limit.
- 4- One or more committees shall be formed by a decision of the head of the Competent Authority. Each committee shall consist of not less than three members. One of the members shall be named chairman and another member shall be a Sharia or legal advisor. A committee so formed shall be tasked with examining the violations and imposing the penalties stated in paragraph 1 of this Article. The committee's decision shall be approved by the head of the Competent Authority or the authorized representative of the head of the Competent Authority. The head of the Competent Authority shall issue a decision stating the committee work rules and committee members' remuneration.
- 5- The party against whom a decision is issued by the committee referred to in paragraph 4 of this Article shall have the right to challenge the decision before any competent court.

## Personal Data Protection Law

### *Suggested amendments*

#### **Article 36**

- 1- Employees and workers to be named by a decision of the head of the Competent Authority shall have the powers to control and inspect the violations stated in this Law or the Regulations. The head of the Competent Authority shall issue the work rules and procedures of those employees in accordance with the applicable laws.
- 2- The employees and workers referred to in paragraph 1 of this Article may seek assistance from criminal control and other relevant entities in carrying out their duties concerning violation control and inspection.
- 3- The entities that are subject to this Law and the Regulations shall enable their employees or workers referred to in paragraph 1 of this Article to carry out their duties pursuant to this Law and the Regulations and the work rules of those employees as issued by the head of the Competent Authority.

#### **Article 37**

A competent court, or the committee referred to in paragraph 4 of Article 35, as the case may be, may include in their penalty judgment or decision a provision that a summary of such judgment or decision be published at the expense of the violator in one (or more) local newspapers distributed in the violator's area of residence, or using any other proper means, based on the type, seriousness and impact of the violation, provided the publishing shall be after the judgment becomes final, the lapse of the deadline for appeals, or the issuance of a final ruling dismissing the appeal against the judgement.

#### **Article 38**

Without prejudice to the provisions of Article 34 and paragraph 1 of Article 35 of this Law, a Public Entity shall discipline any of its employees who violates any of the provisions of this Law and the Regulations, in accordance with the disciplinary provisions and procedures established under law.

#### **Article 39**

Without prejudice to the penalties stated in this Law, any party that suffers material or moral damage as a result of any of the violations stated in this Law or the Regulations may apply to a competent court for proportionate compensation.

#### **Article 40**

Any party that engages in Processing of Personal Data shall preserve the confidentiality of the Personal Data even after the end of such party's occupational or contractual relationship.

#### **Article 41**

The head of the Competent Authority shall issue the Regulations no later than 180 days from the issuance date of this Law, provided that the head of the Competent Authority shall first liaise with the Ministry of Communications and Information Technology, the Ministry of Foreign Affairs, the Communications, Space and Technology Commission, the National Cybersecurity Authority, the Saudi Health Council and the Saudi Central Bank, each in relation to their scope.

#### **Article 42**

This Law shall enter into force upon the lapse of 180 days from the date of publishing the Law in the Official Gazette.