

# PERSONAL DATA PROTECTION MANUAL

UNITED ARAB EMIRATES

---

A SYNOPSIS  
FOR COMPLIANCE



**01**

Introduction



**02**

Legal Framework



**03**

Essential Concepts



**04**

Fundamental Principles/  
Rules to Process Personal Data



**05**

Key Determinations



**07**

Consent





Rights of Data Subjects



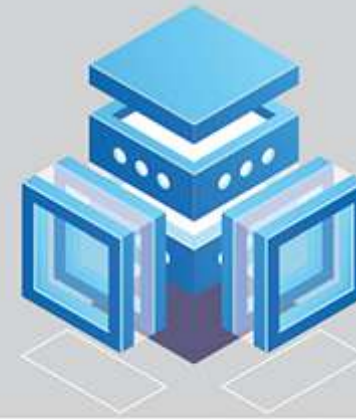
**08**



Cross-Border Transfer of Personal Data

**09**

Roadmap towards Privacy Compliance



**10**



Our Services

**17**

Professional Contributions



**18**



Contact Us

**19**



# Introduction

## What is Privacy?

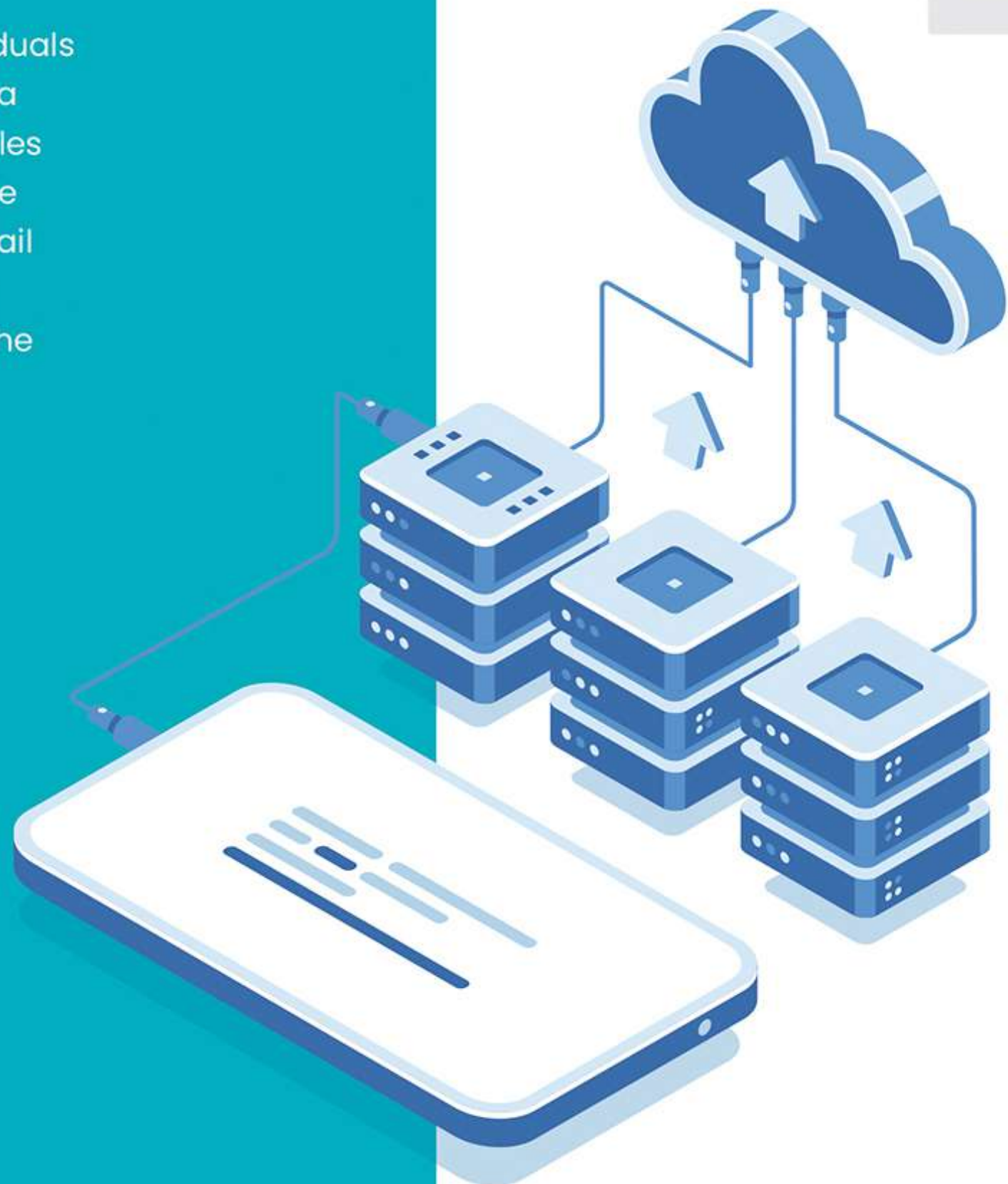
Privacy, in the context of personal data protection, means that individuals' personal information is to be used with free choice of the individuals, in accordance with their wishes and that users of personal information are to act and behave in a fair and transparent manner.

