KPMG

The new Federal Data Protection Law 2021 of the United Arab Emirates

A summary

Kpmg.com/ae

The new Federal Data Protection Law

The UAE has announced the enactment of a new Federal Data Protection Law ('Law') as part of its 'Projects of the 50', a series of development and economic initiatives marking the UAE's 50th anniversary in 2021.

The Federal Data Protection Law constitutes a significant development in modernizing the UAE's onshore data protection laws and represents the first steppingstone to 'adequacy' decisions from other regulators, both in the UAE's financial free zones and globally.

While no data privacy law at the federal level existed previously in the UAE, ADGM and DIFC had both established localized data protection frameworks. The updated law is a new chapter in the UAE's long-standing commitment to globally recognized standards of data protection and is largely modelled on the European Union's GDPR. The goal of the UAE Federal Data Protection Law is to establish enhanced governance and transparency requirements that will facilitate the UAE's alignment with international laws and regulations.

The new regulation provides controls that reflect recognition of the importance of personal data and fundamental protection of data subjects' rights. This includes the use and governance of personal data in emerging technologies.

How will the Law advance the UAE?

- Modernizes the UAE's onshore data protection laws, which will enable innovation and increase trust and credibility with global organizations and data subjects.
- Further positions the UAE when it comes to potentially attracting foreign investors and increasing confidence with respect to data protection.
- Provides 'adequacy' decisions from other regulators—enhancing secure global data sharing and business mobility.
- Empowers individuals' rights relating to the collection and processing of their personal data.
- Guides organizations that need to comply with the Federal Data Protection Law to implement protective measures in data collection and processing to prevent potential breaches.
- Ensures that UAE's Federal data regulator ('UAE Data Office') is guided by international best practices, which have been adopted by European Union Supervisory Authorities and the European Data Protection Board.
- Enables organizations, as well as their clients and business partners, to protect valuable data.
- Aligns with a globally accepted approach and principles for data privacy and protection.
- Provides a framework and guidance for disputes brought before the UAE courts.

What does the new Federal Data Protection Law cover?

01
General provisions
Definitions, objectives and scope of application of the decree-law

02
Data processing
Controls for processing sensitive data

03
Obligations and consent
Data controller and processor obligations, consent conditions

04
Data protection officer (DPO)
Appointment and duties of the DPO

05
Data subject rights
Right to withdraw, right to access and rectify, right to object processing, etc

06
Data protection
Personal data security and impact assessments

07
Cross-border transfer of personal data
Data sharing and complaints processes

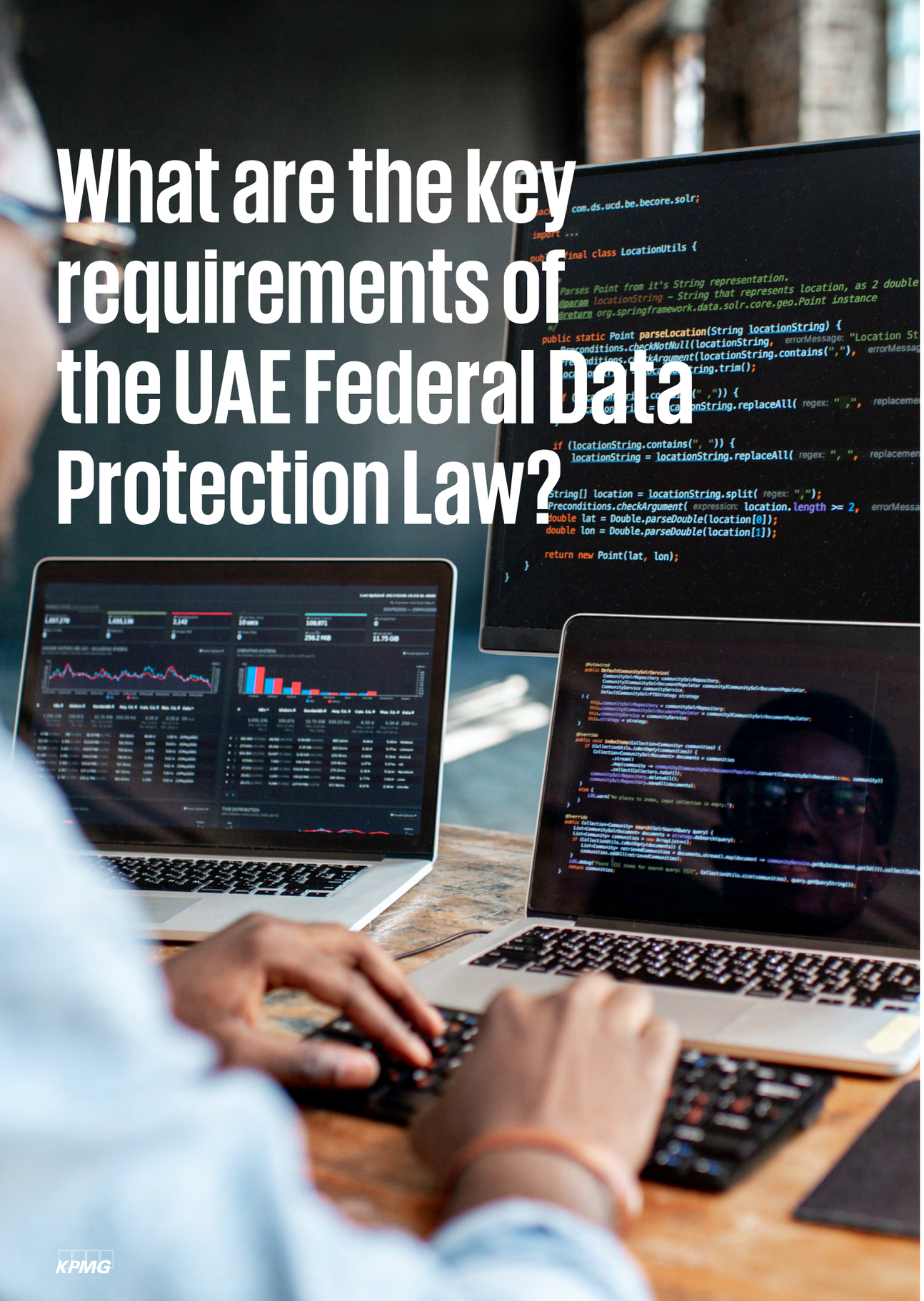
08
Final provisions
Complaints, fines, executive decisions, publication and implementation of the UAE Federal Law

How does the UAE Federal Data Protection Law compare to the GDPR?

