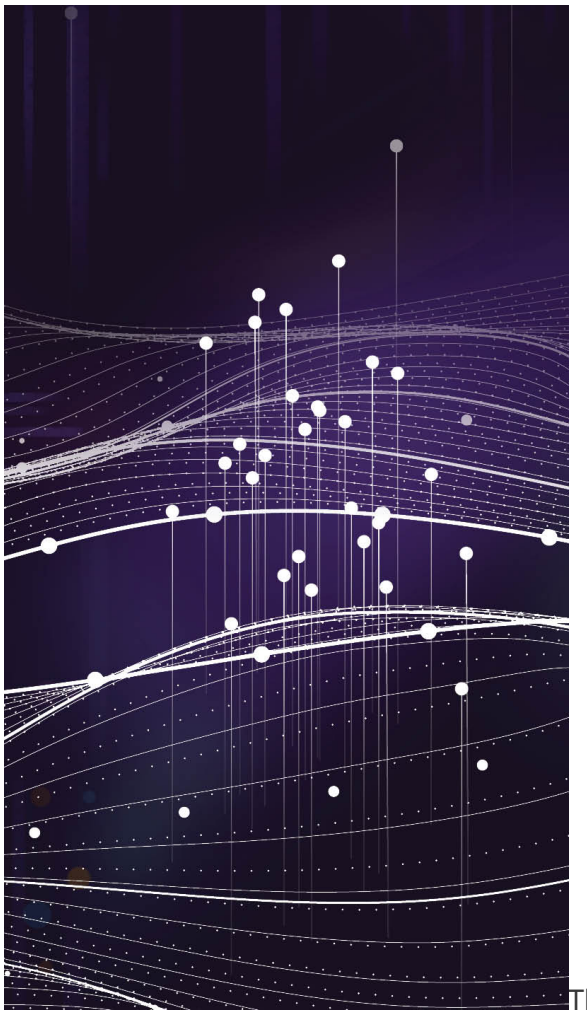
Getting personal: the new DIFC data protection law and what it means for you

Krishna Jhala - Senior Counsel - Digital & Data
k.jhala@tamimi.com - Abu Dhabi

Zil Ur Rehman - Senior Associate - Digital & Data
- Riyadh



The Dubai International Financial Centre ("DIFC') enacted a new data protection law which will more closely align the jurisdiction with the approach to personal data protection presently taken in Europe.

What is personal data protection?

In essence, personal data is any information relating to an individual which allows for direct or indirect identification of such individual. For example, an individual's name, phone number, address, citizenship, IP address is personal information. Protection of personal data is recognised as an extension of the fundamental right to privacy.

Historically, the focus on data protection emerged primarily due to the rise in trans-border commerce and trade that led to a surge in information sharing, and the increased use of computers to process information about individuals. Such advances led to greater concern over the privacy of individuals and their ability to

exercise control over their personal information. The1995 European Union Directive (Directive 95/46/EC) on protection of individuals with regard to the processing of personal data and on the free movement of such data was replaced by the General Data Protection Regulation ('GDPR'), in May 2018. The GDPR was a generational update of personal data protection law that better reflects today's digital age. The new DIFC Data Protection Law (Law No. 5 of 2020) ('New Law') is closely aligned with the approach taken by the GDPR.

DIFC data protection law

DIFC enacted its New Law which came into force on 1 July, 2020 but will be applicable to businesses with effect from 1 October, 2020.The New Law repeals DIFC Data Protection Law (Law No. 1 of 2007 (as amended) 'Old Law')). In essence, the New Law provides a three-month transition period to businesses to offer compliance. Any rights accrued, liability incurred and/or investigations or administrative proceedings commenced under the Old Law will not be affected until 1 October 2020. DIFC has also published its supporting Data Protection Regulations under the New Law ('Regulations') which came into force alongside the New Law on 1 July, 2020. Separately, non-binding guidance on the New Law ('Guide') has also been released in an attempt to facilitate compliance amongst stakeholders.

