TABLE OF CONTENTS

+ 1. Governing Texts

1.1. Legislation relevant to employee monitoring

1.2. Sector-specific legislation relevant to employee monitoring

1.3. Guidelines from supervisory authorities

1.4. Notable decisions, i.e. case law or decisions from supervisory authorities

+ 2. Telephone

2.1. What are the rules for recording telephone conversations?

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

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

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

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

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

2.7. Is there a legal requirement for employers to have a written policy in place governing telephone monitoring?

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

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

+ 3. CCTV

3.1. What are the rules for CCTV surveillance?

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

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

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

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

3.6. Is there a legal requirement for employers to have a written policy in place governing CCTV surveillance?

3.7. Are there any exemptions?

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

+ 4. Email

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

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

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

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

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

4.6. Is there a legal requirement for employers to have a written policy in place governing email monitoring?

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

4.8. What are the retention requirements applicable to data collected through email monitoring?

+ 5. Biometrics

5.1. What are the rules regarding biometric monitoring?

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

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

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

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

5.6. Is there a legal requirement for employers to have a written policy in place governing biometric monitoring?

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

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

+ 6. Device Monitoring

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

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

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

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

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

6.6. Is there a legal requirement for employers to have a written policy in place governing company-owned device monitoring?

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

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

7. Covert Surveillance

8. Employees' Access Rights

9. Penalties

August 2023

1. Governing Texts

1.1. Legislation relevant to employee monitoring

- UAE Federal Constitution of 1971 (only available in Arabic here) ('the Constitution');
- Federal Decree-Law No. 31/2021 on the Issuance of the Crimes and Penalties Law (only available in Arabic here) ('the Penal Code');
- Federal Decree-Law No. 34/2021 (only available in Arabic here) ('the Cyber Crime Law') - Concerning the Fight Against Rumors and Cybercrime;
- Federal Decree-Law No. 3/2003 Regarding the Organization of the Telecommunications Sector ('Telecommunications Law');
- Federal Decree-Law No. 45/2021 On the Protection of Personal Data (only available in Arabic here) ('PDPL');
- Federal Decree-Law No. 44/2021 On the Establishment of the Emirates Data Office ('Data Office Law');
- Federal Decree-Law No. 33/2021 On Regulation of Labor Relations ('Labor Law')
- Abu Dhabi Regulation No. 5/2015 Implementing Abu Dhabi Law No 5/2011 on the Establishment of the Monitoring and Control Centre ('Abu Dhabi MCC Regulation');
- Dubai Law No. 24/2008 on Suppliers and Users of Security Services (only available in Arabic here) ('Dubai Security Services Law');
- DIFC Law No. 5 of 2020 ('DIFC Data Protection Law');
- DIFC Data Protection Regulations 2020 ('DIFC Data Protection Regulations');
- DFSA Conduct of Business Module (COB) [VER43/08-23] ('DFSA COB');
- ADGM Data Protection Regulations 2021 ('ADGM Data Protection Regulations'); and
- FSRA Conduct of Business Rulebook (COBS) (VER14.040723) ('FSRA COBS').

1.2. Sector-specific legislation relevant to employee monitoring

We note that currently, there is no sector-specific legislation on employee-monitoring. Thus, reference needs to be made to the federal legislation enlisted under the section on legislation relevant to employee monitoring above.

1.3. Guidelines from supervisory authorities

The main supervisory authority that deals with employee relations in mainland United Arab Emirates ('UAE') and regulates them in a few free zones is the Ministry of Human Resources and Emiratisation ('MOHRE'). However, currently, there are no guidelines that have been issued by the MOHRE with respect to employee monitoring. Further, Data Office Law stipulates setting up of a Data Office which would be responsible for inter alia preparing policies and legislations related to data protection, proposing, and approving the standards for monitoring the implementation of the PDPL, preparing systems for complaints and grievances related to data protection, issuing guidelines, and instructions for the implementation of the PDPL etc. However, we note that as of date, the UAE Data Office has not been set up yet.

In the Dubai International Financial Centre ('DIFC'), one of the major financial free zones in the UAE, the supervisory authority for data protection matters is the DIFC Commissioner of Data Protection ('DIFC Commissioner'). The DIFC Commissioner is empowered to inter alia audit controllers and processors, conduct investigations and inspections to ensure compliance with the DIFC Data Protection Law, issue findings, initiate proceedings for a contravention of the DIFC Data Protection Law, and impose fines for non-compliance, etc.

