



Employee Data Privacy – United Arab Emirates

Data Privacy Laws and Regulations

What laws apply to the collection and use of individuals' personal information?

Data privacy laws have become more prominent in recent years. As the amount of personal information available online has grown substantially, there has been an enhanced focus on the processing of personal data, as well as the enforcement of such laws.

The United Arab Emirates (UAE) published the first comprehensive national data privacy law in the country, Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data (PDPL). This law went into effect in January 2022, and once the Executive Regulations are released, employers and other data controllers and processors are expected to comply within six months. The Executive Regulations were expected to be issued in March 2022, but as of August 2022, they have not yet been released.



Under the PDPL, processing personal data must be limited to the intended purpose, including

limiting the data being collected and setting retention periods. The PDPL applies to:

- processing the personal data of data subjects residing in the UAE or, who have a place of business in the UAE;
- data controllers (such as employers) or processors located in the UAE who process personal data (regardless of whether the data subjects are inside or outside the UAE); and
- data controllers or processors outside the UAE, who process personal data of data subjects residing within the UAE.

The PDPL does not apply to:

- personal health data regulated by the ICT Healthcare Law (Law No.2 of 2019);
- personal banking data subject to laws regulating the protection of such data;
- companies/establishments located in free zones in the UAE that have a specific legislation on data protection;
- government data and government entities that control or process personal data; and,
- personal data held by security and judicial authorities or any processing of personal data for personal purposes.

UKG HR COMPLIANCE ASSIST

The UAE's free trade zones (also called free zones), are business regions permitted to have their own set of laws, that apply within the zone. Areas outside the free zones (i.e. the majority of the country) are typically referred to as "mainland" or "onshore" for legal purposes. In the mainland, the UAE legislates at a federal government level and also at a local Emirate (e.g. Abu Dhabi, Dubai, etc.) level.



While each free zone may have their own regulations, the federal UAE laws will generally also apply, except when explicitly excluded under the law of the relevant free zone. The PDPL does not apply to businesses located in free zones that have

their own independent data protection laws. Note that general mainland criminal laws will usually apply in free zones.

Data protection related laws at the federal level include:

- **Federal Decree-Law No. 31 of 2021 On the Issuance of the Crimes and Penalties Law (Penal Code, Arts. 431 and 432** – Sets penalties for the violation of private or family life without consent, such as when an individual “lends his ears, records or transmits, through an apparatus of any kind, conversations that took place in a private place or through the telephone or any other apparatus” or, if someone “Captures or

transmits, through any kind of apparatus, the picture of a person in a private place.”

Penalties can also be imposed if an individual divulges a secret unlawfully for personal interests or for the interests of another person without authorization. This law is not typically used to prevent normal business activities, but when operating onshore it is prudent to obtain the consent of individuals when collecting or sharing their data in order to establish a legal basis.

- **Federal Law No. 2 of 2019 on the Use of Information and Communication Technology (ICT) in Health Fields (ICT Health Law)** – Ensures the safety and security of health data information that may be attributed to the health sector. This law places strict limits on the international transfer of health data protected under the ICT Health Law.
- **Federal Decree-Law No. 34 of 2021 Concerning the Fight Against Rumors and Cybercrime (Cybercrimes Law)** – Includes financial and detention penalties for the invasion of privacy, including transferring information, disclosing information and making copies without authorization or a lawful basis for doing so. There are also penalties for using electronic information systems and technology to amend or process a “record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy (Art. 44).”

Defamation can be a serious criminal offence in the UAE (not just under this law but also under other criminal codes and the Shariah concept of slander). Care should be taken to

UKG HR COMPLIANCE ASSIST

not use language which is offensive or highly negative in a subjective sense when discussing any individual. Reviews and appraisals should be treated as highly confidential and restricted to a need to know basis. Article 425 of the Penal Code creates a criminal offence of insulting a person or attributing to a person an incident that may make the person subject to punishment or contempt by using an information network or information technology tool. It is good practice to remind employees to exercise discretion when commenting publicly on people, companies or public bodies. Negative posts about a person on social media, such as Facebook, can lead to criminal proceedings and custodial sentences.