Definitions, objectives and scope of application of the decree-law

GDPR		UAE Federal Data Protection Law
Personal data collected in the EU/EEA i.e. "EU personal data". The GDPR also has **extra-territorial reach.**	**Material and territorial scope**	Data subjects who reside in the UAE or havea place of business there. The new data protection law has an **extra-territorial reach** similar to the GDPR.
Appoint a DPO and lead supervisory authority **under certain conditions.**	**Governance/DPO**	Companies will need to **appoint a DPO under certain circumstances**. The DPO may be an employee of the company or an external party.
Up to **20m** or **4% of global annual revenues.**	**Penalties**	The data protection law **does not expressly state the amounts** of penalties that will apply for breaches of the Law.
Immediately, however a **two-year grace period** was given.	**Implementation period**	Companies will have **six months from the issuance of the executive regulations** to comply with the law.
Disclosure of incidents and data breaches without undue delay and within **72 hours** of the breach.	**Incident and breach response**	The controller shall, **immediately** upon becoming aware of a breach, notify the office of the breach and the findings of the investigation.
Requires companies to create and maintain a record of processing activities. **Record of processing activities (RoPA) is not required if organizations have under 250 employees.**	**Record of processing activities**	**Requires all companies** to create and maintain a more detailed RoPA.
Data protection impact assessments (DPIAs) **are required.**	**Data protection impact Assessment**	Assessment of the impact of protection of personal data **is required.**
Six lawful bases for processing personal data.	**Lawful basis for processing**	**Five lawful bases** for processing—the Data Protection Law does not allow for processing based on a controller's 'legitimate interests'.
There are **eight** data subject rights under the GDPR.	**Data subject rights**	There are **six** data subject rights. The 'right to be informed' within the GDPR is not defined in UAE law. The right to correct and delete data are combined.
One month with potential extension by two additional months to respond to a data subject access request (DSAR) request.	**Rights response timeline**	**No timeline** to respond to the data subject has been defined.
Direct marketing is permitted through **consent and legitimate interest**. Data subjects have the right to **object/ opt-out.**	**Marketing**	Direct marketing is permitted through **consent only**. Data subjects have the right to **object/opt-out.**
Permitted **under specific conditions** and if adequate levels of data protection are required.	**Cross border transfers**	Permitted if the country or territory to which the personal data will be transferred **has legislation for protection of personal data.**

What are the key requirements of the UAE Federal Data Protection Law?



01 General provisions

Objective:
Govern activities related to personal data including its protection and processing, to protect the privacy of individuals and preserve their rights.

Scope of application:
- Every individual who resides in or has a business in the UAE.
- Every organization **in the UAE** that carries out activities involving processing personal data.
- Every organization **outside of the UAE** that carries out the activities of processing personal data for individuals within the UAE.
- The new DP Law has **extra-territorial reach.**

Scope of application exemptions:
- Government data, government authorities who control or process personal data.
- Personal data with the security and judicial authorities.
- Health personal data is governed by legislation regulating the protection and processing of such data.
- Banking and credit personal data and information that are governed by legislation regulating the protection and processing of such data e.g., consumer protection regulation.
- Companies and establishments located in financial free zones in the state that have their own personal data protection legislations e.g. DIFC and ADGM.

Supervisory authority responsibilities:
- Supervise and monitor the implementation and compliance of the Federal Data Protection Law.
- Perform investigations and impose fines/penalties on violators.
- Enhance and expand the coverage and policies of the Federal Data Protection Law.

02 Data processing

Sensitive personal data processing:
Processing sensitive personal data is prohibited without the consent of the data subject. Exceptions are in place (article 5) in cases related to protecting or serving the public interest.

Personal data processing controls:
- Processing should be conducted in a fair, transparent, and legitimate manner.
- Personal data should be collected and limited to a specific and clear purpose.
- Personal data should be accurate and ensure the removal of incorrect personal data.
- Personal data should not allow the identification of its owner after the purpose of processing has been exhausted.
- Personal data should be stored securely.

Legitimate processing requirements:
The processing of personal data is lawful in the following cases:
- Consent has been provided by the data subject.
- The implementation of a contract with the data subject.
- To carry out an obligation established by law to which the data controller is subject.
- To protect the interests of the data subject.
- To protect the public interest.
- To pursue legitimate interests of the data controller without conflicting with the rights and interests of the data subject or public interest.

03 Obligations and consent

Terms of approval:
- The controller must be able to establish the consent of the data subject or their guardian.
- Consent must be prepared in a clear and unambiguous manner.
- The data subject or their guardian withdraws consent to the processing of personal data, and the procedure to do so should be simple and easy.

Data controller obligations:
- Appropriate technical and organizational measures are in place to protect and secure the confidentiality and integrity of personal data.
- Ensure measures are in place to ensure processing of personal data is limited to its intended purpose, the type of processing performed, and period of storage.
- Maintain a personal data record that is to be provided to the supervisory authority when requested. This record should include the following:
  - Data controller information
  - DPO information
  - Description of the categories of personal data
  - Information on the individuals to be disclosed data
  - Processing times
  - Limitations and scope
- The mechanism for erasing/modifying personal data or its processing
- Purpose/lawful basis of processing

- Information related to processing data across borders
- Statement of the technical and organizational measures related to information security and processing operations
- Designating the processor to implement the technical and organizational measures to meet the requirements of the Federal Data Protection Law.
- Provide the supervisory authority with personal data based on the decision of the judicial authority.

Data processor obligations:
- Process data in accordance with the instructions of the data controller.
- Apply the appropriate measures for technical and organizational procedures to secure and protect the confidentiality and integrity of personal data, including the devices used for processing and storage.
- Process data in accordance with the specified purpose and period and notify the data controller if processing exceeds this period.
- Erase data after the processing period or hand it over to the data controller.
- Only disclose personal data or the result of processing in cases authorized by law.
- Maintain a personal data record that is to be provided to the supervisory authority when requested. This record should include the following:
  - Description of the categories of personal data
  - Data of individuals to be disclosed or made available
  - Processing times
  - Limitations and scope

