MEYER – REUMANN & PARTNERS

Elena Schildgen
Dr. Michael Krämer
Tarek Jairwdeh
Dr. Sara Corradi
Verena Nosko
Christine Baltzer-Zacharias
Natacha El Azar
Katharina Jung

UAE AND DIFC CORPORATE COMPLIANCE SERIES

PART 3: Data Protection Compliance – Safeguarding Data in a Digital Era

Data protection has become a critical aspect of doing business in the UAE and DIFC. Companies are expected to handle personal and sensitive information responsibly, not only to comply with the law but also to build trust with customers, partners and employees.

This article, the final part of our three-part series on corporate compliance, explores the legal frameworks, key principles and practical steps for data protection in both onshore UAE and the DIFC.

A. LEGAL FRAMEWORK AND SCOPE

Onshore, the primary law is Federal Decree-Law No. 45 of 2021 ("**PDPL**"), which applies to UAE-based processing and data relating to UAE residents. In the DIFC, Data Protection Law No. 5 of 2020 ("**DIFC Law**") applies, covering DIFC entities and processing occurring within the DIFC. DIFC Law is closely aligned with the EU General Data Protection Regulation ("**GDPR**"), while PDPL codifies rights and obligations for individuals and companies onshore.

Understanding which law applies is essential for companies, as requirements and procedural details differ depending on where the business is set up. Policies,

Elena Schildgen
Dr. Michael Krämer
Tarek Jairwdeh
Dr. Sara Corradi
Verena Nosko
Christine Baltzer-Zacharias
Natacha El Azar
Katharina Jung

processes and internal practices must align with the applicable law to remain compliant and avoid penalties.

B. DATA, PRINCIPLES AND RIGHTS

Personal Data

Personal data includes identifiers such as names, addresses, dates of birth, phone numbers, IP addresses or location data, opinions (for example HR appraisals) and photos or videos. Certain types of information are classified as sensitive personal data, which requires additional protection. This includes ethnicity, health information, political views, criminal convictions and genetic data. For sensitive data, explicit consent is required; simply stating its use in a privacy policy is not sufficient.

In practice, explicit consent could be collected via a clear, separate consent form or checkbox where the data subject actively agrees to the specific use of their sensitive data. For example, ticking a box to confirm consent before submitting health information for HR purposes would be considered as explicit consent.

Principles

Compliance is guided by seven key principles, which apply to any interaction with personal data, whether collecting, storing, organising or deleting it. These principles include:

1. **Lawfulness, fairness and transparency**: Data must be processed legally, fairly and in a way that is transparent to the data subject.

2. **Purpose limitation**: Personal data should only be collected for purposes directly related to the company's objectives and must not contradict the provisions of the law.

3. **Data minimisation**: Data collected should be adequate, relevant and limited to what is necessary for the intended purpose.

4. **Storage limitation**: Personal data should not be kept longer than necessary to achieve the intended purpose.

5. **Accuracy**: Data must be accurate, kept up to date and reasonable steps should be taken to correct or erase inaccurate information without delay.

Elena Schildgen
Dr. Michael Krämer
Tarek Jairwdeh
Dr. Sara Corradi
Verena Nosko
Christine Baltzer-Zacharias
Natacha El Azar
Katharina Jung

6. **Confidentiality and security**: Adequate technical and organisational measures must be implemented to safeguard personal data against unauthorised access, loss or damage.

7. **Accountability**: Companies must be able to demonstrate compliance with data protection laws and principles by having appropriate measures, policies and retention practices in place.

Following these principles helps companies manage risk and protect the individuals whose data they hold.

Data Subject Rights

Both onshore PDPL and DIFC Law grant individuals rights over their personal data, including the ability to access, correct or request deletion of their information. Companies must have procedures in place to respond to these requests promptly and in line with the applicable law.

C. COMPLIANCE, BREACH AND PENALTIES

While the core principles of data protection are similar, the procedural requirements and enforcement mechanisms differ between onshore UAE and DIFC law. The table below highlights key differences in legal framework, scope, breach notification and penalties, helping companies understand what applies depending on their jurisdiction.

Aspect	Onshore UAE (PDPL)	DIFC Law
Legal Framework	Federal Decree-Law No. 45 of 2021	Data Protection Law No. 5 of 2020 (GDPR-aligned)
Scope	UAE-based processing and UAE residents	DIFC entities and processing in DIFC
Legal Basis for Processing	Lawfulness, consent and other statutory grounds	Lawfulness, consent, legitimate interests and other codified grounds
Breach Notification	Notify UAE Data Office, investigate, report findings	Notify Commissioner "as soon as practicable" with full details
Penalties	Cybercrimes Law / Penal Code (pending implementing regulations)	Fines up to USD 100,000 depending on breach type

Data Breach

A data breach occurs when personal or sensitive information is accessed, disclosed, lost or destroyed in an unauthorised manner. If a breach occurs, act quickly: contain

the incident, assess the impact, notify the relevant regulator and affected individuals, remediate the cause and document your actions. Even minor incidents should follow this process, ideally using a pre-prepared checklist.

D. FINAL THOUGHTS

Data protection is no longer optional. Companies operating in the UAE and DIFC must integrate privacy and security into their everyday operations. By understanding the applicable laws, protecting sensitive information, respecting data subject rights and responding promptly to breaches, businesses can maintain compliance and safeguard their most valuable asset: trust.

For companies seeking guidance on data protection compliance, risk assessment or establishing internal privacy frameworks, our team at Meyer-Reumann & Partners will be pleased to help. Get in touch with us by emailing our lawyer Natacha El Azar at natacha@meyer-reumann.com to discuss how to strengthen your governance practices.

This concludes our three-part series on corporate compliance in the UAE and DIFC! While the laws share many principles, their differences highlight why businesses must tailor compliance to their jurisdiction. Staying ahead of these obligations is not just a legal necessity but a competitive advantage.

**Please note this article is for general informational purposes only and does not constitute legal advice.*