## What the Laws, on Privacy Protection, are about?

Laws on protection of personal data, globally, meant to provide a framework through which personal information of individuals is used by others in a controlled or regulated way. Availability of a regulator, to enforce the privacy of individuals, is another reason for the development of laws on this matter.

## What persons are impacted by the Personal Data Protection Laws?

The users of personal information of the individuals are directly impacted by laws on personal data protection. Such users are to follow the principles embodied in the legal framework to protect the privacy of individuals. Deviations therefore entail monetary fines. On the other hand, individuals (natural persons) are positively impacted as the laws provide means to protect their privacy.





## Legal Framework

Federal Decree-Law No. 45 of 2021 on Personal Data Protection has been come into effect on January 02, 2022 (the UAE Law). The Executive Regulations of the UAE Law are yet to be issued. The UAE Law will be implemented with in a period of six months following the issuance of Executive Regulations.

In addition to the UAE Law, Abu Dahbi Global Market (ADGM) and Dubia International Financial Centre (DIFC) have their own framework concerning protection of personal data, applicable in their respective jurisdictions.





# Essential Concepts

It is necessary, for the persons who are impacted by the UAE Law, to be familiar with certain basic concepts contained in the UAE Law. These concepts are central to understand the fundamentals of the UAE Law.

The following concepts are defined in the UAE Law and are explained in simple words hereunder:

**Personal Data** means any piece of information relating to an identified natural person or related to a natural person who can be identified directly or indirectly from that piece of information.

**Sensitive Personal Data** means personal data which reveals race, ethnicity, political or philosophical views, criminal record, biometric data etc of a natural person.

**Data Subject** means natural person to whom personal data relates.

**Controller** means a person who, alone or jointly with others, determines the means and methods of processing of personal data.

**Processor** means a person who processes the personal data on behalf a controller.

**Processing** means any operation performed on personal data, right from its collection till erasure/destruction including storage, alteration, exchange, use etc.

**Consent** means authorization by data subjects (natural persons) to process their personal data by controllers/processors.

The following sections of this manual will discuss above concepts in more details.





# Fundamental Principles / Rules to Process Personal Data

Legal frameworks, across the globe, on personal data protection are set on certain fundamental or general principles. Such principles serve as the guiding rules to govern the processing of personal data by controllers/processors. The fundamental rules, under the UAE Law, are as follows:

<b>Fairness, Transparency &amp; Lawfulness</b>	Controllers/processors are required to process personal data of the data subjects with all the fairness, transparency and lawfulness.
<b>Purpose Limitation</b>	The processing must only be for a clearly specified purpose and personal data is not to be processed for any other reason
<b>Accuracy</b>	The controllers/processors are to keep correct and accurate personal data
<b>Erasure or Rectification</b>	The controllers/processors are to ensure erasure or rectification of incorrect personal data.
<b>Security</b>	The controllers/processors are to implement appropriate technical and organizational measures to protect the personal data.
<b>Storage Limitation</b>	Personal data is not to be kept beyond the time when purpose (for which personal data was collected) is fulfilled
<b>Data Minimization</b>	The amount of personal data must not be excessive, only limited amount of personal data is to be used that is necessary to fulfill the purpose for which personal data is collected.
<b>Controls Specified by Executive Regulations</b>	Processing is subject to any further controls to be specified by the Executive Regulations.



