Ministry of Transport, Communications and Information Technology.

Ministerial Decision

No. 2024/34

Issuing the Executive Regulation of the Personal Data Protection Law

Based on the Personal Data Protection Law promulgated by Royal Decree 6/2022, and

in pursuance of public interest,

Hereby decided the following:

Article I

The attached Executive Regulation of the Personal Data Protection Law shall apply.

Article II

Entities subject to the provisions of the attached regulation shall rectify their status in accordance with its provisions within a period not exceeding one year from the date of its enforcement.

Article III

All that is contrary to the attached Regulation or in conflict with its provisions is hereby repealed.

Article IV

This decision shall be published in the Official Gazette, and comes into force on the day following the date of its publication.

Issued on: 16 Rajab 1445

Corresponding to: 28January 2024

Eng. Said bin Hamoud bin Said Al-Mawali

Minister of Transport, Communications and Information Technology

Executive Regulation of the Personal Data Protection Law

Chapter One

Definitions and General Provisions

Article (1)

In the application of the provisions herein, the terms and expressions shall carry the same meanings as stipulated in the aforementioned Personal Data Protection Law. Additionally, the following terms and expressions shall bear the meanings assigned thereto, unless the context requires otherwise:

1. Law:

Personal Data Protection Law

2. Competent Department

The competent administrative division in the Ministry to manage the protection of personal data.

3. Authorisation:

Consent issued by the Ministry to the controller to process personal data.

4. Disclosure:

Enable third parties, by any means and for any purpose, to access, obtain, or utilize personal data.

5. Personal Data Breach:

Unlawful access to personal data leading to its unauthorised destruction, alteration, disclosure, access, or processing.

Article (2)

The controller or processor, as the case may be, shall provide the Competent Department with any documents, data, information and any other requirement, within (30) thirty days from the date of the Competent Department's request.

Article (3)

To process personal data, the controller may enter into contract with the processor. In the context of the services provided by the processor to third parties, the processor acts as a representative of the controller. Without prejudice to the processor's criminal liability for any violations of the law and this regulation, this representation falls within the scope of civil and administrative responsibility before the Ministry.

Article (4)

Prior to processing personal data, the controller must obtain explicit consent from the personal data subject, provided that the following conditions for the consent are considered:

1. The consent shall be issued by a person of full legal capacity.
2. The consent shall be issued in a clear manner and without coercion.
3. The consent may be provided in writing, electronically, or through any other means specified by the controller.

Chapter Two

Authorisation Process

Article (5)

In the application of the provision of Article (5) of the law, the controller must obtain an authorisation from the Ministry before processing any personal data. The authorisation application, prepared in accordance with the prescribed form, shall include the following information:

1. Name, address, and email of the personal data protection officer.
2. Purpose of processing personal data.
3. Identification and categorization of the personal data to be processed.
4. Details of any processor contracted to process personal data (if any).
5- Identification of any entity or third party to whom the processed personal data will be disclosed.
6. Places where personal data will be transferred or stored.
7. Identification of Systems for managing and protecting personal data.
8. Any other data requested by the Ministry.

Article (6)

When submitting an authorisation request, the controller must include their personal data protection policy and the precautionary measures taken in the event of a personal data breach.

Article (7)

The Competent Department shall review the authorisation application and make a decision within a period not exceeding (45) forty-five days of receiving all required data and documents. In case of rejection, the decision must be justified. Failure to receive a response within the stipulated period constitutes a rejection of the application.

The authorisation applicant may appeal to the Minister within (60) sixty days of receiving the decision notice or becoming aware of it. If no response is received within (30) thirty days of the grievance submission, it shall be considered rejected.

Article (8)

The Minister shall issue the authorisation for a period not exceeding (5) five years, inclusive of the authorised person's data, upon payment of the specified fees. The renewal of the authorisation for such period or periods shall follow the procedures outlined in this chapter.