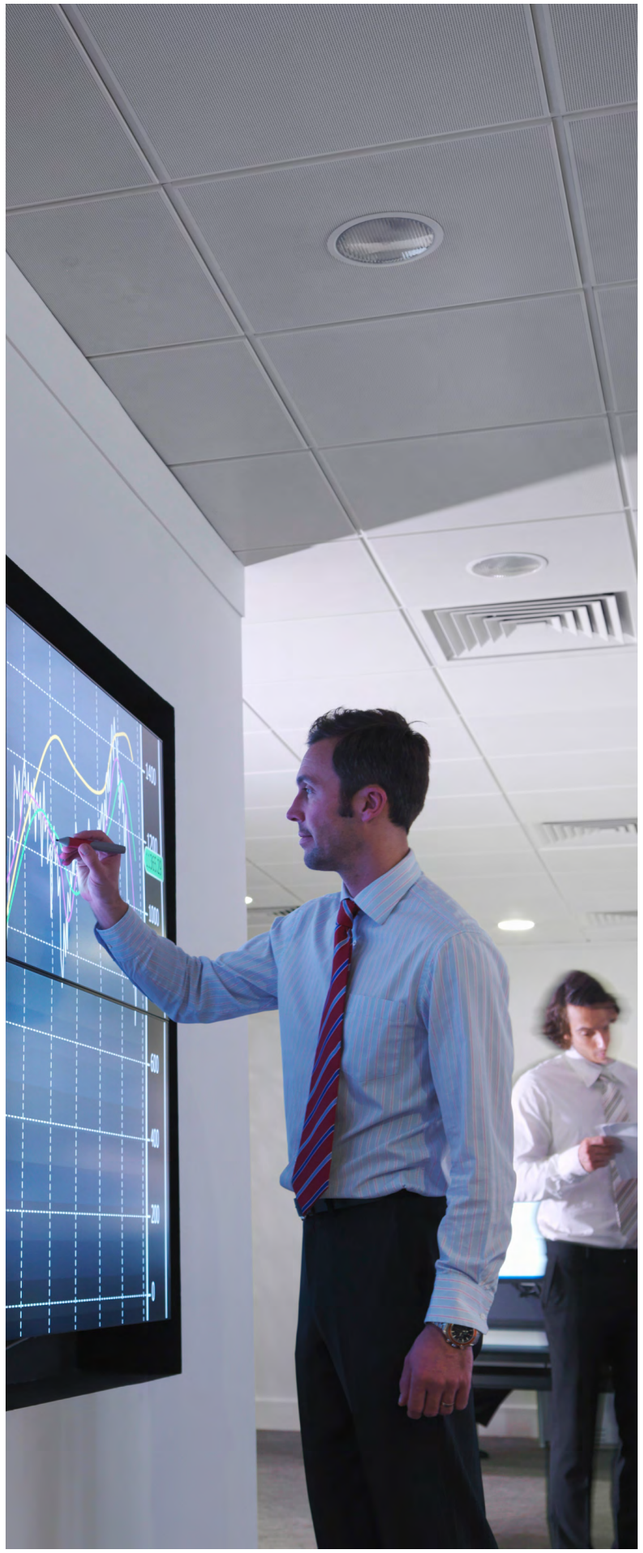
  - The mechanism for erasing/modifying personal data or its processing
  - Purpose of processing
  - Information related to processing data across borders
  - Statement of the technical and organizational measures related to information security and processing operations
- Provide proof of commitment to adhering to the Federal Data Protection Law upon the request of the controller or the supervisory authority.
- Implement processing in accordance with the controls specified in the Federal Data Protection Law and upcoming executive regulations.

Reporting personal data breaches:
- The data controller must report any breach or violation of personal data to the supervisory authority at the earliest possible time from becoming aware of the incident. The notification must contain:
  - Statement of the intrusion, to include its forms, its causes, and the approximate number of records.
  - Data regarding the DPO.
  - Potential and expected effects of the breach or violation.
  - Statement of the proposed implementation to counter the breach or violation.
  - Documented breach or violation and the corrective actions taken.
  - Any data or documents requested by the supervisory authority.
- The data processor must notify the controller if they become aware of any breach or violation of personal data.

04 Data Protection Officer (DPO)

Appointment:
- A DPO must be appointed by the data controller and data processor who possesses the capabilities required to process personal data.
- The DPO may be employed/authorized by the data controller or data processor, either inside or outside of the country.
- The contact address of the DPO must be provided to the Federal Data Regulator (UAE Data Office) by the data controller and data processor.

Data protection officer duties:
- Verify the procedures for the data controller and data processor.
- Receive requests and complaints related to personal data.



- Provide technical advice related to the evaluation procedures and periodic assessments of the personal data protection systems.
- Act as a link between the data controller, data processor, and the supervisory authority where necessary.
- Tasks specified in the executive regulations of the Federal Data Protection Law that will be published.
- Maintain confidentiality of the information and data received throughout the implementation of their duties.

Data controller and data processor duties to the DPO:
- Provide the DPO with the means to ensure that the tasks assigned to them can be performed.
- Provide relevant data regarding the protection of personal data in a timely manner.
- Ensure the DPO has the necessary support and resources required.
- Not to terminate or discipline the DPO based on his performance of duties in accordance with the Federal Data Protection Law.
- Ensure that the DPO is not assigned tasks that may lead to a conflict of interest.
- Communicate with the DPO regarding personal data and its processing.

05 Data subject rights

Right of access to information:
- The data subject has the right to request the following information:
  - Confirmation that the data subject's personal data is subject to processing.
  - The purpose of processing.
  - Automated processing decisions and profiling.
  - Type of personal data subject to processing.
  - Individuals authorized to obtain the personal data of the data subject.
  - Controls and standards for periods of storage and preservation of personal data.
  - Procedures for personal data rectification, erasure, or restriction.
  - How to submit complaints to the supervisory authority.
  - Protection measures related to cross border data processing.
  - Breach events that involve risk to the data subject's personal data.

- The data controller may reject the request for information related to a breach in the following cases:
  - The request is untrue or exaggerated.
  - The request is not feasible due to technical reasoning.
  - The request contradicts investigations by authorities.
  - The request adversely affects the data controller's efforts to protect data.
  - The request violates the privacy and confidentiality of third parties' personal data.