# Key Determinations

To manage privacy at organizational level, it is important to distinguish what is personal data, what is sensitive personal data and who is a controller and processor.

## What is Personal Data

It is important to distinguish clearly which information is personal data and which is non-personal data. It is important to know because the UAE Law is only applicable on personal data and non-personal data is outside the scope of the UAE Law. Few examples of personal data and non-personal data are as follows:

### Personal Data

- Name of an Individual
- Passport Number
- Social Security Number
- Photograph of an Individual



### Non-Personal Data

- Generic email ids (without having name of a natural person)
- Name of a City
- Tax registration number of a company

## What is Sensitive Personal Data

Sensitive personal data is part of personal data (included within the legal definition of personal data) and includes information that directly or indirectly reveals following about a natural person:

- ✓ *Race*
- ✓ *Ethnicity*
- ✓ *Political or philosophical views*
- ✓ *Religious beliefs*
- ✓ *Criminal records*
- ✓ *Biometric data*



In addition, the sensitive personal data also includes data related to natural person's health (like physical, psychological, or mental health).

It is important to distinguish between personal data and sensitive personal data, it is so because the UAE Law places more strict conditions to process sensitive personal data in comparison to personal data.

## Who is Controller and Processor

Controllers and processors are the users of personal data of the data subjects. The UAE Law, to protect the personal data, places certain obligations on controllers and processors. The UAE Law provides different obligations on the controllers and processors and therefore it is important that users of personal data must know their respective positions (whether one is controller or processor) for meeting the prescribed obligations.

The unique characteristics helping to distinguish between controller and processor are:

### Controller

- Decides to collect or process personal data
- Decides the purpose of processing
- Decides what personal data is to be collected



### Processor

- Does not decide to collect or process personal data
- Does not decide the purpose of processing
- Follows instructions of controller regarding processing of personal data



# Consent

As a general rule, the UAE Law provides that processing of personal data without consent of data subject is prohibited. Consent, to valid under the UAE Law, must have the following essentials:

- Clarity
- Specific
- Unambiguous indication of data subject's agreement to process his/her personal data

The consent is to be expressed by a statement or clear affirmative action on part of the data subject.

The UAE Law, however, provides a few exceptions to the aforesaid general rule wherein processing may be done without consent, in following cases:

- Necessity for public interest
- Personal data made public by the data subject
- Necessity to initiate or defend any claim of rights and legal actions (judicial or security procedures)
- Necessity for occupational or preventive medicine to assess working capacity of employees
- Necessity for the protection of public health
- Necessity for the archiving, scientific, historical or statistical purposes in accordance with the law
- Necessity for the protection of interests of data subject
- Necessity for performance of obligations under law concerning recruitment, social security or social protection
- Necessity for the performance of a contract to which data subject is a party
- Necessity for the compliance with obligations under any other law
- Situations as may be specified by the Executive Regulations





# Rights of Data Subjects

The very purpose of the UAE Law is to empower the natural persons (data subjects) and while providing a framework for use of their personal data the UAE Law provides rights to the data subjects. Such rights help ensuring autonomy of the data subjects on the one hand and on the other to help protection of personal data. The data subjects have following rights available under and subject to provisions of the UAE Law:

## Right of access to information

Data subjects have the right to ask controller about their personal data like categories of personal data, purpose of processing, to whom personal data is being shared etc

## Right to request personal data portability

Data subjects have the right to receive their personal data in a structured and machine-readable format and for transfer of personal data to another controller

## Right to rectify or erasure

Data subjects may ask controller to rectify or erase personal data

## Right to restrict processing

Data subjects have the right to ask controller to restrict processing

## Right to stop processing

Data subjects have the right to ask controller to stop processing

## Right to object automated decision making

Data subjects have the right to object to automated decision making that has legal implications or that seriously affects data subjects





# Cross Border Transfer of Personal Data

Cross border transfer of personal data is a significant issue, globally, under various legal regimes related to protection of personal data. Transfer of personal data from one country to another is subject to strict controls under all the relevant laws in the world.

