UAE Federal - Employee Monitoring

TABLE OF CONTENTS

• 1. GOVERNING TEXTS
• 2. TELEPHONE
• 3. CCTV
• 4. EMAIL
• 5. BIOMETRICS
• 6. DEVICE MONITORING
• 7. COVERT SURVEILLANCE
• 8. EMPLOYEES’ ACCESS RIGHTS
• 9. PENALTIES

January 2018

1. GOVERNING TEXTS

1.1. Legislation relevant to employee monitoring

The United Arab Emirates (‘the UAE’) is a federation of seven Emirates, and all Emirates are subject to a set of federal laws while retaining the right to administer their own internal affairs through a local legal infrastructure.

The UAE is also formed by a number of free-zones of which some enjoy a legal infrastructure of their own such as the Dubai International Financial Center (‘the DIFC’) and the Dubai Healthcare City (‘the DHCC’).
For the purpose of the present guidelines, we will, when and if relevant, refer to the laws applicable on a Federal level (‘the Federal Laws’), local level (‘the Local Laws’) and/or the laws enacted by certain free-zone authorities (‘the Free-Zone Laws’).

The UAE does not have any specific law addressing the right of the employer to monitor employees, though several pieces of legislation that apply to all individuals may have an impact on how employees can be supervised by their employer. These include:

**Federal Laws**

- The UAE Constitution of 1971 and its amendments which guarantees the right to privacy and secrecy of communications (‘the Constitution’);
- Federal Law No. 3 of 1987 which enumerates punishments for publication of private matters and/or the unauthorised disclosure of private information (‘the Penal Code’);
- Federal Decree by Law No. 5 of 2012 on combating cybercrimes (‘the Cybercrime Law’);
- Federal Law No. 8 of 1980 on maintaining employees’ information (‘the Labour Law’); and
- Federal Law by Decree No. 3 of 2003 regarding the organisation of telecommunications sector and its amendments (‘the Telecommunications Law’).

**Local Laws**

The Abu Dhabi Global Market (‘ADGM’) Employment Regulations 2015 (‘the ADGM Employment Regulations’) which applies to all organisations that are licensed by the ADGM and contains a section on the protection of personal data of individuals employed by companies within the ADGM.

We note that ‘personal data’ is defined in the regulation as any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity. The term ‘processing’, in relation to personal data means obtaining, recording or holding the personal data or carrying out any operation or set of operations on the personal data including

- organisation, adaptation or alteration of the personal data;
- retrieval, consultation or use of the personal data;
- disclosure of the personal data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the personal data.

**Free-Zone Laws**

Similarly, the DIFC Data Protection Law No. 1 of 2007 and its amendments (‘the DIFC Data Protection Law’) regulates and protects the activities related to personal data of individuals.
Under DIFC Data Protection Law, the term ‘data controller’ is defined as any person in DIFC who determines the purposes and means of the processing of personal data, and the term ‘data subject’ refers to the individual to whom personal data relates and the ‘Commissioner of Data Protection’ is the person appointed to administer the DIFC Data Protection Law. ‘Personal data’ is any information which:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment; or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system and the term ‘processing of personal data’ refers to any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

DHCC Regulation No. 7 of 2013 provides for a data protection system, more specifically regarding the transmission of confidential information, which is intended to control the way in which medical facilities manage and use confidential patient information.

1.2. Sector-specific legislation relevant to employee monitoring

There are currently no sector-specific legislations relevant to employee monitoring in the UAE but rather a combination of potentially applicable Federal, Local and Free-Zone Laws that may be applicable on employers and employees, as set out in Section 1.1 above.

1.3. Guidelines from supervisory authorities

The UAE Ministry of Human Resources & Emiratisation is considered the supervisory authority to administer and ensure compliance with the provisions of the Labour Law which regulate the relationship between employee/employer yet said ministry has not enacted any guidelines that specifically address how employees may be monitored by their employers.

As for the DIFC, we note that the DIFC Data Protection Law appoints the Commissioner of Data Protection as the supervisory authority to administer and ensure compliance with the DIFC Data Protection Law.

