Achieving Data Protection Compliance in the UAE: Essential Guidelines for Businesses

The UAE Federal Decree-Law No. 45/2021 on Data Protection (**DPL**) came into force on 2 January 2022 and is the first comprehensive data protection law to exist at federal level in the UAE. Prior to then, the UAE did not have a stand-alone federal data protection law.

The DPL aims to govern the practices of organisations and businesses that collect, process and store personal data of individuals in a manner consistent with global practices, including the EU's General Data Protection Regulation (GDPR) which is still regarded today as the "gold standard".

The DPL is also supplemented by additional Executive Regulations (**Regulations**) although over a year on since the DPL came into force, we still await their publication. The Regulations remain a crucial piece of the puzzle, as not only is it expected that these will set out key information around fines and other penalties for non-compliance, but also that once they are published, businesses will only have a short 6 month period within which to comply with the DPL. Businesses must therefore take steps to comply with it or face fines and other sanctions as well as reputational damage. For businesses waiting for the Regulations, delaying action could be risky. It is advisable to act now and start implementing necessary measures to ensure compliance, rather than waiting until it may be too late.

In this article, we will provide a brief overview of the DPL, provide practical examples, and highlight 10 key recommendations and practices that businesses can begin to implement ahead of the Regulations being published.

Brief Overview of the DPL

The DPL applies to all processing of personal data within the UAE territory, whether by automated or manual means, as well as any organisation or individual processing data. The DPL also has extra-territorial effect and will apply to all data generated and processed outside of the UAE where individuals in the UAE are concerned. What this means in practice is that, amongst other things:

- A UAE-based company that processes personal data of its customers must comply with the DPL, whether its uses automated software or manual methods.

- An international company, with no physical presence in the UAE, that processes personal data of UAE residents is also subject to the DPL. For instance, an e-commerce platform headquartered in the US but serving customers in the UAE must adhere to the DPL.

- If a UAE resident uses a service provided by a company based outside the UAE, the data processed by that company still falls under the jurisdiction of the DPL. This could include, for example, a social media platform or an email service provider.

The DPL also covers various types of personal data, including identification data, financial data, location data, as well as more sensitive personal data such as genetic and biometric data.

However, there are some notable exceptions - for instance, the DPL will not apply to i) government data or government authorities that process personal data, ii) health and banking or credit personal data to where there is already applicable legislation regulating the processing of such data, iii) entities within UAE free zones that are already governed by their own data protection laws such as the DIFC and ADGM, etc. These exceptions help ensure that the DPL does not conflict with existing regulations or create redundancies for organisations operating in specific sectors or free zones.

For the first time, individuals are also afforded a number of rights under the DPL. These developments can be considered game changers for the UAE, as they introduce significant advancements and improvements to what is currently being undertaken. Here are some practical examples of these rights:

1. **Right to know what data is collected**

   Example: A customer can request an online retailer to provide information about the personal data collected about them, such as their name, address, and purchase history.

2. **Right to know the purpose of processing**

   Example: A user of a fitness app can ask the app provider to clarify the reasons for collecting their workout data, such as improving the app's features or providing personalised exercise recommendations.

3. **Right to know how long data is retained for**

   Example: A former employee can inquire about the duration their former employer retains their personal information, like contact details or performance records, after their departure from the company.

4. **Right to have their data rectified**

   Example: A user who discovers incorrect information in their online banking profile can request the bank to correct the error, such as updating their address or phone number.

5. **Right to have their data deleted**

   Example: A user who no longer wishes to use a social media platform can request the deletion of their account and all associated personal data, like photos, messages, and friends list.

These rights empower individuals to better manage and protect their personal information. In preparation for the upcoming DPL, businesses can implement several measures to ensure compliance and create a robust data protection framework, as follows:

10 Key Recommendations & Practices for UAE Businesses

1. Conduct a Data Audit

Businesses should carry out a comprehensive data audit to identify the types of personal data they collect, process, store, and share. This will help them to better understand their data processing activities and align their practices with DPL requirements.

2. Implement Data Subject Rights Procedures

Establish processes to handle data subject rights requests, such as requests for access, rectification, and deletion of personal data. Businesses in the UAE should also be able to respond to these requests within the timeframes specified, which may yet be detailed in the Regulations.

3. Review and Update Data Processing Agreements

Assess existing contracts with third-party data processors to ensure they meet the DPL's requirements. Businesses should update or renegotiate agreements as necessary to establish clear responsibilities and obligations for data protection.

4. Implement Appropriate Security Measures

Businesses must implement appropriate technical and organisational measures to ensure the security and confidentiality of personal data. These measures are essential to prevent the unauthorised access, disclosure, alteration, or destruction of personal data and may include data encryption, data backup and recovery, and regular system updates and patches.

5. Have a Data Breach Response Plan

A data breach response plan outlines the procedures and protocols in the event of a data breach, and should include incident reporting, investigation, and notification procedures to ensure timely response in order to minimise the harm caused to individuals whose data is breached.

6. Have an Adequate Consent Collection Mechanism

Under the DPL, the primary or default basis on which businesses may lawfully process personal data is a data subject's express and specific consent and for this reason, businesses must ensure they have an adequate consent collection mechanism in place. There are of course exceptions to the rule and the Regulations may well set out further cases where consent is not specifically required.

7. Implement Appropriate Policies

Businesses should develop and implement comprehensive data protection policies and procedures (both internal and external) that include clear information on the collection and processing of personal data as well as guidelines for data protection, security, retention, and disposal. These should be reviewed and updated regularly to ensure compliance with the DPL.

8. Provide Data Protection Training

Businesses should provide adequate training to their employees on the DPL and their responsibilities regarding personal data protection. This includes training on the awareness of the risks associated with processing personal data as well as the business' policies and procedures for handling personal data.

9. Appoint a Data Protection Officer (DPO)

Depending on the business' processing activities, they may be required to appoint a DPO (for instance if they are processing large volumes of sensitive personal data). A DPO would effectively be responsible for implementing and overseeing the DLP compliance program and would therefore need to have relevant experience and expertise to manage data protection matters.

10. Conduct a Data Protection Impact Assessment (DPIA)

A DPIA is a risk assessment exercise to evaluate the data privacy implications of processing personal data, the potential harm to individuals, and mitigation measures. Businesses that carry out high-risk processing activities must perform DPIAs and document the findings to demonstrate compliance with the DPL.

Conclusion

The DPL is a significant development in the UAE's data protection landscape. Whilst the exact timeline for the publication of the Regulations remains unclear, organisations should not delay in taking proactive steps to ensure compliance and prepare for the new regulatory landscape.

The DPL presents an opportunity for businesses to review and enhance their data protection practices, making it essential for them to act now and get their ship in order. Waiting for the Regulations to be published may leave insufficient time for businesses to make the necessary adjustments, increasing the risk of non-compliance and potential penalties. By embracing the DPL and acting today, businesses can position themselves as responsible and forward-thinking entities, ready to navigate the ever-evolving data protection landscape.

For those seeking guidance, our team of experts, well-versed in both the GDPR and local UAE laws, is available to assist businesses in navigating the complexities of data protection and ensuring compliance with the DPL. Their expertise will prove invaluable as your business adapts to the new regulatory environment.

For further information and guidance on how we can assist your business in complying with the DPL, please get in touch.

Key contacts

Saleem Adam
Partner, Int Corporate
+971 2 410 7611
SAdam@trowers.com

Sapna Desai
Associate, Int Corporate
+971 4 302 5138
SDesai@trowers.com