Another major financial free zone in the UAE is the Abu Dhabi Global Market ('ADGM'), wherein the Office for Data Protection is the supervisory authority for data protection matters within this jurisdiction, which is headed by the Commissioner of Data Protection ('ADGM Commissioner'). Further, the ADGM also has an Employment Affairs Office ('EAO') that oversees the operations of the ADGM employment laws with respect to providing guidance, stakeholder liaison, and ensuring best practices on employment matters. However, the EAO has not provided any guidance with respect to employee monitoring in the ADGM.

1.4. Notable decisions, i.e. case law or decisions from supervisory authorities

We note that there are no such cases presently in UAE mainland, DIFC, or ADGM that are specific to employee monitoring.

However, there is a prominent employee-related data protection case that was decided by the DIFC Courts which dealt with the handling of the personal data of a DIFC employee.

In the case of *The Dubai Financial Services Authority v. (1) The Commissioner Of Data Protection (2) Anna Waterhouse* (DIFC 051, 085/2018), Anna Waterhouse was employed as the Head of Legal Compliance at Deutsche Bank, a DFSA authorized firm, from 2007 to 2014. The Dubai Financial Services Authority ('DFSA') conducted investigations into Deutsche Bank's activities, including that of Waterhouse's, for potential breaches of DIFC Law No. 1 of 2007 ('DIFC Law of 2007'). The DFSA accused Waterhouse of intentional falsification of information, which she defended by claiming abuse of process. The Financial Markets Tribunal ('FMT') ruled against her defense, attributing the breaches to her recklessness.

In 2017, Waterhouse filed a Subject Access Request ('SARs') under DIFC Law No. 1 of 2007, seeking correspondence related to her from 2011. The DFSA declined to comply, citing Article 39(2) of the DIFC Law of 2007 and its potential interference with their investigative powers. Waterhouse complained to the DIFC Commissioner of Data Protection, asserting that DFSA had failed to prove substantial prejudice as required by Article 39(2) of the DIFC Law of 2007. She argued that the requested data could be redacted to maintain confidentiality. The DIFC Court sided with Waterhouse, stating that DFSA must prove exemption from compliance rather than relying on a blanket refusal based on potential prejudice to their power. The DIFC Court emphasized proportionality and stated that the DFSA should have systems in place to provide specific data, given the serious nature of allegations against Waterhouse.

The DFSA appealed, contending that complying with SARs from individuals under investigation could lead to more requests and hinder their investigative powers. They also claimed complying with Waterhouse's SARs would be costly and time-consuming. The DIFC Court rejected these arguments, suggesting the cost could have been managed within the DFSA budget or by requesting assistance from the UAE Government. The DIFC Court accepted DFSA's appeal on certain categories of information that could prejudice the investigation but upheld the DIFC Commissioner's decision that the DFSA had breached the law. The DIFC Court stressed that Waterhouse had a right to access her data and that the DFSA should have demonstrated the specific prejudice the SARs would cause to their investigative powers.

2. Telephone

2.1. What are the rules for recording telephone conversations?

This depends, on whether the device has been given by the employer for the purpose of employment and if that has been clearly defined in the employment document, strictly maintaining that the device should only be used for employment purposes and consent has been taken from the employ-

ee, then the employer has full rights to monitor/record telephone conversations.

UAE MAINLAND

Article 31 of the Constitution provides persons in the UAE, irrespective of their nationality, the freedom to correspond through post, telegraphy, or other means of communication, the secrecy of which is guaranteed by the Constitution.

In this regard, eavesdropping or recording, or transmitting, through a device of any type, conversations done privately or by phone or any other device, without the person's consent, is a punishable crime under Article 431 of the Penal Code, as it is considered as an interference with a person's constitutional right to privacy. Eavesdropping on phone calls without consent is also specifically punishable under Article 433 of the Penal Code. Moreover, an act of eavesdropping, interception, recording, communication, transmission or disclosure of conversations, communications, or audio or video materials is also considered a punishable offense under Article 44 of the Cyber Crime Law. Further, if a person eavesdrops on the content of phone conversation without prior permission from the judicial authorities or uses telecommunication services to harm, disturb, or hurt other person's feelings, or uses it for any other illegal purpose, they will be subject to punitive actions under Article 72 (bis 2) and Article 72 (bis 3) of the Telecommunications Law.