The ADGM, on the other hand has created the ADGM Registration Authority (‘the Registrar’) which is an independent body having the powers to administer Data Protection Regulations and enforce its provisions.
1.4. Notable decisions, i.e. case law or decisions from supervisory authorities

Not applicable.

2. TELEPHONE

2.1. What are the rules for recording telephone conversations?

The Federal Laws do not specifically provide rules for recording employees’ telephone conversations in the workplace yet other provisions of the Federal Laws, Local and Free-zones Laws guarantee the right to privacy and safeguard of personal data and may be potentially applicable on instances such as recording telephone conversations in the workplace. These are:

- Article 31 of the UAE Constitution which states an individual enjoys ‘freedom of communication by post, telegraph or other means of communications and the secrecy thereof shall be guaranteed in accordance with the law’;
- Article 15 of The Cybercrime Law which punishes the capture and interception of any communication intentionally and without permission through an information network;
- Article 72 of the Telecommunications Law penalises copying or disclosing the content of any sort of communication without the right to do so;
- Article 378 onwards of the Penal Code criminalises offences in relation to the interception or disclosure of correspondence or telephone conversations without previous consent;
- Part 2 of the DIFC Data Protection Law on general regulations on the processing of personal data; and
- Article 51 of the Employment Regulations enacted by the ADGM on processing personal data by the employer.

2.2. For which purposes may an employer carry out this type of monitoring?

Many businesses are required, by nature, to monitor telephone conversations as a way for managing risk such as banks, trading houses, insurance and brokerage companies.

Other companies that are not required by nature to monitor telephone conversations may decide to do so for training purposes and/or to ensure the quality of the services provided by its employees.

2.3. Is prior notification/approval with the data protection authority required?

For the time being, there is no data protection authority or similar governmental body established at a federal level in the UAE.
As for the DIFC, Article 19 (2) of the DIFC Data Protection Law stipulates that the data controller must notify the Commissioner of Data Protection of any data processing and when:

- sensitive personal data (defined as the personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal original, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life) is being processed; and
- personal data is being transferred outside of the DIFC.

2.4. Is prior notification/approval/consultation from works councils required?

There are no works' councils established in the UAE.

2.5. Is consent required from employee? If so, how should consent be sought?

According to the Federal Laws, specifically the Cybercrime Law, Telecommunications Law and the Penal Code, it is not permissible to record phone conversations unless the consent of the parties is obtained.

**DIFC Data Protection Law**

Articles 9 and 10 of the DIFC Data Protection Law states that personal data and sensitive personal data may only be processed if the written approval of the data subject is obtained. The DIFC Data Protection Law does not describe how the consent can be sought, rather only mentions that it is should be obtained in writing.

**ADGM Employment Regulation**

Article 51 (7) of the ADGM Employment Regulations stipulate that the written consent of the data subject is required for the processing of personal data outside of the ADGM. The same article further mentions that such consent may be obtained in a written contract of employment or other written contract between the employee and the employer.

2.6. Is consent required from other party to the call? Is so, how should consent be sought?

Although the Federal Laws do not explicitly mention whether the consent of the other party is required, we believe that the consent must also be obtained by all parties to the conversation as a precautionary measure for employers to avoid punishments stipulated under the applicable Federal Laws.
The common way used in order to obtain the consent of all the parties would be to inform them in advance that the call may be monitored.

2.7. Is there a legal requirement for employers to have a written policy in place governing telephone monitoring? If not, is there a recommendation to have one?

The potentially applicable UAE Laws do not require that employers have written policies in place governing telephone monitoring yet it is prudent and advisable that employers implement adequate and detailed policies that describe the purpose of monitoring and recording telephone conversations in the workplace.

2.8. Are there any exemptions to the legal requirements which govern this type of monitoring?

The Federal Laws do not foresee any exemptions to the legal requirement of consent given by the subject to be monitored.