Right to request transfer of personal data:

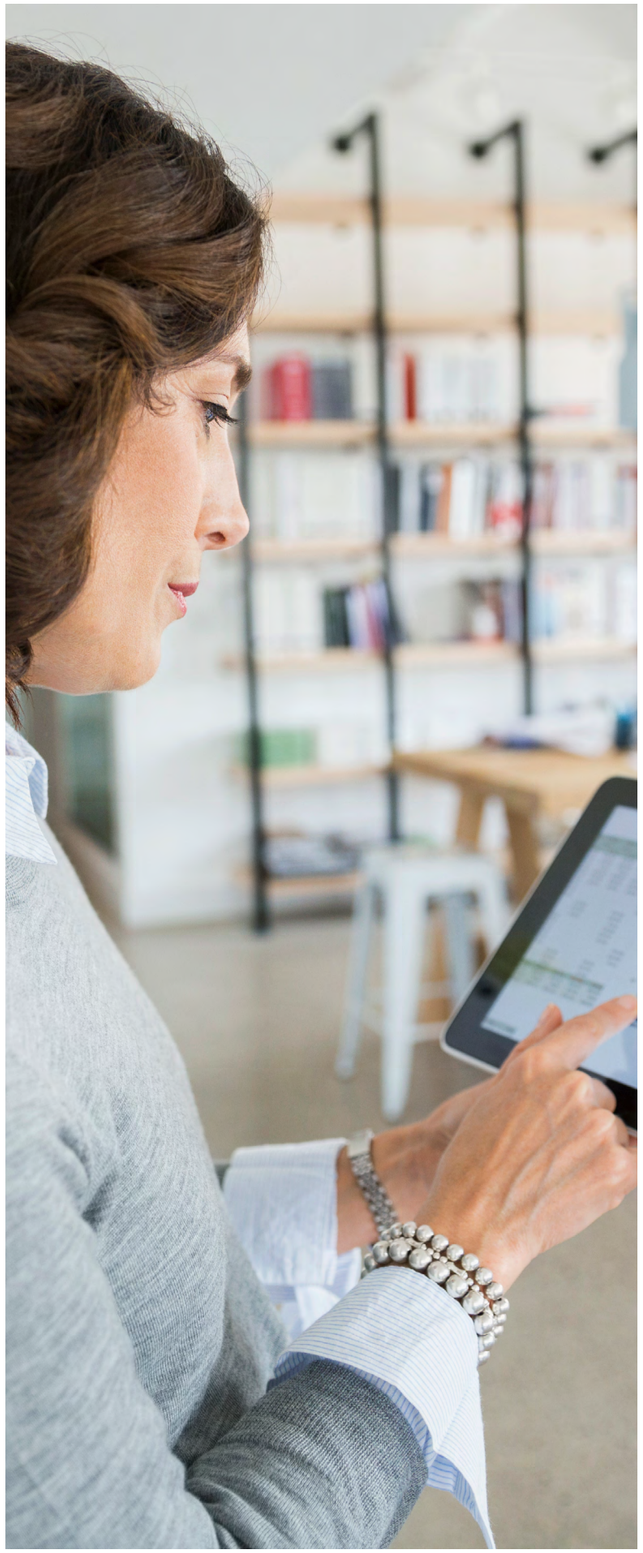
- Data subjects have the right to obtain their personal data that has been provided to the controller for processing.
- Data subjects have the right to request the transfer of their personal data to another controller when feasible.

Right to correct or delete personal data:

- Data subjects have the right to request the correction of their inaccurate personal data to be completed in a timely manner.
- Data subjects have the right to request the erasure of personal data in the following cases:
  - The personal data is no longer necessary for the purposes it was collected.
  - The data subject has revoked consent on which processing was based.
  - The data subject objects to the processing of personal data.
  - The absence of legitimate reasons for the data controller to continue processing.
  - The processing of personal data was carried out in violation of the Federal Data Protection Law.

Right to restrict processing:

- Data subjects have the right to request to restrict processing of their data in the following cases:
  - The data subject objects to the processing of their personal data.
  - The data subject objects to the accuracy of their personal data.
  - The processing was carried out in violation of the Federal Data Protection Law.
  - The data subject's needs for claiming or defending their legal rights.
- The data controller may proceed with the processing of personal data without consent in the following cases:
  - Limited to storing personal data.
  - Processing to protect the public interest or third-party rights.



  - Necessary to establish a legal claim or defense of rights.
  - The data controller must inform the data subject if the restrictions have been lifted and processing continues.

Right to stop processing:

- The data subject has the right to object to the processing of their personal data in the following cases:
  - The processing was carried out in violation of the Federal Data Protection Law.
  - The processing was carried out for marketing purposes including profiling relating to direct marketing.
  - The processing was carried out for scientific or statistical research and not for the public interest.

Right of processing and automated processing:

- The data subject has the right to object to any decisions issued by automated processing.
- The data subject may not object to the automated processing in the following cases:
  - If the processing is necessary to enter a contract between the data subject and the data controller.
  - If the decision is authorized by law.
  - If the data subject or their guardian have expressed consent.
- The data controller must apply procedures to protect the privacy and confidentiality of personal data while ensuring that the data subject can request access to their personal data and challenge the decisions of automated processing.

Methods of communication with the data controller:

- The data controller must provide appropriate and clear methods of communication to allow the data subject to exercise any of their rights.

06 Data protection

Security of personal data information:

- Appropriate technical and organizational security measures should be in place to protect all personal data in accordance with the global standards, in particular:
  - Encryption of personal data and data hiding mechanisms such as pseudonymization.
  - Procedures to ensure continuity for confidentiality and integrity, validity and flexibility of personal data.
  - Procedures to retrieve and access personal data in event of technical failures.
  - Procedures to support testing and evaluation of security measures.
- Evaluation of security measures should take the following into account:
  - The risks associated with processing personal data, such as loss, modification, or disclosure.
  - The cost, nature, scope, context, and processing of personal data and their potential risks accordingly.

Assessment of the impact of personal data protection:

- The data controller must assess the impact of proposed processing operations on the protection of personal data before carrying out the processing. This assessment should include the evaluation of the following:
  - A clear and systematic explanation of the processes for the protection of personal data and its purpose.
  - Potential risks to privacy and confidentiality of personal data.
  - Measures to reduce the potential risks.
- Assessments of the impact of personal data protection are necessary in the following cases:
  - processing personal data through automated processing that have legal consequences or would seriously affect the data subject.
  - Processing will take place on a large volume of sensitive personal data.
- The data controller must coordinate assessments with the data protection officer.
- The data controller must review the evaluation criteria periodically.
- The supervisory authority will release a list of processing operations that do not require assessments.

07 Cross-border transfer of personal data

Cross-border transfer of personal data:

- Personal data may be transferred outside of the country in the following cases only:
  - The country that the personal data will be transferred to has specific legislation for personal data protection through a supervisory authority (requirements will be specified in the executive regulation).
  - The country has agreements related to the protection of personal data with the countries the data will be transferred to.
  - The supervisory authority must be notified before the cross-border transfer of sensitive personal data.
- Personal data may also be transferred outside of the country if the following criteria are met:
  - The data controller guarantees to protect the personal data.
  - The data subject has expressed consent for cross border data transfers.
  - The transfer is necessary to preserve the interests of the data subject.
  - The transfer is necessary to carry out legal obligations.
  - The transfer is necessary to conclude/implement a contract between the data controller and the data subject.
  - The transfer is necessary to protect the public interest.