Given the above, Article 5(2) of the PDPL stipulates that 'Personal data must be collected for a specific and clear purpose and may not be processed at any subsequent time in a manner incompatible with that purpose. However, personal data may be processed if the purpose of processing is similar or close to the purpose for which such data is collected.' The PDPL defines 'personal data' as 'any data relating to an identified natural person, or on who can be identified directly or indirectly by way of linking data, using identifiers such as name, voice, picture, identification number, online identifier, geographic location, or one or more special features that express the physical, psychological, economic, cultural, or social identity of such person.'

Moreover, the PDPL requires the controller to obtain the consent of the data subject prior to processing their personal data. As per Article 6(1) of the PDPL, the following conditions must be met to obtain the consent of the data subject:

- the controller must be able to prove the consent of the data subject to process their personal data;
- the consent must be given in a clear, simple, unambiguous, and easily accessible manner, whether in writing or electronic form; and

- the consent must indicate the right of the data subject to withdraw it and that such withdrawal must be easily made.

Thus, while recording of telephonic conversation is considered as a breach of an individual's privacy and has criminal implications under various legislation, if a controller has a clear and specific purpose for collecting telephonic recordings, they can do so, provided that they take prior consent of the data subject before making such recordings. It is important to note that 'consent,' for the purpose of the PDPL, must be given by the data subject by 'a statement or by a clear affirmative action.'

There are however a few circumstances under which controllers may process personal data without the data subject's consent. Article 4 of the PDPL stipulates these circumstances, which are as follows:

- if the processing is necessary to protect the public interest;
- if the processing is for personal data that has become available and known to the public by an act of the data subject;
- if the processing is necessary to initiate or defend against any actions to claim rights or legal proceedings or related to judicial or security procedures;
- if the processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the UAE;
- if the processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs, and medical devices, in accordance with the legislation in force in the UAE;
- if the processing is necessary for archival purposes or for scientific, historical, and statistical studies, in accordance with the legislation in force in the State. If the processing is necessary to protect the interests of the data subject;
- if the processing is necessary for the controller or data subject to fulfill their obligations and exercise their legally established rights in the field of employment, social security, or laws on social protection, to the extent permitted by those laws;
- if the processing is necessary to perform a contract to which the data subject is a party or to take, at the request of the data subject, procedures for concluding, amending, or terminating a contract;
- if the processing is necessary to fulfill obligations imposed by other UAE laws on the controller; and
- any other cases set by the Executive Regulations of the PDPL.

Please note that the Executive Regulations of the PDPL have not yet been issued in the UAE.

While free zones in the UAE are exempt from certain federal laws and regulations, federal criminal law is still applicable to them. Thus, the aforementioned provisions of the Constitution, Penal Code, Cyber Crimes Law, and Telecommunications Law are applicable to the DIFC, ADGM, and other free zones.

DIFC

As per the DIFC Data Protection Law, 'Personal Data' is defined as 'any information referring to an identified or Identifiable Natural Person.' Further, an 'Identifiable Natural Person' means a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural, or social identity.'

The DIFC Data Protection Law stipulates that personal data shall be *inter alia*:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- processed for specified, explicit, and legitimate purposes determined at the time of collection of personal data; and
- processed in a way that is not incompatible with the purposes determined at the time of collection of personal data.

Further, the following are considered the lawful basis for processing personal data:

- the data subject has given free and unambiguous consent to the processing of that personal data for specific purposes;
- processing is necessary for the performance of a contract to which a data subject is a party, or in order to take steps at the request of a data subject prior to entering into such contract;
- processing is necessary for compliance with applicable law that a controller is subject to;
- processing is necessary in order to protect the vital interests of a data subject or of another natural person;
- processing is necessary for the performance of a task carried out by a DIFC Body in the interests of the DIFC, the exercise of a DIFC Body's powers and functions, or the exercise of powers or functions vested by a DIFC Body in a third party to whom personal data is disclosed by the DIFC Body; or

- processing is necessary for the purpose of legitimate interests pursued by a controller or a third party to whom the personal data has been made available, except where such interests are overridden by the interests or rights of a data subject.

Further, the DFSA COB which is issued by the DFSA, the financial services regulatory authority of the DIFC, mandates that a firm that is licensed by the DFSA, must take reasonable steps to ensure that it makes and retains recordings of its voice and electronic communications when such communications are with a client or with another person in relation to a transaction, including the receiving or passing of related instructions. This would include voice recordings of the employees with such clients or persons. However, this obligation is not applicable to such voice and electronic communications which are not intended to lead to the conclusion of a specific transaction and are general conversations or communications about market conditions.

