Employee Data Privacy – United Arab Emirates

Employee Consent

Do I have to obtain employees' consent in order to collect their personal data?

The processing of any personal data may impose obligations to the individuals the data is related to, the data subjects. Some jurisdictions only recognize processing personal data as lawful if the data subject has provided express consent. Other jurisdictions require a legal obligation to process the data and may not require consent. The processing of HR personal data has raised questions and court decisions in a few countries, and interpretations may vary based on data privacy and labor law requirements.

The UAE's Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data (PDPL) prohibits the processing of personal data with the consent of the data subject (Art. 4). There are a number of exceptions to obtaining consent. The exceptions most likely to impact employers include when data processing is:

- for personal data that has become available and known to the public by an act of the data subject;
- necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures;
- necessary for the assessment of the working capacity of an employee in accordance with legislation;
- necessary to protect public health, including the protection from communicable diseases and epidemics in accordance with legislation;
- necessary to protect the interests of the Data Subject;
- necessary for the Controller or Data Subject to fulfill his/her obligations and exercise his/her legally established rights in the field of employment, social security or laws on social protection, to the extent permitted by those laws; or, when
- necessary to perform a contract to which the data subject is a party or, to undertake procedures for concluding, amending or terminating a contract at the request of the data subject.

For consent to be valid (Art. 6): (i) the employer (or other data controller) must be able to prove the data subject consented to the processing; (ii) the consent request must be given in a clear,

simple, unambiguous and easily accessible manner, in written or electronic form; and, (iii) the consent request must indicate the right to withdraw consent, and the withdrawal process must be made easily.

The failure to obtain consent in certain circumstances could mean that there is no defense available if a complaint is made under other laws, such as the Penal Code (Arts. 431 and 432) or the law on Combatting Cybercrimes. Penalties for breaches of these laws can be severe and include prison sentences as well as fines.

Any transfer of personal data to a third party, publication of employee data (e.g. on a website or social media) or obtaining data through intrusive means such as photography, video recordings or online monitoring, risks violating other laws. It is therefore prudent to obtain consent before carrying out high-risk activities. On the mainland, these laws are enforced through local law enforcement (breach of privacy falls within the prohibitions in the Penal Code or the Cybercrimes Law). Any breach of the PDPL would be penalized by the UAE Data Office.

The processing of protected health data is separately regulated under the ICT Health Law (Federal Law No. 2 of 2019 on the Use of Information and Communication Technology (ICT) in Health Fields), which has additional restrictions relating to the collection, processing and transfer of health data. At this time, it's unclear whether health-related employment data would be subject to this requirement or whether the law will only apply to healthcare companies such as medical providers and insurers.

The PDPL requires a limited amount of information to be provided to data subjects before processing their personal data, compared to the more detailed privacy notice requirements under the EU's General Data Protection Regulation. Information is limited to (i) the purpose of processing; (ii) the recipients or categories of recipients with whom the personal data will be shared, both inside and outside the UAE; and, (iii) safeguards for cross-border personal data processing.

Free Trade Zones:

When free zones have a data protection law, the personal data should be processed and handled in accordance with that law. However, the federal UAE laws will generally also apply, except when they are explicitly excluded under the law of the relevant free zone (such as the PDPL for free zones with data protection laws in place).

General mainland criminal laws usually apply in free zones. Most of the relevant mainland criminal law provisions refer to the need for a "lawful permission" to undertake the activity in question. In the absence of a specific lawful permission, this is usually interpreted to mean that consent is required. Where free zones include laws that provide lawful permission, it will generally be sufficient to mitigate the risk under the mainland law.

However, the relevant mainland criminal laws are drafted more generally than data protection laws in many respects, so it is possible that a person employed in a free zone could make a complaint under a mainland law and that the police could decide to investigate and refer to the public prosecutor.

For example, if an employer chooses to publish information about an employee on social media, and the employee feels the information exposes them to ridicule, the employee can allege a breach of the Law Combatting Cybercrimes. Therefore, it is important for free-zone companies to carefully consider high-risk activities. If the activity is a discretionary one, it may be worth seeking the employee's consent to the specific activity, even if it is not required under the free zone law.

Some free trade zones in the UAE have specific requirements relating to the collection of personal data, including employee data. For example, the Dubai International Financial Center (DIFC) and the Abu Dhabi Global Market (ADGM) both have requirements similar to the European Union's General Data Protection Regulation, with consent being one of the lawful options to process personal information. However, these are jurisdictions based on the common law system and they will lean heavily on UK and European jurisprudence and guidance when interpreting their laws. Using consent in the employment context is often questionable under EU law, due to the unequal employee/employer relationship (i.e., the employee may not be able to give their free consent). Generally, the best basis for processing employee personal data under the ADGM and DIFC laws will usually be that:

- it is necessary to collect the personal data for the performance of the employment contract, and/or
- it is in the legitimate interests of the employer to do so (demonstration of the legitimate interest may require an impact assessment).

Note that 'legitimate interest' is not grounds for processing personal data under the PDPL.

In the DIFC and ADGM, the processing of special categories of personal data is permitted in the context of employment (i.e. For recruitment, visa or work permit processing, the performance of an employment contract, administration of pensions, etc.) (DIFC Law No. 5 of 2020, Art. 11b and ADGM Data Protection Regulations 2021, Section 7(2)(b)).

The DIFC and the ADGM both require providing the employee (or other data subject) with specific information about the employer (or other data controller) and the processing of personal information (DIFC Law No. 5 of 2020; ADGM Data Protection Regulations 2021). They also both have additional processing requirements when sensitive or special categories of personal data will be processed.

Last updated September 2022.