08 Final provisions

Communication with the supervisory authority:

- The data controller or data processor must notify the supervisory authority regarding personal data processing operations that are undertaken, and any amendments made.
- The supervisory authority must then refer the notification to the local authority through the agreed-upon coordination procedures.

Complaints:

- The data subject may file a complaint with the supervisory authority if they have reason to believe that any violation of the provisions of the Federal Data Protection Law has occurred.
- The office shall receive complaints submitted by the data subject and refer them to the competent local authority for consideration and decision.
- Any interested party may submit a complaint to the supervisory authority regarding any decision, punishment, or action taken within 30 days of the notification of the decision. This must be responded to within 30 days of submission by the supervisory authority.

Administrative fines:

- Violators of the provisions of the Federal Data Protection Law shall be punished with a fine.
- The supervisory authority will direct violators to take corrective measures, such as appointing a DPO.

Executive decisions:

- The Council of Ministers shall issue executive regulations by the end of March 2022 regarding the implementation of the provisions of the Federal Data Protection Law, and rules and regulations related to the protection and processing of personal data.
- The Council of Ministers may authorize the supervisory authority to issue controls and systems for any provisions of the Federal Data Protection Law.

Reconciliation:

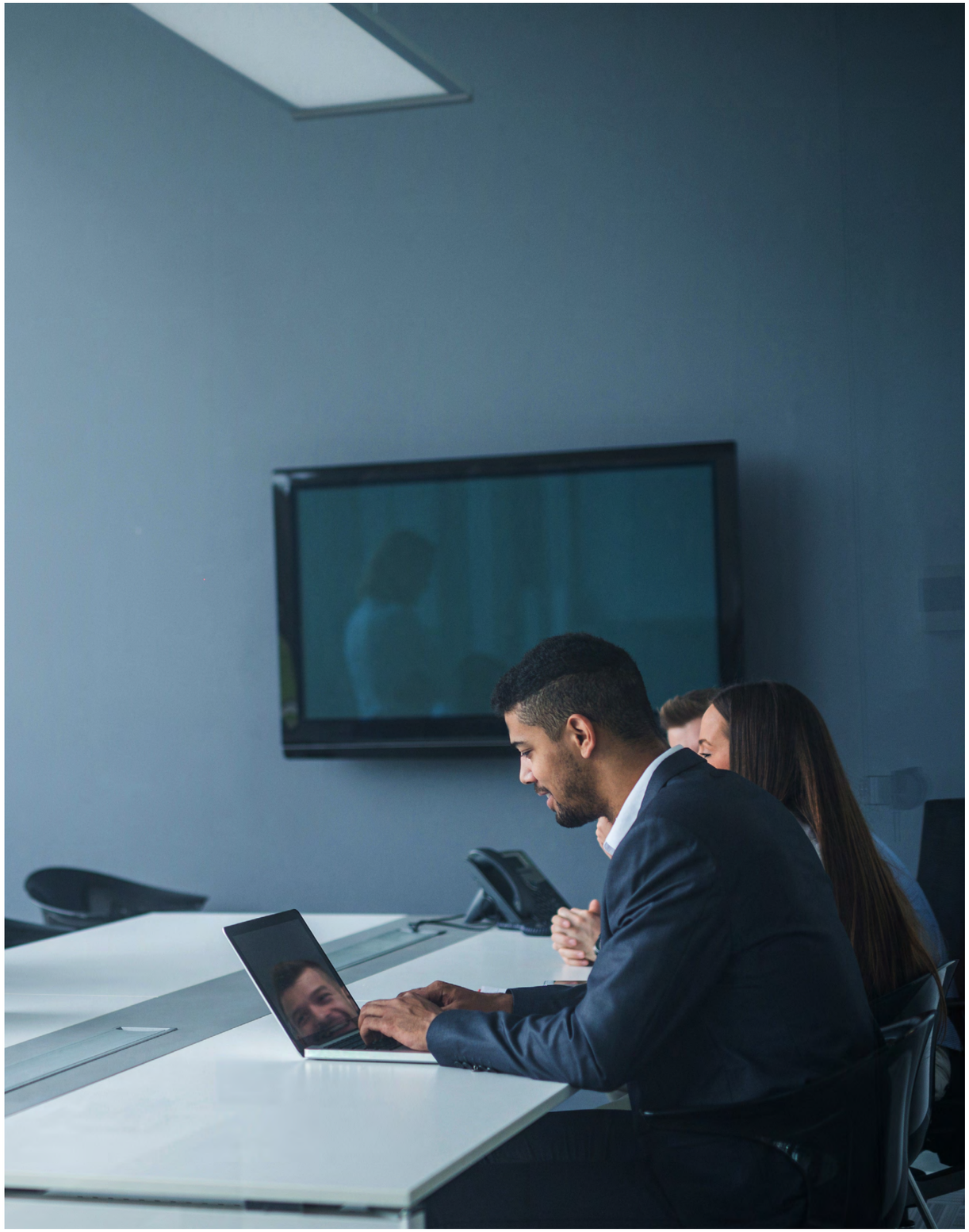
- Those who are addressed by the provisions of the Federal Data Protection Law shall adjust their status within two years from the date of its enforcement.

Cancellations:

- Every provision that contradicts or conflicts with the Federal Data Protection Law may be repealed.

Publication and implementation:

- This Federal Data Protection Law will be published in the official gazette and shall come into force six months after the date of its publication.



What are the penalties of non-compliance?

Administrative penalties can be imposed as part of a decision by the Council of Ministers. The level of sanctions is expected to be specified in the subsequent executive regulations. Fines (amount to be published), depending on the corresponding contraventions of the Federal Data Protection Law.

The UAE Federal Data Protection Law will potentially provide a six-month period for existing establishments, giving data controllers, data processors, and the supervisory authority time to adjust to the requirements of the new regulation and avoid technical non-compliance of the new regulation. This six-month period will start once the executive regulations are published, towards the end of march 2022, which means that relevant organizations must be compliant towards the end of September 2022.

What can we expect based on the GDPR?

Fines and penalties imposed due to GDPR breaches provide insight into the possible trends that will be seen once the UAE Federal Data Protection law is enforced. Statistics calculated by CMS Legal, regarding public GDPR breaches between its enforcement in 2018 up till 2022, identified that there are over 900 instances of organizations being issued with fines for violating GDPR regulations, which when combined, resulted in over €1.5 billion in penalties.

Analysis of GDPR fines over time has shown an increase in the number of GDPR violations per year, increasing by 113% between July 2020 to July 2021, while the average cost of fines per year has also increased. The largest GDPR breach fine was issued to Amazon in 2021, amounting to an unprecedented €746 million.