2.9. What are the retention requirements applicable to data collected through telephone monitoring?

There are no retention requirements applicable to data collected through telephone according to UAE Laws.

**ADGM Employment Regulation**

Article 51 of the employment regulation mentions that personal data must not be kept 'for longer than is necessary' by the employer (having regard to the purpose or purposes for which they are processed).

3. CCTV

3.1. What are the rules for CCTV surveillance?

Under UAE Laws, the use of CCTV is still relatively unregulated yet a person's right to privacy must be considered when installing CCTVs. In fact, article 378 of the UAE Penal Code stipulates that a 'person shall be punished by detention and the fine if he prejudices the privacy of the individual or family life by committing any of the following acts other than in the events as permitted by law or without the consent of the victim: to eavesdrop, record or transmit by any device of any kind whatsoever conversations in a private place or by way of telephone or any other device, to take or transmit by any
device of any kind whatsoever a photo of a person in a private place [...]’ this means that signage should be displayed if CCTV is installed or that prior written consent be obtained from individuals who may be recorded by CCTV in a specific area, including the workplace.

Local Laws

Dubai Law No. 24 of 2008 and its amendments ‘regarding security service providers and users’ which enumerates in its Article 16 the business activities that must satisfy certain security specifications including employing CCTV. These include hotels and short-stay residences, financial and monetary institutions, manufacture and sale of precious metals and stones, shooting ranges, military and hunting equipment stores, shopping and leisure centres, precious materials storage facilities, hazardous materials storage facilities, precious commodities stores/outlets, large department stores, petrol stations, internet services, storage services, aircraft and balloon clubs.

3.2. For which purposes may an employer carry out this type of monitoring?

There are no specifications as to the purpose of carrying out monitoring through CCTV yet companies are usually equipped with these devices when such is necessary for the organization and maintenance of security, depending on the type of activity carried out by the company.

In the Emirate of Dubai, the Dubai Police imposes that companies carrying out certain business activities to install security equipment such as CCTV. Please refer to Section 3.1.

3.3. Is prior notification/approval with the data protection authority required?

Please refer to Section 2.3.

3.4. Is prior notification/approval/consultation from works councils required?

Please refer to Section 2.4.

3.5. Is consent required from employee? If so, how should consent be sought?

In instances where CCTV are installed in the workplace, relying on implied consent of the employees is not advisable and the prior written approval of the employee is recommended. This may be mentioned in the employment agreement and/or internal policies of the company.
3.6. Is there a legal requirement for employers to have a written policy in place governing CCTV surveillance? If not, is there a recommendation to have one?

There is no explicit legal requirement for employers to have a written policy under UAE Law yet it is highly advisable that employers put in place internal policies to inform employees of the CCTV in the work premises which explicitly describe the location and purpose of the CCTV.

3.7. Are there any exemptions?

Recorded footage should not be used abusively by the employer and the CCTV must not be placed in private areas such as the toilets, prayer rooms etc.

3.8. What are the retention requirements applicable to data collected through CCTV surveillance?

Under Federal Laws, there is no retention requirements applicable to data collected through CCTV surveillance.

4. EMAIL

4.1. What are the rules regarding monitoring of employees' emails?

As a general rule, employers have the right to monitor and access the company’s property which include email server, devices such as mobile, laptops, tablets provided that the (1) the employees are made aware of this right and that (2) the purpose of accessing and monitoring the emails (or other devices) is strictly related to work and not to private and family matters.

The potentially applicable legislations that regulate to which extent the employer may monitor and have access to an employee’s work email and other devices are as follows:

- Article 31 of the UAE Constitution which states an individual enjoys ‘freedom of communication by post, telegraph or other means of communications and the secrecy thereof shall be guaranteed in accordance with the law’;
- Article 15 of The Cybercrime Law which punishes the capture and interception of any communication intentionally and without permission through an information network;
- Article 72 of the Telecommunications Law penalises copying or disclosing the content of any sort of communication without the right to do so;
- Article 378 onwards of the Penal Code criminalises offences in relation to the interception or disclosure of correspondence or telephone conversations without previous consent.
- Part 2 of the DIFC Data Protection Law on general regulations on the processing of personal data; and
4.2. For which purposes may an employer carry out this type of monitoring?