Applicability and Scope

The scope of the DIFC's data protection regime has expanded under the New Law. The Old Law was applicable to Controllers registered within the jurisdiction of the DIFC. In contrast, the New Law methodically sets its scope out as not only applying to Controllers incorporated within the jurisdiction of DIFC (whether or not processing takes place in DIFC) but also as applying to Controllers and Processors (regardless of their place of incorporation, whether elsewhere in the UAE or abroad) that process personal data in the DIFC as a part of stable arrangements other than on an occasional basis. The Guide explains that stable arrangements include legally binding or recognised agreements or relationships of an existing, valid type may be enough to require that the principles and objectives of the New Law are demonstrated in such arrangements.

The question then arises as to whether the New Law and the Regulations are applicable to remote processing service providers. In this respect, the Guide elaborates that while non-DIFC entities may be subject to the New Law and the Regulations either directly or indirectly, they are not necessarily required to register with or notify operations to the Commissioner other than by way of the relationship with the DIFC-based relevant entity, nor are they required to complete other administrative tasks. However, they may be subject to fines, warnings or public reprimand by way of such relationships or arrangements, either directly or indirectly. According to the New Law, Processing "in the DIFC" occurs when the means or personnel used to conduct the processing activity are physically located in the DIFC.

Basics and processing of consent

The New Law expands the scope of Processing activities in comparison to the Old Law and generally incorporates the principles for Processing of Personal Data as set out in the GDPR i.e. lawfulness, fairness and transparency, adequacy/minimisation, accuracy, storage limitation and integrity/security. The conditions for lawful basis for Processing Personal Data as stipulated in the New Law are also largely based on the GDPR and include necessary processing for protection of the vital interests of the Data Subject or of another natural person; a condition which was not covered by the Old Law.

In comparison to the Old Law, there is greater emphasis on the conditions of a Data Subject's consent

which, when needed, must be freely given by a clear affirmative action which shows an unambiguous indication of consent. Where Processing is based on consent, a Controller must be able to demonstrate that consent has been freely given and the Controller should implement appropriate and proportionate measures to assess the ongoing validity of the consent. In the context of an employee –employer relationship, it may be hard for the employer to establish that consent was freely given. In the Commissioner's opinion, consent is therefore unlikely to be a good basis for employers to rely on and may be subject to challenge. Employers should consider other lawful bases for processing employee Personal Data.

This position is more in line with the GDPR, although, the New Law does not address certain additional aspects covered in the GDPR such as the conditions applicable to processing of children's data. (i.e minors who cannot legally consent.)

Special Categories of Personal Data

Special Categories of Personal Data (previously referred to in the Old Law as Sensitive Personal Data) includes "*Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person*." Such data must not be processed unless one of the conditions set out in the New Law exists (in addition to the general requirements for Processing and lawfulness).

In this respect, most notably (and in comparison to the Old Law), the New Law grants specific rights to the Controller to process Special Categories of Personal Data for Data Subjects' employment purposes including recruitment, visa or work permit processing, the performance of an employment contract and termination of employment. Such processing rights are also available to Controllers in a healthcare context.

Legitimate interests

In comparison to the Old Law, the New Law provides clarity on what constitutes "legitimate interests" for purposes of Processing (i.e. restricting the use of the legitimate interests' right to process) as follows:

- prohibition on public authorities from relying on legitimate interests as the lawful basis for Processing Personal Data;
- transfer of Personal Data by Controllers within their organisational group, for internal administrative purposes is considered a legitimate interest; and
- a Controller has a legitimate interest in Processing Personal Data if it is necessary and proportionate to prevent fraud or ensure network and information security.

Data Controllers and Processors

The New Law places compliance obligations directly on the Processors as well as the Controllers. In addition to such obligations, Controllers and Processors must enter into a legally binding written agreement governing any processing activities.

Where there are two or more Controllers jointly determining the purposes and means of processing such Controllers will be referred to as Joint Controllers and should also enter into a legally binding agreement

clearly defining each of their responsibilities regarding compliance with obligations under the New Law.