Article (9)

Using the designated form, the controller must inform the Competent Department of any amendments to the data included in the issued authorisation, within (15) fifteen days from the date of making these amendments.

Article (10)

The authorisation may be revoked under any of the following circumstances:

1. Upon the request of the controller.
2. If the controller violates the provisions of the law or this Regulation.
3. Failure to notify the Competent Department of amendments to the authorisation’s data within the specified period.
4. If it is determined that the controller obtained the authorisation through fraud, deception, forgery, or by providing incorrect data or information.

Chapter Three

Processing Child's Personal Data

Article (11)

The controller or processor, as applicable, must obtain explicit consent from the guardian of the child before processing their personal data.

The controller or processor, as applicable, may request from the Child the minimum details of their guardian to verify the guardian`s identity and obtain their consent.

Article (12)

While processing the personal data of the child, the controller or processor, as applicable, shall adhere to the following guidelines:

1. The purpose of the processing must be clear, straightforward, secure, and free from fraud and misrepresentation.
2. Processing should be limited to the minimumpersonal data necessary to achieve its specified purpose.

Article (13)

The controller or processor, as applicable, shall determine and provide the means by which the guardian of the child can access the personal data of their child for the purpose of updating and amending them.

Article (14)

The controller or processor, as the case may be, shall not disclose or share the personal data of the child with third parties unless express consent is obtained from the guardian.

Article (15)

The individual who is incapacitated, ineligible, or disqualified shall be represented by their guardian or trustee, as appropriate. The provisions outlined in this chapter shall govern the processing of their personal data.

Chapter Four

Rights of the Personal Data Subject

Article (16)

The personal data subject may submit a written request to the controller to exercise any of their rights outlined in clauses (a, b, c, d, and e) of Article (11) of the law, without incurring any charges. The controller must respond to the request within a maximum period of (45) forty-five days from the date of receiving the request. Additionally, the personal data subject may request the cessation of the processing of their personal data until the request is addressed.

Article (17)

The controller may partially or fully reject the personal data subject's request if it is deemed unjustifiably repetitive or if fulfilling it requires extraordinary effort.

In all cases, the controller must inform the personal data subject of the reasons behind the refusal within the time-frame specified in Article (16) herein.

Article (18)

The personal data subject shall be entitled to request the controller to delete their personal data under the following circumstances:

1. Termination of the purpose for which the data was processed.
2. Withdrawal of consent for the processing of their data, without prejudice to the provision of Article (17) herein.
3. Non-compliance of the data processing with the provisions of the law or this Regulation.

However, the controller may, as the case may be, reject the request of the personal data subject under the following circumstances:

1. Compliance with a legal obligation imposed on the controller by any law, judgment, or court decision.
2. The Existence of a dispute between the controller and the personal data subject.

Article (19)

The personal data subject is entitled to request from the controller a copy of their personal data that has been processed, provided in a legible and clear electronic or paper format. The copy provided mustn't contain any personal data that could identify another individual.

Article (20)

The personal data subject is entitled to transfer their personal data to a new controller, provided that the current controller transfers the personal data to the new controller if they are legally obliged to do so.

Chapter Five

Obligations of the Controller and Processor

Article (21)

The controller or processor, depending on the circumstance, must display a personal data protection policy in a conspicuous place that allows the personal data subject to view it before their data is processed. the policy shall, at minimum, outline the mechanisms and procedures for the personal data subject to exercise their rights as stipulated in the law and this Regulation.

Article (22)

Before sending any advertising, marketing material or with commercial purpose to the personal data subject, the controller must adhere to the following procedures:

1. Obtain the written consent of the personal data subject.
2. Notify the personal data subject of the methods by which advertising, marketing, or commercial materials will be sent.
3. Specify the Mechanism to opt-out of receiving further advertising, marketing, or commercial materials.
4. Immediately cease sending advertising, marketing, or commercial materials upon receiving a request for suspension from the personal data subject, and do so free of charge.