Employers have the right to monitor company’s property for purposes related to work such as monitoring, training, ensuring quality services.

4.3. Is prior notification/approval with the data protection authority required?

Please refer to Section 2.3.

4.4. Is notification/approval/consultation with works council required?

There are no works' councils established in the UAE.

4.5. Is consent required from employee? If so, how should consent be sought?

The fact that the email server belongs to the company’s assets implies that the company will have full access to the server. Still it is advisable that the employers inform their employees of the company’s right to access and make use of the emails exchanged and contained in the work email. This approval is usually sought through either the internal policies of the company signed by the employees or in the form of a provision contained in the employment agreement.

4.6. Is there a legal requirement for employers to have a written policy in place governing email monitoring? If not, is there a recommendation to have one?

There is no legal requirement for employers to have a written policy in UAE laws, but the employers should have written policy to make them aware employees that they are being monitored such is usually described in the employment agreement (under clause 'company's property') and/or employees' handbook which is handed to employees usually upon them joining the company.

4.7. Are there any exemptions to the legal requirements which govern this type of monitoring?

Please refer to Section 2.8 above.
4.8. What are the retention requirements applicable to data collected through email monitoring?

Under UAE Federal Laws, there is no retention requirements applicable to data collected through email monitoring.

5. BIOMETRICS

5.1. What are the rules regarding biometric monitoring?

The Federal Laws do not regulate biometric monitoring.

5.2. For which purposes may an employer carry out this type of monitoring?

Federal Laws does not regulate biometric monitoring, therefore, does not provide rules regarding the purposes for the employer to carry out biometric monitoring.

5.3. Is prior notification/approval with the data protection authority required?

Please refer to Section 2.3.

5.4. Is notification/approval/consultation with works council required?

There are no works' councils established in the UAE.

5.5. Is consent required from the employee? If so, how should consent be sought?

There are currently no regulations governing employees' biometric data under Federal Laws.

5.6. Is there a legal requirement for employers to have a written policy in place governing biometric monitoring? If not, is there a recommendation to have one?

UAE Federal Laws does not stipulate about biometric monitoring, and there are no requirements of written policies regarding this type of monitoring yet it is recommended that the employees are aware of the collection of their personal data and the purposes of the biometric monitoring through the issuance of company internal policies.
5.7. Are there any exemptions to the legal requirements which govern this type of monitoring?

UAE Federal Laws do not contemplate biometric monitoring hence does not foresee any exemptions.

5.8. What are the retention requirements applicable to data collected for biometric monitoring?

There are no laws regarding employee data protection and biometric monitoring under UAE Federal Laws.

6. DEVICE MONITORING

6.1. What are the rules regarding company-owned device monitoring?

Please refer to Section 4.1.

6.2. For which purposes may an employer carry out this type of monitoring?

Please refer to Section 4.2.

6.3. Is prior notification/approval with the data protection authority required?

Please refer to Section 2.3.

6.4. Is notification/approval/consultation with works council required?

Please refer to Section 2.4.

6.5. Is consent required from the employee? If so, how should consent be sought?

Please refer to Section 4.5.
6.6. Is there a legal requirement for employers to have a written policy in place governing company-owned device monitoring? If not, is there a recommendation to have one?

Please refer to Section 4.6.

6.7. Are there any exemptions to the legal requirements which govern this type of monitoring?

Please refer to Section 4.7.

6.8. What are the retention requirements applicable to data collected from the company owned devices?

Please refer to Section 4.8.

7. COVERT SURVEILLANCE

There are no instances under UAE Federal Laws in which an employer may carry covert surveillance.

8. EMPLOYEES’ ACCESS RIGHTS

**Federal Laws**

Under the Labour Law, employers must keep certain record of each employee, containing personal information such as the name, address, phone number, salary, position yet the Labor Law is silent as to whether or not the employee has access to such records.