The UAE Law also provides strict controls and personal data, as a first principle, may only be transferred outside UAE in following cases duly approved by the regulator:

- To a state or territory having personal data protection laws in place whereby data subjects can exercise rights and having provisions relating to imposition of appropriate measures against the controllers or processors through a regulatory or judicial entity (principle of adequate protection)
- To a state with whom UAE has bilateral or multilateral agreements related to personal data protection



## How to transfer Personal Data to country having no adequate protection or with whom UAE has no bilateral or multilateral agreement

As an exception to above mentioned first principle, personal data may be transferred outside UAE in following cases in accordance with the controls and requirements to be specified by the Executive Regulations:

- Under a binding contract or agreement between the personal data sender and controller/processor in the other country to the effect that controllers/processors in that other country will follow provisions of the UAE Law
- With express consent of the data subject
- Transfer is necessary for performance of obligations and establishing rights before the judicial entities
- Transfer is necessary for the performance of contract between controller and data subject or between controller and a third party for the interests of data subject
- Transfer is necessary for the performance of an act relating to international judicial cooperation
- Transfer is necessary for the protection of public interest



# Roadmap towards Privacy Compliance

**A**

Adherence to fundamental principles/rules to process personal data



Provision of information to the data subjects

**B**

**C**

Security of Personal Data: Implementation of technical and organizational measures



Personal data protection impact assessment

**D**

**E**

Record maintenance








Ensuring compliance by data processors

F

G

Responding to data subject's requests



Data breach notifications

H

I

Appointment of data protection officer



Communication with data subjects

J



# A Adherence to fundamental principles/ rules to process personal data

Controllers and processors, under the UAE Law, are required to adhere to the fundamental principles as described in detail at Page No. 04 of this manual. The observance of those fundamental principles goes to the very roots of the legal framework to provide due protection to the rights of the data subjects.



# B Provision of information to the data subjects

As part of principal of fairness (transparency) the controllers are required to provide following information to data subjects prior to processing their personal data:

- Purpose of the processing
- Third parties with whom personal data will be shared (within UAE and outside UAE)
- Safeguards to be applied while transferring personal data outside UAE





# C Security of Personal Data: Implementation of technical and organizational measures

The controllers and processors, under the UAE Law, are required to implement appropriate technical and organizational measures for the protection of personal data.

## Technical Measures

- Security of network and information systems
- Security of data held within systems
- Security of website and any other online service or application
- Security of devices

## Organizational Measures

- Having a culture of security awareness at all levels, board-C level positions and all other staff of a company
- Company is to carry out a detailed exercise to identify any risks arising out of its processing of personal data
- There must be a dedicated person within the company with primary responsibility to deal with the data privacy issues.
- The company must develop and then implement the standard operating procedures concerning protection of personal data and all employees are suitably trained to apply the SOPs.
- Development of adequate continuity plans is also part of organizational measures to protect personal data. Business continuity plans help to execute actions in case of any breach of personal data.





# D Personal data protection impact assessment

In certain circumstances the UAE Law requires that controllers, before the processing, are to carry out an assessment of the impact of processing operations. The impact assessment is necessary in following cases:

- When personal data processing involves a systematic and extensive evaluation of personal data based on automated processing including profiling or the processing has legal effects significantly affecting the data subject.
- When personal data processing involves large scale of sensitive personal data.



# E Record Maintenance

Controllers and processors are to keep appropriate records of all the processing activities, including:

- Details of controller, processor and data protection officer
- Purpose of processing
- Description of categories of personal data
- Persons authorized to access personal data
- Timeframe, restrictions and scope of processing
- Erasure and modification mechanism
- Cross-border transfer of personal data
- Description of technical and organizational measures for security of personal data





## F Ensuring compliance by data processors

The controllers are to appoint processors (to carry out personal data processing on their behalf) assuring to implement appropriate technical and organizational measures so that all the requirements of the UAE Law are adequately being met by the processors. The contract between controller and processor, in this regard, is to record scope, subject, purpose, nature and type of personal data and categories of personal data to be processed by the processor.