The New Law casts an obligation upon the Processors to notify the Controller in cases where its processing activity infringes the New Law. Failure to do makes the Processors liable to penalty under the New Law.

Data Controllers and Processors are required to maintain a written electronic record of their processing activities. The New Law makes it mandatory to include certain information in such records. The types of information required is largely mirrored in the records' requirements contained in the GDPR and include the name and contact details of the Controller or Processor, the Joint Controller and any Data Protection Officer ('DPO'), if appointed; purposes of processing, descriptions of data, data subjects and recipient categories. The aforementioned list is not exhaustive and is only for illustrative purposes.

Data Protection Officers

Another key new feature of the New Law which previously remained unaddressed is the introduction of the GDPR concepts of DPO and Data Protection Impact Assessments ('DPIA'). As per the New Law, it is mandatory for official DIFC bodies (except for courts acting in judicial capacity) and Controllers and Processors systematically or regularly engaged in High Risk Processing Activities to appoint a DPO. Definition of High Risk Processing Activities include:

- processing that includes the adoption of new or different technologies or methods (e.g. AI or Blockchain) with materially increased risk to the security or rights of a Data Subject or rendering it more difficult for a Data Subject to exercise their rights;
- processing of a considerable amount of Personal Data (including staff and contractor Personal Data) and where such processing is likely to result in a high risk to the Data Subject, including due to sensitivity of the Personal Data or risks relating to the security, integrity or privacy of the Personal Data;
- the processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling (the automated processing of Personal Data to evaluate the personal aspects relating to a natural person primarily to analyse or predict aspects concerning the person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements), and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or
- a material amount of Special Categories of Personal Data is to be processed.

The Guidance issued by the Commissioner provides useful insights on the parameters of High Risk Processing Activities. Most notably, where processing involves a considerable amount of Personal Data and the risk to Data Subjects is high. the Commissioner refrains from setting any specific quantitative thresholds in respect of what constitutes a "considerable amount" of Personal Data but gives specific instances of that may qualify as processing a considerable amount of Personal Data. Such entities include a:

- Controller with several hundred staff;
- Controller with several thousand customer records;
- business which collects, stores or analyses Personal Data on behalf of its customers;
- Processor which provides outsourced business services involving Personal Data, such as HR or payroll systems or IT support services; and
- provider of hosted subscription services or self-service online services.

Another interesting feature of the New Law is that where a DPO is appointed the DPO must reside in the United Arab Emirates unless he or she is an individual employed within an organisation's group and performs a similar function for the entire group on an international basis. The DPO is required to act independently and report directly to senior management..

Data Subjects' rights

The New Law appears to have greatly expanded the scope of Data Subjects' rights in order to achieve greater consistency with the GDPR. Accordingly, the New Law grants Data Subjects a full set of rights in respect of consent withdrawal; access/rectification and erasure of data; objection to and restriction of processing; data portability; not being subject of automated individual decision making; and anti-discrimination. The anti- discrimination right is an additional right from the California Consumer Privacy Act, which states that the Controller may not discriminate against a Data Subject who exercises any rights under the New Law including: (i) deny any goods or services; (ii) charge different prices or rates, including through the use of discounts or other benefits or imposing penalties; (iii) providing a less favourable level or quality of goods or services; or (iv) suggesting either of the above to the data subject. Similar to the GDPR, the New Law is data-subject-centric.

Transferring data outside the DIFC

The requirements, in respect of transferring Personal Data outside of the DIFC to jurisdictions where adequate levels of protection are implemented, are generally based on data export requirements contained in the GDPR. The Commissioner is empowered to determine which jurisdictions implement adequate levels of protection based on certain factors which include, amongst others: considering the recipient's jurisdictional rule of law; access to Personal Data by authorities; and the existence of effective data protection regulations. A list of adequate jurisdictions has been published in Appendix 3 of the Regulations.