ADGM

The ADGM Data Protection Regulations require that personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Further, the ADGM Data Protection Regulations stipulate that processing is lawful only in the following circumstances:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

- processing is necessary for compliance with a legal obligation to which the controller is subject under applicable law;
- processing is necessary to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out by a public authority in the interests of ADGM, or in the exercise of ADGM's, the Financial Services Regulatory Authority's ('FSRA'), the ADGM Court's, or the Registration Authority's functions or in the exercise of official authority vested in the Controller under applicable law; or
- processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or rights of the data subject which require protection of personal data.

Further, the FSRA COBS which is issued by FSRA, states that certain firms licensed by the FSRA must appoint an authorized person, who must make and retain recordings of voice and electronic communications that are:

- with a client or with another person in relation to a transaction, including communications relating to the receipt, execution, arrangement of execution of client orders and passing of related instructions; and
- made with, sent from, or received on equipment either provided by the licensed firms to an employee or contractor or use of which by an employee or contractor has been sanctioned or permitted by the licensed firms.

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

The purpose for monitoring telephonic calls would differ in each organization, largely depending upon the nature of their business activities. If the device is provided by the employer and as long as the purpose is well defined and the required prior consent is taken, employers may carry out this monitoring in line with the processing controls under the PDPL. In other words, if there is legal and/or authoritative ground and direction then monitoring can be valid.

As mentioned in the section on what are the rules for recording telephone conversations above, employers can carry out this monitoring without the consent of the employees under the circumstances stipulated in Article 4 of the PDPL.

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

UAE Mainland

Currently, there is no established Data Office in the UAE, and as such there is no requirement of obtaining any prior approval or giving prior notification to such a body in the UAE.

DIFC

As per the DIFC Data Protection Law, every controller or processor registered in the DIFC must register with the DIFC Commissioner by filing a notification of processing operations. Further, the controller must consult with the DIFC where a data protection impact assessment ('DPIA') indicates that, despite taking the applicable measures, the risks to the rights of data subjects remain particularly high and the controller has already carried out or wishes to commence or continue carrying out a processing activity.

Further, a controller is not prohibited from commencing the processing before or during a consultation period where there is insufficient time to complete such consultation in advance and there is a pressing business need to commence processing, provided it is not likely to override the vital interests of data subjects whose personal data is being processed. Such processing shall comply with the DIFC Data Protection Law and the controller shall remain liable for breaches under the DIFC Data Protection Law prior to or during the consultation period.

ADGM

There is no requirement for any prior approval to be obtained from the ADGM Commissioner. However, ADGM entities must notify to the ADGM Commissioner about the date from which they have started processing of personal data.

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

Please note that there are no works councils in the UAE, and thus no such prior notification, approval, or consultation is required.

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

UAE Mainland

As stated in the section on what are rules for recording telephone conversations above, Article 6(1) of the PDPL requires that the following conditions must be met to obtain the consent of the data subject:

- the controller must be able to prove the consent of the data subject to process their personal data;
- the consent must be given in a clear, simple, unambiguous, and easily accessible manner, whether in writing or electronic form; and
- the consent must indicate the right of the data subject to withdraw it and that such withdrawal must be easily made.

Thus, prior written consent must always be sought from the employee before processing any of their personal data. Usually, the consent is sought at the time of signing a written employment agreement. Consent clauses are either embedded within the employment contract or is sought separately. Such clauses must clearly state the personal data that the employer will process and the purpose of processing it.

DIFC

Before processing any personal data, employers in the DIFC must ensure that the employee has given free and unambiguous consent to the processing of that personal data for specific purposes.

ADGM

ADGM employers must ensure that consent is freely given, specific, and informed and is an unambiguous indication from the employees to have their personal data processed. Such indication can be given in writing, electronically, or orally, by a statement, or by a clear affirmative action.

Further, the ADGM Data Protection Regulations lay down the following controls with respect to obtaining consent:

- silence, pre-ticked boxes, or inactivity do not constitute consent;
- for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes for which it is intended the personal data will be processed;
- where processing is based on consent, the controller must be able to demonstrate that the data subject has consented to processing of their personal data;
- if the data subject's consent is given in the context of a written declaration that also concerns other matters, the request for consent must be presented in a manner which is clear-

ly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language; and

- when assessing if consent is freely given the assessor must take into account whether the data subject has a genuine or free choice or is unable to refuse or withdraw consent without detriment and the performance of a contract is conditional on consent to the processing of personal Data that is not necessary for the performance of that contract.

