New DIFC Data Protection Law: Act now to ensure compliance

What does the new law require and what do you need to do?

On 21 May 2020 His Highness Sheikh Mohammed bin Rashid Al Maktoum enacted the Dubai International Finance Centre ("**DIFC**") Data Protection Law No.5/2020 (the "**New DP Law**"). The New DP Law comes into effect on **1 July 2020** and will replace and significantly expand the existing Data Protection Law No.1 of 2007 ("**Current Law**").

The New DP Law will align the DIFC legislative regime with international data privacy standards – including the European General Data Protection Regulation ("**GDPR**") – and heralds a step change in data protection ("**DP**") law in the DIFC.

The Board of Directors of the DIFC Authority has also issued new Data Protection Regulations ("**Regulations**") that set out the procedures for notifications to the Commissioner of Data Protection ("**Commissioner**"), accountability, record keeping, fines and adequate jurisdictions for cross-border transfers of personal data.

The New DP Law applies to businesses operating, conducting, or attempting to conduct, business in or from the DIFC, whether or not processing takes place in the DIFC.

So what does the New DP Law mean for your business?

The purpose of the New DP Law is to provide standards and controls for the processing and free movement of personal data, and to protect the fundamental rights of data subjects, including how such rights apply to the protection of personal data in emerging technologies. Individuals' rights over their data have been enhanced and clarified and there is more detail on certain legal bases for processing, such as legitimate interests and consent.

The New DP Law focuses in particular on the enhanced accountability of **controllers and processors**, with the introduction of requirements for compliance programmes, appointing data protection officers where necessary, conducting data protection impact assessments and imposing contractual obligations that protect individuals and their personal data.

There is no longer a permit process for cross-border data transfers or processing of special categories of personal data, and the New DP Law and Regulations also provide for appropriate data sharing structures between government authorities, signifying a key

step forward in data sharing standards within the UAE and the region. General fines for serious breaches of the New DP Law, in addition to or instead of administrative fines, as well as increased maximum fine limits, have been introduced.

Controllers wishing to use new technologies like Artificial Intelligence (AI) and Blockchain are permitted to manage potential conflicts with data subjects' rights, such as the right to erasure, through the use of safeguards, for example, providing enhanced information at the outset.

In light of the Covid-19 pandemic, businesses subject to the New DP Law are being given a **grace period** of three (3) months – **to 1 October 2020** – to take the necessary steps to ensure compliance.

Although October is a few months away, most businesses will have a lot of work to do in order to prepare for compliance with the New DP Law. To ensure compliance with the New DP Law by October, it is vital that organisations take the following steps now:

- **take stock of their current DP practices**
- **understand the impact of the changes to DP law for them and on their business**
- **take any necessary action.**

Where to start?

Right here! This document sets out an essential ten point DP checklist. The starting point for organisations that handle personal data should be a **data audit**, as this will go some way towards satisfying the new accountability requirements and help identify what other steps they need to take. This should be undertaken as soon as possible to ensure full compliance by the time the New DP Law is implemented.

Key points for organisations to address in preparing for implementation of the New DP Law are:

- Privacy notices (more information must be added, to ensure they meet the new requirements).
- A review of policies and procedures in light of the heavier penalties that may apply for non-compliance with DP legal requirements.
- A review of the legal bases currently adopted for processing personal data, including special categories of personal data.
- Making sure current processes for complying with data subject access can cope with the new shorter timeframes for responding to requests and reporting any data breaches to the Commissioner.
- New and enhanced data subject rights in relation to personal data.
- Reviewing third party service provider agreements to ensure compliance with the new DP requirements.
- Negotiations with service providers over the extent of their liability for DP law breaches and any indemnities required.

Stephenson Harwood can help companies navigate their initial data audit and address the above points. Full contact details of our team of experts are on the last page of this document should you wish to find out more about our range of experience providing DP advice or should you have any general DP queries arising from this document.