Article (23)

The controller and the processor shall appoint the external auditor in accordance with the following requirements:

1. The auditor must be accredited and licensed by the Ministry.
2. The auditor must maintain independence and must not have any direct or indirect connections with the controller or processor.

In all cases, the controller and the processor must grant the external auditor access to review and examine the records, processing systems, and data required for the audit process.

Article (24)

The controller and the processor shall provide the Competent Department with a copy of the external auditor's report within a maximum period of (60) sixty days from the date of the appointment of the external auditor.

Article (25)

The controller and the processor are prohibited from publishing, sharing, or disclosing the personal data outlined in Article (5) of the law, except within the limits and in the cases prescribed by law or when it complies with a court judgment or judicial decision.

Article (26)

The controller shall guarantee the confidentiality of personal data by adhering to the following controls and procedures:

1. Establishing, using and activating electronic systems to prevent unauthorised access, breach, alteration, or misuse of personal data.
2. Establishing mechanisms for recovering personal data in the event of physical or technical incident.
3. Conducting regular testing of the effectiveness of the technical procedures implemented.

Article (27)

Without prejudice to the provision of Article (18) herein, the controller or processor, as the case may be, shall maintain the documents of processing operations, considering the following guidelines:

1. The retention of processing documents shall be based on specific and legitimate reasons.
2. A retention period appropriate to the purpose of processing shall be defined.
3. Provide technical protection systems to retain processing documents securely.

Article (28)

The controller or processor, as the case may be, shall establish a dedicated register of personal data processing activities, which shall include, at minimum, the following details:

1- Data of the Personal Data Protection Officer.

2. Description of the categories of personal data held and details of individuals authorised to access personal data.

3. Duration, limitations, and scope of processing.

4. Deleting, modifying, or processing personal data mechanism.

5. Purpose of processing personal data.

6. Entities with whom personal data is disclosed and the purposes of such disclosure.

7. Details of any entity to which personal data is transferred.

8. Any information regarding the transfer and processing of personal data across borders.

9. Technical and organizational measures for information security and processing operations.

10. Any personal data breaches, including details of the incidents, its impact, and any remedial or corrective actions taken.

Article (29)

The controller shall update the record of processing activities on an ongoing basis, and submit it to the Competent Department upon requested.

Chapter Six
Personal Data Breach

Article (30)

The controller must notify the Competent Department within (72) seventy-two hours after becoming aware of the breach if it poses a risk to the rights of the personal data subjects. The report shall include, at minimum, the following:

1. Description and details of the nature of the breached data and the consequences of the breach.

2- The data and contact information of the controller or any other focal point to obtain further information.

3. Description of the possible effects of the breach.

4. Corrective actions or technical and organisational measures that the controller will take to address the breach, including, where necessary, proposed measures to mitigate potential adverse effects.

5. Corrective actions,and technical and organisational measures taken by the controller immediately upon becoming aware of the breach and before informing the Competent Department.

Article (31)

Upon receiving the notice outlined in Article (30) herein, the Competent Department may document it in the register designated for this purpose and take the following measures as it deems appropriate:

1. Assessing the procedures and measures implemented by the controller to mitigate the damage resulting from the breach.

2. Requesting to notify the personal data subject of the breach, if deemed necessary by the Competent Department, without prejudice tothe provision of Article (32) herein.

3. Providing appropriate guidance or support to the controller based on available capabilities.

Article (32)

In the event of a personal data breach, the controller shall notify the personal data subject within a period not exceeding (72) seventy-two hours after becoming aware of the breach, if such breach would result in serious harm or high risks to the personal data subject. The notice shall include the following:

1. The type and nature of the breach.

2. Details of the personal data that has been breached.

3. Recommendations for limiting or mitigating the effects of the breach, if required.

Article (33)

The controller shall document instances of personal data breach cases, including their causes, consequences, and the corrective actions or technical and organisational measures taken, and maintain records in accordance with the duration specified by the Competent Department, within the register outlined in Article (28) herein.