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

Wherever applicable, the provisions of the PDPL, the DIFC Data Protection Law, and the ADGM Data Protection Regulations will also apply to the other party to the call. Thus, their prior consent must also be sought before their calls are recorded. The consent must be sought under the same conditions as stipulated in the section on is consent required from employees and how it should be sought above. Further, before the call is recorded, it is common practice for either the employee or an interactive voice response to inform the other party that their call may be recorded. Since it is impractical to obtain written consent from the other party for a call recording, they may be either given an option to opt-in or opt-out of the call recording option. Thus, if they opt-in for the call recording, they would have expressly provided their consent to it.

2.7. Is there a legal requirement for employers to have a written policy in place governing telephone monitoring?

There is no legal requirement for employers to have a written policy that governs telephone monitoring. However, given that the PDPL places a certain heavy obligation on controllers and processors of personal data, it is advisable that employers have a proper written policy that outlines:

- the kind of personal data they are processing;
- the purpose of processing;
- how they obtain the prior consent of data subjects (in this case, the employees);
- DPIA policies;
- anonymization and pseudonymization measures;
- the rights of the employees *vis-a-vis* their personal data in accordance with the data protection laws;
- how the employees can express their grievance to the employer against any violation of their personal data rights;
- measures that the employer is taking to maintain the security of the personal data collected;

- the plan of action in case of any breach of the personal data; and
- personal data retention, correction, and erasure policies.

This is also applicable to employers in the DIFC and the ADGM.

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

UAE Mainland

As mentioned in the section on what are the rules for recording telephone conversations above, the PDPL stipulates the following circumstances under which controllers may process personal data without the data subject's consent:

- if the processing is necessary to protect the public interest;
- if the processing is for personal data that has become available and known to the public by an act of the data subject;
- if the processing is necessary to initiate or defend against any actions to claim rights or legal proceedings or related to judicial or security procedures;
- if the processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health, or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the UAE;
- if the processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs, and medical devices, in accordance with the legislation in force in the UAE;
- if the processing is necessary for archival purposes, or for scientific, historical, and statistical studies, in accordance with the legislation in force in UAE;
- if the processing is necessary to protect the interests of the data subject;
- if the processing is necessary for the controller or data subject to fulfill their obligations and exercise their legally established rights in the field of employment, social security, or laws on social protection, to the extent permitted by those laws;
- if the processing is necessary to perform a contract to which the data subject is a party or to take, at the request of the data subject, procedures for concluding, amending, or terminating a contract;
- if the processing is necessary to fulfill obligations imposed by other UAE laws on the controller; or

- any other cases set by the Executive Regulations of the Personal Data Protection Law.

Please note that the Executive Regulations of the Personal Data Protection Law have not yet been issued in the UAE.

DIFC

The provisions of the DIFC Data Protection Law would not be applicable to any operations performed on the personal data of a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose, or law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including safeguarding against and preventing threats to public security.

ADGM

The ADGM Data Protection Regulations do not apply to the processing of personal data: by a natural person for the purposes of purely personal or household activity, or by public authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security.

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

UAE Mainland

Article 5(7) of the PDPL states that 'personal data may not be kept after fulfilling the purpose of processing thereof.' Thus, while the PDPL does not specify any retention period for personal data, employers must note that personal data must not be kept after the purpose of processing it is fulfilled.

However, the Labor Law states that employers must retain a worker's records for up to two years after the termination of their services. Further, as per Article 5.1.1.13 and Article 6.1.6 of Central Bank's Consumer Protection Standards issued on December 31, 2020, companies can retain consumer data, including telephonic call recordings, for five years from the termination of the business relationship or the closing of a consumer's account with the licensed financial institution or upon completion of a casual transaction (in respect of a consumer with whom no business relationship is established), whichever is more recent. Since these telephonic recordings would also include the recordings of employees' voices, this would inadvertently also be applicable to the employees.