## G Responding to data subject's requests



The UAE Law provides certain rights to the data subjects, as detailed at Page No. 08 of this manual. Data subjects are entitled to approach controllers with their requests for exercise of such rights. Data controllers are bound to respond to such requests in accordance with the UAE Law. As the framework (the UAE Law) is all about to protect the interests of data subjects and to confer rights on them, therefore it is imperative that controllers keep them prepare to respond to all such requests.

## H Data breach notifications

Data breach means an unauthorized access, to personal data resulting in any kind of transmission, exchange transfer or even destruction of personal data through.

- Replication
- Transmission
- Distribution
- Exchange
- Transfer
- Destruction
- Modification





Data controllers are required to report a breach to regulator and to data subjects when the breach has the effect to compromise the privacy or confidentiality of the data subjects or when the breach results in risks to safe custody of the personal data.

#### **Contents of data breach notification**

- Description of nature of the breach
- Details of the Data Protection Officer (if any)
- Potential and expected effects of the breach
- Description of actions and measures taken
- Description of measures to minimize negative effects of the breach

## **I Appointment of data protection officer**

In following cases the controllers are required to appoint a Data Protection Officer:

- When Processing is likely to result in a high risk to the privacy
- When Processing involves a systematic and overall assessment of sensitive personal data
- Data Protection Officer is also required to be appointed where processing involves profiling and automated processing
- In cases where processing involves a large scale of sensitive personal data, Data Protection Officer is required to be appointed

Controllers are, therefore, required to assess their position with respect to the mandatory appointment of Data Protection Officer.

## **J Communication with data subjects**

The UAE Law requires that controllers are to provide clear and appropriate means and mechanism enabling the data subjects to raise any request and to exercise any of the rights. The controllers are, thus, to made available adequate means for the data subjects to make their requests and to exercise their rights.





# Our Services

Bizilance Legal Consultants have the experience to advise clients on data privacy compliance, cross border transfer of data, development of personal data privacy related polices and other documents etc.

We offer focused and tailor-fit services to our clients with the objective that our clients remained compliant with the applicable legal requirements concerning personal data protection. Our suite of services include:

## Situational Analysis & Compliance Framework

- Initial assessment of current practices & processes regarding handling of personal data
- Development of compliance framework in accordance with the Framework
- Gap identification between initial assessment and compliance framework
- Advisory on filling the Gaps

## Advisory

- Application of the Framework
- Compliance management
- Reg Tech (advisory to use technology in consonance with the Framework)
- Development & review of documentation (Policies & Procedures, Notices etc)
- Breach reporting
- External data protection officer services

## Awareness & Training

- Basic awareness workshops/seminars for employees and management
- Capacity building of the inhouse staff entrusted with matters related to protection of personal data
- Specific training sessions (either audience specific or subject specific)

## Health Check

- Compliance review (an exercise to ascertain conformity with the compliance framework)
- Risk assessment (based on compliance review to highlight specific areas which are potentially prone to risk)
- Compliance profiling (matrix showing strong and weak areas in relation to follow the compliance framework)
- Remediation (devising means to overcome any shortfalls to follow the compliance framework)



# Professional Contribution

Directors in Bizilance Legal Consultants regularly contribute professional articles, regarding data privacy, in various international publications of repute including International Comparative Legal Guides, Chambers & Partners, Legal 500, Lexology, Mondaq etc.

We also regularly organize/contribute in webinars on data privacy issues with our partners and other professional platforms/research organizations including Mondaq, Legal 500 etc.





## Contact Us

Contact us to discuss how we can assist you to implement privacy compliance program.



**SAIFULLAH KHAN**

Director

saifullah.khan@bizilancelegal.ae  
linkedin.com/in/saifullahkhan  
+971 58 184 8960



**SAEED HASAN KHAN**

Director

saeed.hasan@bizilancelegal.ae  
linkedin.com/in/saeedhasankhan  
+971 52 914 1118





# Bizilance

Legal Consultants

D 4-5, Suite 407, Al Sarab Tower, Level 15th, ADGM Abu Dhabi, United Arab Emirates  
00 971 2 711 9786 , 00 971 52 914118  
contact@bizilancelegal.ae | www.bizilancelegal.ae