The Cybercrimes law (Article 44) creates an offence of (in summary) assaulting the privacy of a person by overhearing or intercepting communications, capturing or transferring pictures of a person or, publishing news or comments about a person via an electronic system or network without lawful permission. On the mainland, this means that it is important to obtain the consent of any individuals you are publicly commenting on or featuring in pictures. It is important for employees to also understand these risks.

In order to monitor staff communications, employers should have a process for obtaining consent from employees. There are no particular rules or requirements around the form or content of the consent.

- **Regulatory Framework for Stored Values and Electronic Payment Systems,**

published by the UAE Central Bank, 1/1/2017 – Gives the Central Bank the power to regulate digital payment mechanisms and infrastructures, including free trade zones (but excluding financial free zones). Under this regulation, licensed Payment Service Providers are responsible for maintaining the confidentiality of user identification and transaction records.

- **Regulatory Framework for Consumer Protection,** published by the UAE Central Bank in December 2020 along with accompanying standards in January 2021 – Introduces key data protection requirements for licensed financial institutions (LFIs) with the UAE Central Bank relating to protecting client's personal data. Under the Regulatory Framework, LFIs, amongst others, must establish a department to: oversee and manage the protection of consumer personal data; implement retention policies and appropriate security measures to prevent the misuse of consumer personal data; and, in the event of a data breach, notify the Central Bank and affected consumers.

Free Trade Zone Laws

While the UAE doesn't have an overarching data privacy law, some of the free zones do have their own data privacy laws which apply to employees who work within a particular free zone. Data protection laws in the free trade zones include:

UKG HR COMPLIANCE ASSIST

- **Abu Dhabi Global Market (ADGM)** – The Data Protection Regulations 2021, replaced the Data Protection Regulations 2015, and sets the core requirements for data controllers processing personal data in the ADGM. The Regulations, which are based on the European Union’s General Data Protection Regulation, applies to entities incorporated in the ADGM.
- **Dubai Healthcare City (DHCC)** – The Health Data Protection Regulation No. 7 of 2013 is designed to promote and protect patient health information in the DHCC.
- **Dubai International Financial Centre** – Data Protection Law, DIFC Law No. 5 of 2020 (effective July 1, 2020) replaces the DIFC’s original data protection law and applies to all

companies within the DIFC, as well as non-DIFC entities which data controllers and data processors who regularly process personal data in the DIFC under stable arrangements. The law is based substantially on the GDPR.



The UAE Data Office is the regulator for personal data privacy in the UAE (note the Data

Office is not active as of August 2022).

The free zones with data protection laws have their own regulator responsible for enforcing them.

Last updated September 2022.

DISCLAIMER: The information contained in this document is for general information purposes only and is not intended to be a source for legal, tax, or any other professional advice and should not be relied upon as such. This information is not intended to create, and the receipt of it by the reader does not constitute, an attorney-client relationship. All legal or tax questions or concerns should be directed to your legal counsel or tax consultant. Laws and regulations may change and UKG Inc. ("UKG") cannot guarantee that all the information in this document is accurate, current or complete. UKG MAKES NO REPRESENTATION OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE DOCUMENT OR THE INFORMATION OR CONTENT CONTAINED HEREIN AND SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES INCLUDING BUT NOT LIMITED TO ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY, OR COMPLETENESS OF THIS INFORMATION. TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, NEITHER UKG, NOR ITS AGENTS, OFFICERS, EMPLOYEES, SUBSIDIARIES, OR AFFILIATES, ARE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE OR PROFITS, OR BUSINESS INTERRUPTION), EVEN IF THE UKG HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT, ARISING IN ANY WAY OUT OF THE USE OF OR INABILITY TO USE THIS INFORMATION. This document and the content are proprietary and confidential information of UKG. No part of this document or its content may be reproduced in any form, or by any means, or distributed to any third party without the prior written consent of UKG © 2022 UKG Inc. All rights reserved.