CPNI
Centre for the Protection of National Infrastructure

大成 DENTONS

UAE: Relevant legislation

As at March 2018, no privacy or data protection legislation was in place at a federal level in the UAE. However it is advisable and prudent that employers ensure that appropriate disclosure and consent mechanism are used at all times when collecting and processing data re employee monitoring. This can be achieved through consent and notices.

Constitution of the UAE

- Provides that 'freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with law'.

UAE Penal Code

- Prohibits the unauthorised use or disclosure of private information.
- Use of employee personal information should only occur with the employee's explicit consent to such use, and general principles of confidentiality should be applied.

UAE Cyber Crime Law

- Prohibits the unauthorised reception or interception of any communication through any computer network.
- Prohibits the invasion of privacy using information technology (other than in cases allowed by law), including (but not limited to):
  - '…interception, recording…or disclosure of conversations or communications, or audio…';
  - 'Photographing others or…copying or saving electronic photos';
  - 'Publishing…electronic photos…comments, statements or information even if true and correct';
  - 'Processing a record…for the purpose of…offending another person or for attacking or invading his privacy'.
- It is a crime to insult someone using information technology which leads them to being subject to punishment or to be held in contempt by others.

Principles deduced from case law

No case law on employee monitoring was found for this jurisdiction. Furthermore, as the UAE is a civil jurisdiction, there is no binding precedent system, so case law cannot be used as a reliable means of interpreting how such matters may be judged by a UAE Court in the future. However, the following general principles relating to data privacy and monitoring can be deduced from the legislation:

- The employee would need to prove the losses they have suffered as a direct result of the disclosure of their personal data before the civil courts if damages are to be awarded;
- Given sensitivities around what constitutes personal information, it is prudent that employers ensure appropriate disclosure and consent mechanisms are used at all times when collecting and processing data in relation to employee monitoring;
- Monitoring of IT systems by an employer may occur provided the employee has consented to such monitoring. This can be accomplished using consent and notice wording contained in the terms and conditions that either accompany or are included in the employer's HR policies and handbooks.

The future

GDPR: The UAE is not currently recognised as providing adequate protection of personal data as defined by GDPR. This means that additional safeguards may need to be in place in order for organisations to transmit personal data from UAE to the EU. UAE companies that collect personal data from EU citizens and companies with established operations in the EU should consider whether their operations fall within the scope of the GDPR and, if so, the steps that need to be taken to achieve compliance with its requirements.

Qatar has become the first Gulf Cooperation Council (GCC) country to have a national level comprehensive privacy law regime. There is often a GCC regional regulatory 'domino effect', so other countries are likely to follow suit.

It is anticipated that there will be imminent changes to the UAE privacy regime and, as such, legislative changes should be monitored closely moving forward.

CPNI
Centre for the Protection of National Infrastructure

大成 DENTONS

Organisations must be aware that legal considerations for employee monitoring will vary from organisation to organisation and specific issues will arise depending on the nature of the organisation undertaking monitoring and the risks it is trying to mitigate. Dentons UK and Middle East LLP (Dentons) prepared a report for CPNI on Employee IT Monitoring in March 2018 (the Report), to serve as a legal resource only, it is not a substitute for professional advice. This document provides a snapshot of some of the information contained in the Report and must not be read in isolation. Neither the Report nor this document are designed to provide legal or other advice and you should not take, or refrain from taking, action based on their content. The Report and this document are not a comprehensive report of all the information or materials that are relevant to this area of law, and do not address any particular concerns, interests, value drivers or specific issues you may have. This is a complex area of law that is changing rapidly. If you require assistance with a specific issue, you should seek legal advice from an appropriately qualified professional. Organisations planning to implement or review existing employee monitoring should seek their own professional advice. The Report (and therefore the information contained in this document) was current as of the date of the Report publication (being March 2018). Neither CPNI nor Dentons owe any duty to you to update the content of the Report or this document at any time for any reason. Please note the Report and this document do not represent the views of CPNI or Dentons. Neither CPNI nor Dentons UK and Middle East LLP accept any responsibility for any loss which may arise from reliance on the Report and/or this document.

© Crown copyright 2018