DIFC

Under the DIFC Data Protection Law, when the purpose of processing personal data ceases to exist or changes, then the controller and processor of data must securely and permanently delete, anonymize, pseudonymize, encrypt, or put beyond further use of the personal data. However, they are not required to do so where such personal data is:

- necessary for the establishment or defense of legal claims or must be retained for compliance with applicable law;
- being used in scientific research activity conducted in the public interest or in the interests of the DIFC in accordance with all applicable laws, in a manner that does not present risks to the rights of data subjects; or
- part of a dataset used to lawfully train or refine an artificial intelligence ('AI') system in a manner that does not present risks to a data subject's rights.

However, the DFSA COB mandates that the recording made as per the DFSA COB must be retained for a minimum of six months.

ADGM

The ADGM Data Protection Regulations do not set any minimum or maximum retention periods, however, where the basis for processing changes, ceases to exist, the controller must ensure that all personal data, including personal data held by processors, is securely and permanently deleted, anonymized so that the data is no longer personal data and no data subject can be identified from the data including where the data is lost, damaged or accidentally released, pseudonymized, securely encrypted or put beyond further use.

However, a controller or processor is not required to do any of the above, where such personal data is:

- necessary for the establishment or defense of legal claims or must be retained for compliance with applicable law;
- being used in scientific research activity conducted in the public interest or in the interests of the ADGM in accordance with all applicable laws, in a manner that does not present risks to the rights of data subjects; or
- part of a dataset used to lawfully train or refine an AI system.

However, the FSRA COBS mandates that the recordings made under the FSRA COBS must be retained for a minimum of two years.

3. CCTV

3.1. What are the rules for CCTV surveillance?

UAE Mainland

Generally, as mentioned in the section on what are the rules on recording telephone conversations above, Article 31 of the Constitution, Article 431 of the Penal Code, and Article 44 of the Cyber Crime Law would be able applicable to CCTV surveillance in the UAE, along with the provisions under the PDPL. Moreover, while there is no federal legislation governing CCTV surveillance, there are laws issued by different emirates within the UAE pertaining to this.

Abu Dhabi

Article 12 of the Abu Dhabi MCC Regulation requires that the following public and private establishments in Abu Dhabi must have monitoring and control systems, including a CCTV system:

- hotels, furnished apartments, and time-limited accommodation;
- banks, exchange offices, monetary, and financial institutions;
- shopping and entertainment centers and clubs;
- gas stations;
- gold and jewelry shops;
- warehouses and storehouses of valuable materials and dangerous substances;
- hospitals and health care centers;
- sport clubs;
- ports, airports, and land ports of entry;
- commercial buildings and workers' residential cities; and
- public and private schools, universities, and institutes.

Under the Abu Dhabi MCC Regulation, the Monitoring and Control Centre ('MCC') of Abu Dhabi is always vested with the powers to grant permits, no-object certificates, and approval certifications to public and private establishments to engage in monitoring activities.

Dubai

Article 3 of the Dubai Security Services Law requires security service providers, which include physical or legal persons providing security protection services, including but not limited to, selling, and installing any television cameras ('security systems'), that will be used for supervision, monitoring, recording or alarming, to obtain the prior consent of the Protection Systems Department in Dubai.

Further, this Dubai Law also stipulates that these security systems must be available in important commercial sectors in Dubai such as banks, exchange houses, gold and jewelry shops, hotels, shopping complexes, hospitals, etc.

Sharjah

As per a manual published by the Electronic Services and Communications Department of the Sharjah Police, any establishment that wants to install any security system, including CCTV, must obtain approval to do so from the Security Surveillance Systems Department of the Sharjah Police.

Recently the Governments of Sharjah and Ajman have issued decisions to bakeries and restaurants to install CCTV surveillance in their establishments.

Further, various manuals and guidelines have been issued by different security regulatory authorities in various emirates, which require that proper signage must be displayed in visible areas that inform that the particular area is under CCTV surveillance.

DIFC

Please refer to our response in the section on what are the rules on recording telephone conversations above.

ADGM

Please refer to our response in the section on what are the rules on recording telephone conversations above.

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

Please refer to our response to this in the section on telephone above. Additionally, if the employer's business activity falls under any of the important commercial sectors, they would by law, would have to carry out the necessary CCTV surveillance.

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

Please refer to our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

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

Please see our response to this in the section on telephone above.

Further, it is common practice to also install proper signage in visible sites in case any area is under CCTV surveillance.

3.6. Is there a legal requirement for employers to have a written policy in place governing CCTV surveillance?

Please refer to our response to this in the section on telephone above.