Chapter Seven

Personal Data Protection Officer

Article (34)

The controller must designate the personal data protection officer, in accordance with following controls:

1. Possesses the qualifications necessary to fulfill the responsibilities outlined in Article (35) herein.
2. Be aware of the law,, this Regulation, and the personal data protection practices adopted by the controller or processor.
3. Demonstrates professional competence and is capable of consistently and appropriately handling all aspects related to personal data protection.

Article (35)

The personal data protection officer shall undertake the following tasks:

1. Submitting proposals and consultations to the controller or processor in relation to their obligations stipulated in the law and this regulation.
2. Following up on the implementation of the policies of the controller or processor relating to the protection of personal data.
3. Following up the implementation by the controller or processor of their obligations stipulated in the law and this regulation.
4. Coordinating with the Competent Department in matters relating to the processing of personal data.

Article (36)

The controller shall publish information regarding the personal data protection officer, including their name and contact details, through any available means. The personal data subject retains the right to contact the personal data protection officer regarding all matters concerning the processing of their personal data.

Chapter Eight

Transferring personal data beyond borders

Article (37)

Before transferring personal data outside the borders of the Sultanate of Oman, the controller shall obtain the explicit consent of the personal data subject. Furthermore, the transfer of data shall not affect national security or the supreme interests of the state. The consent of the personal data subject is not required in one of the following cases:

1. If it fulfills an international obligation outlined in an agreement involving the Sultanate of Oman
2. If the transfer is conducted in a manner that anonymizes the personal data subject, making it unlinkable to the individual and unidentifiable in any manner.

Article (38)

Before transferring personal data outside the borders of the Sultanate of Oman, the controller must ensure that the external processing entity provides an adequate level of protection for personal data. This level of protection shall not be less than what is prescribed by law and this Regulation.

Article (39)

The controller shall evaluate the level of protection provided by the external processing entity and assess the risks associated with transferring personal data. This evaluation shall include the following aspects:

1. Description of the nature and volume of the personal data intended for transfer, including its sensitivity level.
2. Purpose of the processing of personal data, the extent of processing, and entities with whom the data will be shared.
3. The duration of the processing of personal data, and whether it will take place in a restricted or accidental manner only once or repeatedly and regularly within a limited period.

4. Phases involved in the transfer of personal data, including the countries involved and the final destination of the personal data.
5. The effects and risks that may result from the transfer process, and the extent of its impact on the personal data subject.

Article (40)

The Ministry may request a copy of the evaluation report prepared by the controller to ensure that the external processing entity has an adequate level of protection.

Chapter Nine

Complaints and Penalties

Article (41)

The personal data subject or any concerned individual has the right to submit a complaint or report to the Competent Department regarding any violation of the provisions of the law, this Regulation, and decisions issued in its implementation, prepared in accordance with the prescribed form within (30) thirty days of becoming aware of the violation. Upon receiving the complaint or report, the Competent Department must notify the controller with a copy of the complaint or report within (7) seven days from the date of its submission.

Article (42)

The controller is entitled to respond to the complaint or report submitted against them within a period not exceeding (14) fourteen days from the date of notification.

Article (43)

The Competent Department shall decide on the complaint or report within (60) sixty days from the day following the expiry of the period specified in Article (42) herein. Failure to respond within that period shall be deemed a rejection.

Article (44)

In the event of a violation of the provisions of this Regulation, the Minister may impose one of the following administrative penalties:

1. Warning
2. Suspending the authorisation until the violation is rectified.
3. An administrative fine not exceeding (2000) two thousand Omani Riyal for each violation.
4. Cancellation of the authorisation.

Article (45)

Any individual subject to the administrative penalties outlined herein may lodge a grievance with the Minister within (60) sixty days from the date of being notified of the violation decision or being aware of it. The Minister must decide on the grievance within (30) thirty days from its submission. Failure to respond within this period is deemed a rejection of the grievance.