It is possible to forecast the adoption and enforcement of the UAE Federal Data Protection Law using trends seen over the past few years since GDPR has been implemented. The number of violations reported will probably grow yearly, along with the cost of fines.

Organizations that will be affected by the UAE Federal Data Protection Law must be proactive and ensure that they adhere to regulations to protect any personal information that they possess and prevent being fined. The top causes of GDPR violations provide visibility of significant concerns that organizations affected by the UAE Federal Data Protection Law should identify within their own data handling procedures.

Top causes of GDPR violations:

01 Insufficient legal bases for processing personal information

02 Insufficient measures in place to ensure information security

03 Lack of compliance with general principles of data processing

04 Lack of fulfilling the rights of data subjects

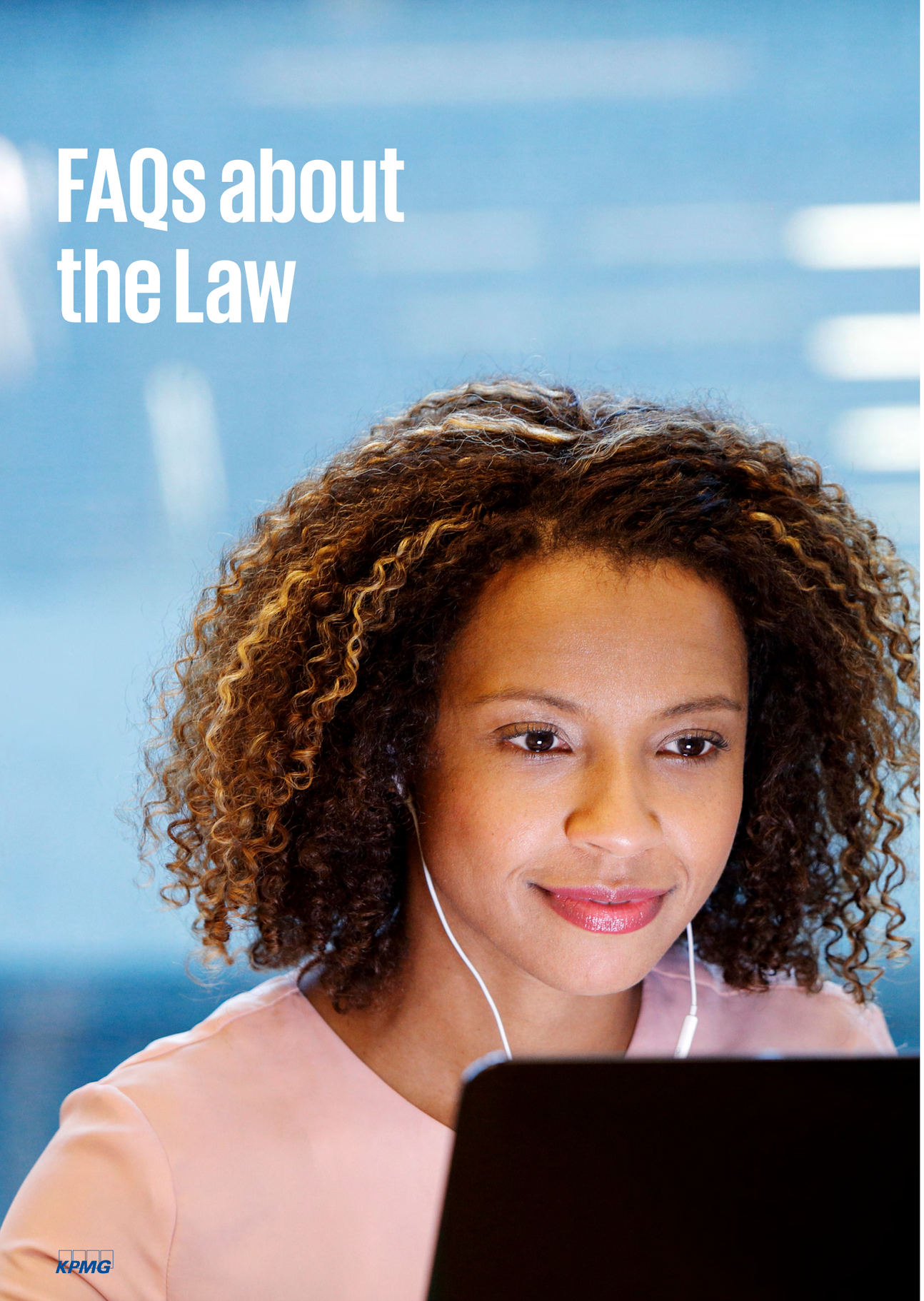
05 Lack of cooperation with relevant supervisory authorities

06 Insufficient notification of data breaches and incidents

07 Lack of a designated DPO

08 Lack of agreement for data processing

FAQs about the Law



Who does the Federal Data Protection Law apply to?

- Organizations within the UAE that process personal data.
- Organizations outside of the UAE that process personal data of the data subjects in the UAE.

Who is exempt from the Federal Data Protection Law?

- Government data, government authorities who control or process personal data.
- Personal data with the security and judicial authorities.
- Health personal data is governed by legislation regulating the protection and processing of such data.
- Banking and credit personal data and information which are governed by legislation regulating the protection and processing of such data e.g. consumer protection regulation.
- Companies and establishments located in the financial free zones in the state which have their own personal data protection legislation e.g. DIFC and ADGM.

Does the UAE Federal Data Protection Law contain general security obligations for controllers and processors?

- Yes, there are security requirements highlighted in the UAE Federal Data Protection Law.
- There is a specific section (article 20) that highlights the types of controls that organizations should implement such as encryption, anonymization, etc.

How can organizations comply with cross-border data transfers regulations?

- The new UAE data protection law highlights that transfers can only take place to approved countries (the list is yet to be released by the new UAE data office) or in limited other circumstances (contractual necessity; public interest).
- We expect the upcoming executive regulations to include details of approved countries.
- Organizations can create RoPA or data flow diagrams (DFDs) to create a high-level overview of countries where their data is flowing.