3.7. Are there any exemptions?

Please refer to our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

---

4. Email

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

UAE Mainland

The legislation and provisions enlisted in our response in the section on what are the rules for recording telephone conversations above would also be applicable to monitoring of employees' emails. In this regard, if the emails refer to employees' personal emails, then their monitoring would be in violation of the employees' right to privacy and the employer would have to face the necessary criminal penalties.

However, if the emails in question are the emails that are being communicated for the purpose of employment, such emails would be considered as the employer's property, and the employers would reserve the right to access and monitor any work property, such as emails, electronic devices, company vehicles, etc.

DIFC

Please refer to our response in the section on what are the rules for recording telephone conversations above.

ADGM

Please refer to our response in the section on what are the rules for recording telephone conversations above.

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

Please refer to our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

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

As stated in our response in the section on what are the rules regarding monitoring employees' emails above, there is no consent to be taken from the employees to monitor their work emails.

4.6. Is there a legal requirement for employers to have a written policy in place governing email monitoring?

We note that there is no legal obligation on the employer to have a written policy to monitor the work emails of the employees. As such there is no recommendation to include monitoring of work emails as part of the employer's written policy given that the work emails are the property of the employer.

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

Please see our response to this in the section on telephone above.

4.8. What are the retention requirements applicable to data collected through email monitoring?

Please refer to our response to this in the section on telephone above.

---

5. Biometrics

5.1. What are the rules regarding biometric monitoring?

UAE Mainland

The PDPL stipulates that personal data includes sensitive personal data and biometric data. Under the PDPL, 'biometric data' is defined as 'personal data resulting from processing, using a specific technique, relating to the physical, physiological, or behavioral characteristics of a data subject, which allows or confirms the unique identification of the data subject, such as facial images or dactyloscopy data.' Under the PDPL, biometric data is also classified to fall under sensitive personal data.

Thus, all the aforementioned controls, measures, and provisions under the PDPL, would be equally applicable to biometric data.

DIFC

We note that biometric data is classified under special category of personal data under the DIFC Data Protection Law. Under the DIFC Data Protection Law, special categories of personal data shall not be processed unless one or more of the following conditions apply:

- a data subject has given explicit consent to the processing for one or more specified purposes;
- processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of a controller or a data subject in the context of the data subject's employment, including but not limited to recruitment, visa, or work permit processing, the performance of an employment contract, termination of employment, the conduct of proceedings relating to employment and the administration of a pension, retirement, or employee money purchase benefit scheme;
- processing is necessary to protect the vital interests of a data subject or of another natural person, where the data subject is physically or legally incapable of giving consent; or

- processing is carried out by a foundation, association, or any other non-profit-seeking body in the course of its legitimate activities, subject to appropriate assurances and provided that the processing relates solely to the members or former members of such an entity, or to other persons who have regular contact with such a body in connection with its purpose.

ADGM

Just as in the DIFC Data Protection Law, the ADGM Data Protection Regulations also classify biometric data under the category of special categories of personal data and prohibit the processing of such data. However, biometrics may be processed in the following circumstances *inter alia*:

- the data subject has given explicit consent to its processing for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment law, provided that when the processing is carried out, the controller has an appropriate policy document in place; or
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

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

Please refer to our response to this in the section on telephone above.

Further, for entities registered in DIFC, please refer to our response in the section on what are the rules regarding biometric monitoring above.

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

Please refer to our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

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

Please see our response to this in the section on telephone above.

5.6. Is there a legal requirement for employers to have a written policy in place governing biometric monitoring?

Please refer to our response to this in the section on telephone above.

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

Please see our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

6. Device Monitoring

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

Please refer to our response in the section on what are the rules regarding monitoring employees' emails above.

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

Please refer to our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

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

Please see our response to this in the section on telephone above.

6.6. Is there a legal requirement for employers to have a written policy in place governing company-owned device monitoring?

Please refer to our response to this in the section on telephone above.

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

Please see our response to this in the section on telephone above.

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

Please refer to our response to this in the section on telephone above.

7. Covert Surveillance

Please refer to our response to this in the section on telephone above.