**DIFC Laws**

Article 17 of the DIFC Data Protection Law states that a data subject has the right to obtain from the data controller upon their request a confirmation in writing as to whether or not personal data relating to the employee is being processed and information at least as to the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data are disclosed.
ADGM Employment Regulations

Article 51 (8) of the ADGM Employment Regulations stipulate that a data subject is entitled to be provided with access to their employer’s records containing the personal data of the data subject provided that a minimum of 20 business days prior written notice is granted to the employer. The same article provides that the data subject may only use this access for the purpose of notifying the employer of any inaccuracy in the personal data.

9. PENALTIES

The penalties for non-compliance are as follows:

- Article 380 of the Penal Code states that whoever opens a letter or cable without consent of the person to whom it is sent or overhears a telephone call shall be punished by a fine not less than AED 3,000 (approx. €680). A culprit shall be punished by detention for a period of at least three months or by a fine of at least AED 5,000 (approx. €1,130), if he divulges the contents of said letter, cable or telephone call to a person other than that to whom it is addressed, and without his consent, where such an act causes damage to others.
- Article 15 of the UAE Cybercrimes Law states that any person who captures or intercepts any communication through any information network, intentionally and without permission, shall be punished by imprisonment and a fine not less than AED 150,000 (approx. €33,870) and not exceeding AED 500,000 (approx. €112,910) or by any of these punishments. Any person who disclosed the information obtained unlawfully by receiving or interception of communications shall be punished by imprisonment for a period not less than one year.
- Article 21 of the UAE Cybercrime Law stipulates that a person who used an information network, electronic information system or any of the information technology tools in assaulting the privacy of a person in cases other than those permitted in Law shall be punished by imprisonment for a period not less than six months and a fine not less than AED 150,000 (approx. €33,870) and not exceeding AED 500,000 (approx. €112,910) or by any of these punishments by any of the following methods:
  - overhearing, interception, recording, transferring, transmitting or disclosure of conversations, communications or audio or visual materials;
  - capturing pictures of third party or preparing electronic pictures or transferring, exposing, copying or keeping those pictures;
  - publishing electronic news or pictures or photographs, scenes, comments, statements or information even if they were correct and real.
- Article 22 of the UAE Cybercrime Law states that any person who used without permission any information network, electronic site or information technology tool to expose confidential information obtained by occasion or because of his work shall be punished by imprisonment for a period not less than six months and a fine not less than AED 500,000 (approx. €112,910) and not exceeding AED 1,000,000 (approx. €225,815) or by any of these punishments.
- Article 72 of the Telecommunications Law penalises with imprisonment of not more than one year and a fine of not less than AED 50,000 (approx. €11,290) and not more than AED 1,000,000 (approx. €225,815) or either of these penalties if that person:
  - uses Telecommunications Apparatus in an offensive or disruptive manner, or so as to be a nuisance towards others, or for any unlawful purpose;
copies or discloses, without a right to do so, the content of any communication, telephone
message or any of the telecommunications services whether or not working under any
licensee or related to a licensee by any relationship enabling that person to reveal the
contents of any communication or telephone message or any of the telecommunications
services.

- The DIFC Data Protection Law imposes pecuniary fines for general contraventions which is
  regulated in the Article No. 36 and the Schedule 2 provides for fines imposed on the misuse of
  personal information, specifically under the Schedule 2 which specifies fines, the main ones are of
  USD 10,000 for processing sensitive personal data without prior approval of the data subject.

ABOUT THE AUTHORS

Rania El Tawil

BSA Ahmad Bin Hezeem & Associates LLP

Rania El Tawil is an Associate with the Corporate and M&A practice, based in BSA Ahmad Bin Hezeem &
Associates’ DIFC office in Dubai. She specialises in corporate transactions, mergers & acquisitions and
company formations, as well as real estate and intellectual property issues, employment claims and
contract review.

Rania holds a Masters of Law in corporate, banking and finance law from Fordham Law School, New York.

rania.eltawil@bsabh.com