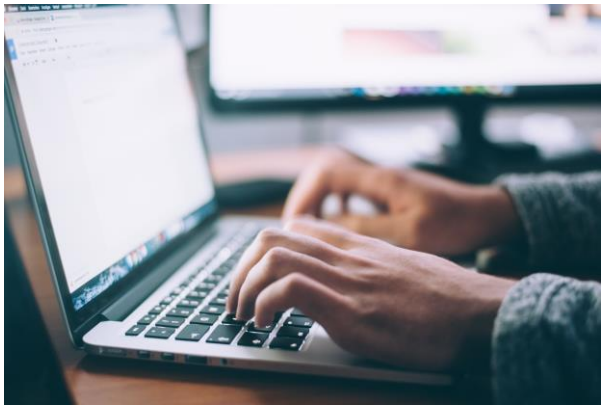
Employee Data Privacy – United Arab Emirates

Security Requirements

What security obligations are imposed on data controllers and data processors?

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and prevent alteration, corruption or access by unauthorized third parties. Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk.



Employers and other data controllers who process the personal data of UAE residents should take appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks associated with processing. Security measures should follow international standards and best practices, which may include (Federal Decree-Law No. 45 of 2021 , Art. 20):

- encryption and pseudonymization;
- processes and measures which ensure the confidentiality, safety, validity and flexibility of personal data processing systems and services;
- applying processes and measures that ensure timely retrieval and access in the event of any physical or technical failure; and,
- applying processes that ensure a smooth testing, evaluation and assessment of the effectiveness of technical and organizational measures to ensure the processing is secure.

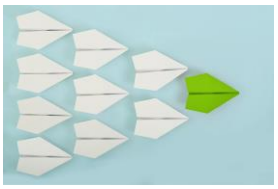
Employers should assess the nature, costs, scope and purposes of the personal data processing, and the potential risks associated with the processing when assessing security measures.

It is important to take practical steps to limit unauthorized disclosure of sensitive information to third parties. Disclosure of sensitive information without the consent of the concerned individual(s) could constitute an offence under the Penal Code (Art. 379).

Therefore, general best practice measures should be followed to protect both employee and job applicant data.

There are some sector-specific security requirements which may impact employee data processing. Federal Law No. 2 of 2019 on the Use of Information and Communication Technology (ICT) in Health Fields imposes security requirements on health-related data in the healthcare sector. For example, encryption is required for email and electronic communications containing patient information. It is currently unclear if this law will apply to all employee-related health data or just to health data held by healthcare companies, such as medical providers and insurers.

Some free trade zones in the UAE have specific security obligations relating to processing personal data. For example, the Dubai International Financial Center and the Abu Dhabi Global Market both require the implementation of technical and organizational measures to protect the processing of personal data. These laws do not mandate specific technical standards but require a risk-based approach appropriate to the processing activity and the risk of harm.



HR Best Practices:

Follow general best practices, such as ensuring contracts with service providers detail the security and confidentiality measures that will be implemented. Before implementing any security measures, assess the nature, potential expense, scope and purposes of the personal data processing as well as any risk associated with the personal data processing.

In the free trade zones, there may be more specific security requirements.

Last updated September 2022.