8. Employees' Access Rights

UAE Mainland

The PDPL does not provide any right to data subjects to access their data. However, Article 13 of the PDPL does give them the right, *inter alia,* to obtain information on the following, with respect to their personal data:

- the types of personal data that are processed;
- purposes of processing;
- decisions made based on automated processing, including profiling;
- targeted sectors or establishments with which their personal data is to be shared, whether inside or outside the UAE;
- controls and standards for the periods of storing and keeping their personal data;
- procedures for correcting, erasing, or limiting the processing and objection to their personal data;

- protection measures for cross-border processing;
- procedures to be taken in the event of a breach or infringement of their personal data, especially if the breach or infringement poses a direct and serious threat to the privacy and confidentiality of their personal data; and
- the process of filing complaints with the Data Office.

However, any of the above requests are subject to the controller's refusal in the following circumstances:

- the request is not related to any of the aforementioned, or is excessively repetitive;
- the request conflicts with the judicial procedures or investigations made by the competent authorities;
- the request may adversely affect the efforts of the controller to protect information security; or
- the request affects the privacy and confidentiality of the personal data of others.

As such there are no rights stipulated under the Labor Law that give employees the right to access their records and data with the employer. However, as data subjects, they would be able to exercise their rights under the PDPL.

DIFC

Upon request, an employee has the right to obtain from the employer, without charge and within one month of the request:

- confirmation in writing as to whether or not personal data relating to them 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; and
- a copy of the personal data undergoing processing, provided in an appropriate format, including but not limited to electronic form or hard copy format, and of any available information as to its source, including up-to-date information corresponding with the information requirements for when the personal data is obtained from the employee and when it is not obtained from the employee.

ADGM

An employee would have the right to obtain from the employer access to their personal data where it is confirmed that their personal data is being processed, amongst other rights under the ADGM Data Protection Regulations.

9. Penalties

The PDPL does not specify any administrative penalties that would be considered a violation under the legislation. The violations and penalties are expected to be specified in the awaited Executive Regulations of the PDPL.

Penal Code

Article 431 of the Penal Code punishes any person with imprisonment and a fine if they interfere with the right to privacy of any individual if they commit any of the following acts in violation of any law or without the consent of the victim:

- eavesdropping or recording, or transmitting, through a device of any type, conversations done privately or by phone or any other device; or
- taking or transmitting, through a device of any type, pictures of any person in private.

If any public official commits any of the above acts, they shall be liable to imprisonment of up to seven years and a fine.

Article 434 punishes a person with a fine of no less than AED 3,000 (approx. $817) if they eavesdrop on a phone call.

Cyber Crimes Law

Article 13 of the Cyber Crimes Law punishes a person with detention and/or a fine of at least AED 50,000 (approx. $13,615) and not more than AED 500,000 (approx. $136,147) if they use information technology ('IT') to collect, keep, or process personal data of any national or resident in the UAE in violation of any law that is in force.

Article 44 of the Cyber Crimes Law punishes a person with detention for a period of not less than six months and/or a fine of not less than AED 150,000 (approx. $40,844) and not more than AED 500,000 (approx. 136,147) who uses IT to breach the privacy of a person or their private or family life without their consent by:

- eavesdropping, interception, recording, communication, transmission, or disclosure of conversations, communications, or audio or video materials;
- taking photographs of others at any public or private place or preparing, communicating, exposing, copying, or keeping electronic images thereof;
- spreading news, electronic images, photographs, footage, comments, data, or information, even if true and correct, to harm such person;
- taking, communication, or publication of photographs of the casualties, dead persons, or victims of accidents or disasters without permission or consent of the concerned persons; or
- tracking, detecting, disclosing, exposing, copying, or keeping data of geographical sites of third parties.

Telecommunications Law

Article 72 (2) of the Telecommunications Law stipulates that eavesdropping on the content of phone conversations without prior permit from pertinent judicial authorities will be punishable with imprisonment and/or a fine.

Article 72 (3) of the Telecommunications Law punishes a person with imprisonment for a period not exceeding one year, and/or a fine not exceeding AED 50,000 (approx. $13,615), for exploiting or using telecommunication services, or harming, disturbing, or hurting other person feelings or for any other illegal purpose.

Labor Law

Article 63 of the Labor Law stipulates a fine of AED 5,000 (approx. $1,362) to AED 1,000,000 (approx. $272,294) for failing to comply with the obligations under the Labor Law.

DIFC Data Protection Law

The DIFC Data Protection Law stipulates various penalties ranging from $10,000 to $100,000 for any violations or contraventions.

ADGM Data Protection Regulations

Under the ADGM Data Protection Regulations, depending on the nature, gravity, and duration of the contravention, the ADGM Commissioner may impose a fine of up to $28,000,000.