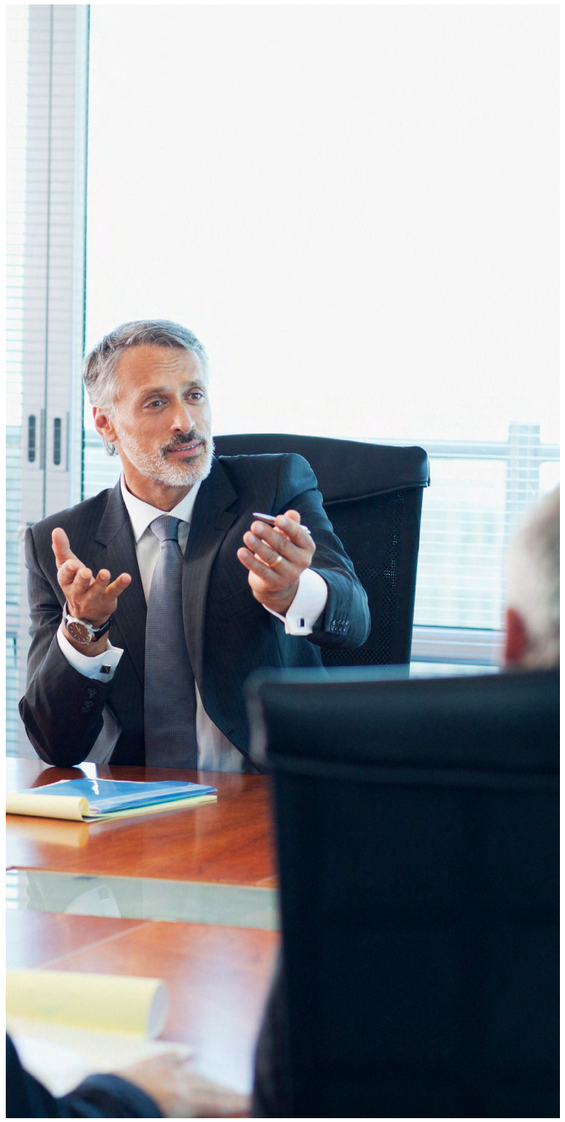
When is the compliance deadline of the Federal Data Protection Law?

- The Federal Data Protection Law came into force on 2nd January 2022.
- The executive regulations have not yet been published.
- Organizations will have six months after the executive regulations are published to comply with the Federal Data Protection Law.

Who will monitor compliance with the Law?

UAE's Data Office will be established according to the Federal decree-law no 44 of 2021, which was enacted at the same time as that of Federal Data Protection Law. This Data Office will:

- Ensure protection of personal data in the UAE.
- Be the sole authority which in the future will issue further policies regarding data privacy, handle complaints, investigate data breaches.
- Impose penalties for non-compliance against the Law.



What are the next steps if organizations don't have a data privacy framework in place?

- Organizations that have not already developed a data privacy framework in line with the GDPR will need to carry out a more comprehensive program of work. Some of the activities will include (but are not limited to):

Assess:

- Organizations need to first identify if the Federal Data Protection Law is applicable to them.
- If so, a compliance current state assessment is necessary to be performed against the Federal Data Protection Law to determine gaps.
- Identify if a DPO is required.

Design:

- Develop a privacy framework and governance structure.
- Develop applicable policies, procedures, standard operating procedures (SOPs), templates and controls.

Implement:

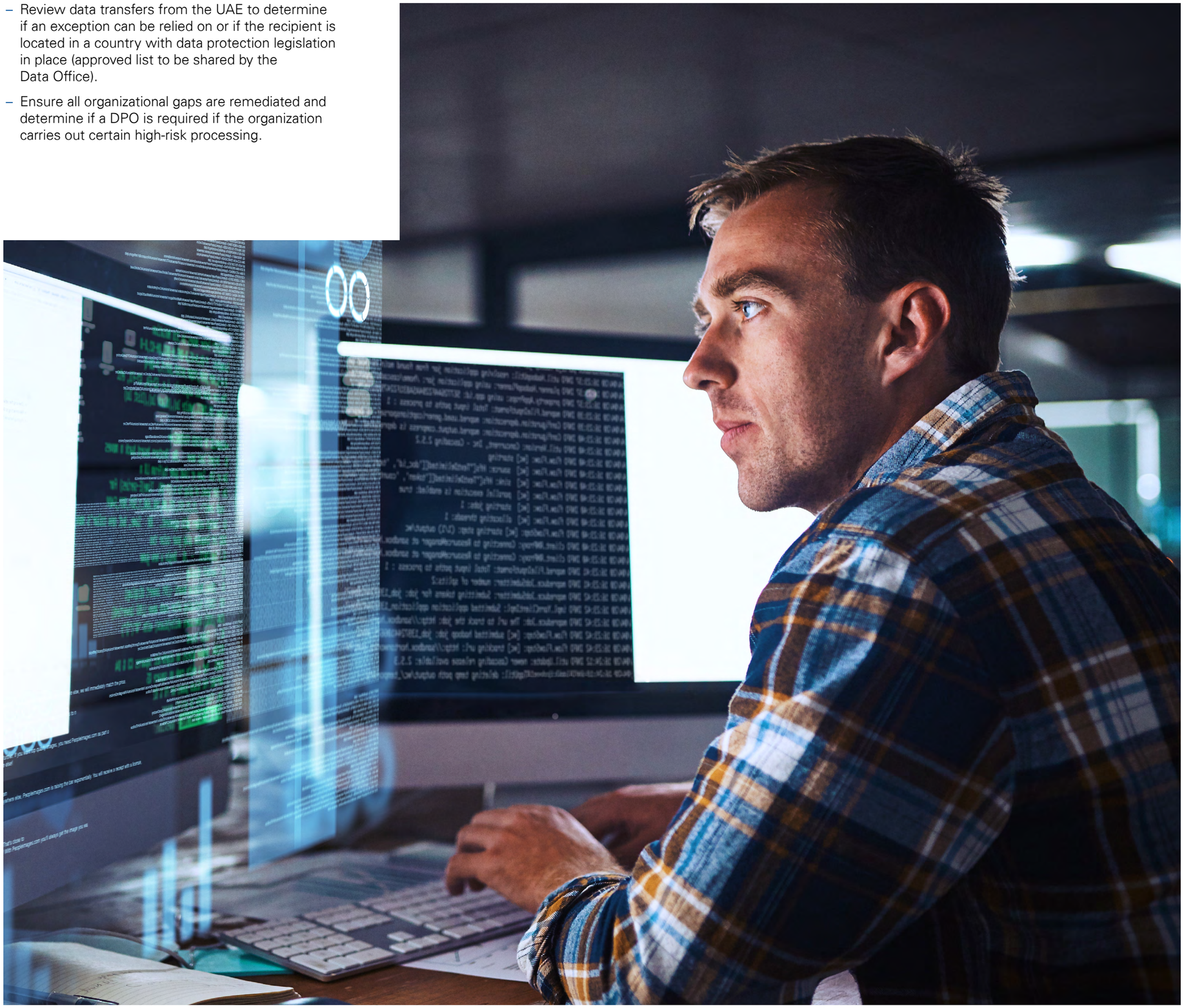
- Establish a RoPA and conduct DPIAs.
- Implement data subject rights and consent management processes.
- Implement third party management procedures and data breaches processes.
- Implement appropriate technical and organizational measures are in place to secure data.