Similar to the GDPR, where personal data is being transferred to jurisdictions which do not provide adequate levels of protection one of the following conditions must be met:

- the Controller or Processor ensures appropriate safeguards are in place such as: binding corporate rules or the adoption of standard data protection clauses as issued by the Commissioner (this list is non-exhaustive); and data subjects have enforceable rights and remedies available to them; or
- one of the derogations listed in the New Law (which includes the explicit consent of the Data Subject, necessity for performance of contract and reasons of public interest) applies; or
- one of the limited circumstances listed in the New Law (which includes non-repetitive transfers, limited number of Data Subjects and compelling legitimate interests of the Controller) applies.

The Regulations mention that the Commissioner has approved and published standard contractual clauses that may be used for transfers to non-adequate jurisdictions outside the DIFC.

Further, a key new feature of the transfer regime under the New Law is the introduction of "binding corporate rules" to facilitate the transfer of Personal Data between members of a corporate group. A Controller or Processor can only rely upon such rules if the Commissioner has approved them and if they are only used for transfers inside the Controller or Processor's corporate group. A new list of jurisdictions meeting the adequacy criteria, as found under the Old Law, is provided in the Regulations.

Breach notifications

The impact of breach notifications are also largely based on those contained in the GDPR. Controllers are required to report Personal Data Breaches which compromise the security to the Commissioner as well as those that breach confidentiality or privacy of a Data Subject. Such notification must be made to the Commissioner as soon as practicable in the circumstances. Processors should notify the relevant Controller

without undue delay after becoming aware of Personal Data breach. In certain circumstances, notification must also be provided to the affected Data Subjects.

Fines and disputes

In terms of enforcement, failure to comply with a direction by the Commissioner or a violation of the New Law may result in the imposition of fines ranging from US$10,000 to US$100,000 (depending on the nature of the contravention). The heaviest administrative fines relate to contraventions in respect of the rights of Data Subjects. The Commissioner may also issue a general fine for a violation of the New Law by an appropriate and proportionate amount, taking into account the seriousness of the contravention and the risk of actual harm to any relevant Data Subjects. Data Subjects are entitled to compensation for any damages suffered arising out of a violation of the New Law by an obligated party. The New Law also grants Controllers and Processors the right to appeal any decision or direction of the Commissioner with the DIFC courts.

Conclusion

The New Law also contains certain other provisions such as data sharing with authorities, codes of conduct, cessation of processing and certification schemes.

- **Data sharing**: Subject to the requirements of the New Law, a Controller or Processor must consider certain factors when responding to a request from any requesting authority (i.e. a public authority over the person or any part of its group of companies) for the disclosure and transfer of any Personal Data. Such factors include, most notably, where reasonably practicable, obtaining appropriate binding written assurances from the requesting authority.
- **Cessation of processing**: where the basis of processing ceases to exist the Controller is required to cease the processing due to exercise of Data Subject's rights. The Controller shall ensure that all Personal Data, including that held with the Processor, is permanently deleted or anonymised, pseudonymised, permanently encrypted or archived in a manner where it is "put beyond further use".
- **Codes of conduct and certification schemes**: The New Law further provides for a mechanism whereby a Controller or Processor (or any other organisation including academic organisations) may develop a code of conduct containing guidance on compliance with the requirements of the New Law and submit a draft of the same to the Commissioner for approval. The New Law additionally provides for the establishment of certification schemes for the purposes of enabling a Controller or Processor to demonstrate compliance with the New Law. Such certification can only be implemented by an organisation approved by the Commissioner.

In order to ensure compliance by 1 October 2020, Controllers and Processors should start reviewing their processing activities including, in particular, transfer mechanisms to jurisdictions outside the DIFC, considering whether or not a DPO is required to be appointed as per the New Law, ensuring compliance with requirements for High Risk Processing Activities, and ensuring their privacy notices provide complete list of Data Subject rights and fulfil the consent and other requirements set out under the New Law.

For further information please contact Krishna Jhala (K.Jhala@tamimi.com).