Monitor:

- Develop checklist, compliance dashboards as required to monitor progress and compliance.
- Conduct privacy awareness and training sessions.

What are the next steps if organizations already comply with the GDPR?

- Organizations that already comply with the GDPR will be able to take fewer additional compliance steps.
- However, these organizations should start with a gap analysis activity, to find out what are the deltas with other data protection laws and perform adjustments according to the new UAE Federal Data Protection Law, for example (not limited to):
  - Establish another legal basis for processing that relies on legitimate interests under the GDPR.
  - Update RoPAs to comply with the specific requirements of the Data Protection Law.
  - Ensure the organization can comply with data breach reporting requirements.
- Review data transfers from the UAE to determine if an exception can be relied on or if the recipient is located in a country with data protection legislation in place (approved list to be shared by the Data Office).
- Ensure all organizational gaps are remediated and determine if a DPO is required if the organization carries out certain high-risk processing.



How can KPMG assist?

Our approach assists clients in achieving sustainable data protection and improved compliance. By gaining a better understanding of existing data practices and the impact of new regulations on business strategies and models, we support organizations in aligning their information protection plans with dynamic business and compliance priorities.

We perform data privacy and protection engagements, leveraging an ecosystem of innovative technology partners and privacy management solutions:

Assess

- Data privacy maturity assessments
- Data privacy gap assessments against applicable laws and regulations
- Data privacy audits
- Current state gap assessments
- Remediation reports
- Roadmap development

Design

- Data privacy strategy and program definition
- Data privacy framework design
- Data privacy policies, procedures, templates
- Contract and notice documentation
- Privacy governance structure and target operating model
- Data privacy management tool design

Implement

- Data privacy framework implementation
- Data discovery and classification
- Data mapping, RoPAs, DPIAs
- Data subject requests
- Consent management
- Data breach management
- Third-party management
- Information security controls
- Privacy management tool implementation

Monitor and train

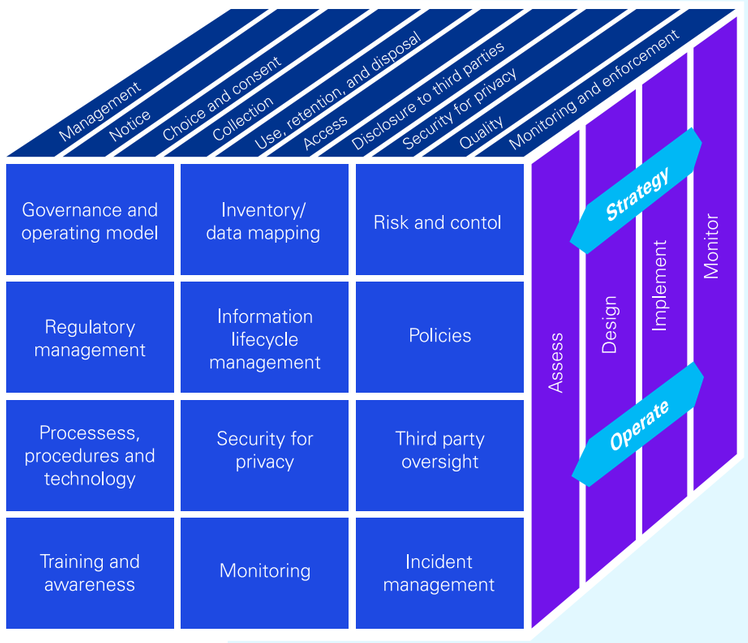
- DPO-as-a-service: End-to-end data privacy management services
- Checklist, KPIs, compliance dashboards, and templates, as required to monitor progress and compliance
- Privacy awareness sessions
- Role-based advance training
- Privacy retainer advisory services

Our global data privacy footprint

KPMG's cyber security and privacy practice is present in major markets around the world – 29 countries in total. We assist organizations in transforming their security, privacy, and continuity controls while maintaining the confidentiality, integrity, and availability of critical business functions.

KPMG's privacy management framework

The KPMG privacy management framework is modular and is composed of distinct components that organizations may employ to promote accountability with applicable privacy laws and regulations. We aim to provide a practical and pragmatic structure for organizing the day-to-day management, and the oversight required to mitigate privacy risk exposures. KPMG's approach includes steps to assess, monitor, design, strategize, implement, and operate privacy requirements.



For almost 50 years, KPMG Lower Gulf Limited has been providing audit, tax and advisory services to a broad range of domestic and international, public and private sector clients across all major aspects of business and the economy in the United Arab Emirates and in the Sultanate of Oman. We work alongside our clients by building trust, mitigating risks and identifying business opportunities.

KPMG Lower Gulf is part of KPMG International Cooperative's global network of professional member firms. The KPMG network includes approximately 236,000 professionals in over 144 countries. KPMG in the UAE and Oman is well connected with its global member network and combines its local knowledge with international expertise, providing the sector and specialist skills required by our clients.

KPMG is widely represented in the Middle East: along with offices in the UAE and Oman, the firm operates in Saudi Arabia, Bahrain, Kuwait, Qatar, Egypt, Jordan, the Lebanon, Palestine and Iraq. Established in 1973, the Lower Gulf firm now employs approximately 1,783 people, including about 190 partners and directors across the UAE and Oman.

As we continue to grow, we aim to evolve and progress, striving for the highest levels of public trust in our work.

Our values are:

Integrity: We do what is right;

Excellence: We never stop learning and improving;

Courage: We think and act boldly;

Together: We respect each other and draw strength from our differences;

For Better: We do what matters.

To meet the changing needs of our clients, we have adopted an approach aligned with our global purpose: Inspiring Confidence, Empowering Change. Our three pillars **– exceptional quality of service, an unwavering commitment to the public interest, and building empowered teams** – are the foundation of our firm.

Disclaimer: Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Contact us

Timothy Wood
Partner
Digital and Innovation-Cyber

KPMG Lower Gulf Limited

+971 56 409 6842
timothywood@kpmg.com

Chris Toumazos
Associate Director,
Digital and Innovation-Cyber

KPMG Lower Gulf Limited

+971 56 504 9672
ctoumazos1@kpmg.com

www.kpmg.com/ae
www.kpmg.com/om

Follow us on:

@kpmg_lowergulf

Publication name: United Arab Emirates – New Federal Data Protection Law 2021

Publication number: 3936

Publication date: March 2022