Checklist for New DP Law Compliance

1 Information held by organisations

Under the Current Law, there is an implicit requirement that controllers know what data they hold and how that data is held. The New DP Law makes this explicit, requiring **controllers** to record and document details including the data they hold, the purposes for processing that data and who the data is shared with. **Processors** must also document their processing activities, in line with the requirement to demonstrate compliance.

By doing this, organisations may discover certain DP issues that need to be addressed. For example, controllers may identify certain data that is not necessary and make arrangements for its deletion.

To comply with this new requirement, organisations should consider carrying out a data audit covering:

- ✓ **the personal data held and source of that data**
- ✓ **how the data is stored, where it is stored and how long for**
- ✓ **the reason(s) it is necessary to process that data whether it is lawful to process that data**
- ✓ **who else has access to the data.**

2 Communicating privacy information

Controllers should already use privacy notices that provide fair processing information to data subjects such as employees and customers and that might also seek express consent to the processing of personal and special categories of personal data.

The New DP Law enhances the existing requirements so that it will be necessary for controllers to communicate additional information to data subjects, including:

- The reason(s) and the legal basis which they are relying on to process personal data.
- Data retention periods or criteria for how long data will be held.

- Information about data subjects' rights including the right to complain to the Commissioner where individuals think there is a problem with the way their data is being handled.

All notices must be concise, transparent, intelligible and easily accessible.

Controllers will need to review their existing privacy notices and update them in line with the new requirements.

3 Data rights (including subject access requests)

The Current Law already provides certain rights to data subjects (such as employees and customers) over the personal data that a controller may hold about them. This includes a right to access their personal data and rights to stop certain data processing.

The New DP Law makes significant enhancements and additions to these rights, including a new right to delete personal data where continued processing is unnecessary and a right to "data portability", which is the ability to request that certain data is transferred to a different controller.

In addition, the subject access request ("**SAR**") requirements are being made more onerous, so that:

- The time for compliance with any SAR will be one month.
- The ability to charge a fee for a SAR has been removed.
- It is possible to refuse, or ask for a reasonable administration fee for, unfounded or excessive SARs but prescribed information must be provided to the data subject in such circumstances.

Under the New DP Law organisations may be able to lawfully refuse requests from data subjects to rectify or erase personal data if they are unable to do so for technical reasons.

Organisations should consider how their procedures should change to comply with these enhanced rights.

4 Data subject consent

Consent to the processing of personal data must be freely given, specific, informed and unambiguous in order to be valid. We expect that a positive opt-in will be required and so it will not be possible to infer consent from silence, pre-ticked boxes or inactivity. Requests for consent that are bundled in with other terms, rather than clearly separated out, will probably not be sufficient.

Controllers that rely on consent to process data will need to review existing consents to determine whether they would be adequate under the New DP Law or whether there are more appropriate legal grounds to rely on than consent. New consent mechanisms for customers and employees may be required, to ensure compliance with the New DP Law.

Data subjects will have the right to withdraw consent at any time and this could potentially create significant operational issues for controllers. In addition, consent that is compliant with the New DP Law may be difficult to obtain by employers from their employees, since the imbalance of power means that consent may not be seen as having been freely given. As such, controllers may need to look for a different legal basis for processing in the employment context.

5 Legal basis for processing personal data

The legal basis (or bases) adopted for processing personal data will have more of an impact under the New DP Law, as some individuals' rights will be modified depending on the legal basis adopted. For example, if controllers rely on consent, the data subjects may have stronger rights, including a right to deletion of their data.

Alternatives to data subject consent for non-special category personal data include where processing is necessary for the performance of a contract with the data subject or for the purposes of legitimate interests pursued by the controller (except where those interests are overridden by the interests, rights or freedoms of the data subject).

Controllers need to determine the legal basis on which personal data is processed, document this and update the relevant privacy notices to explain it.

6 Accountability – demonstrating compliance

The New DP Law includes an accountability principle, which effectively means organisations must not only comply with the data protection principles but also demonstrate how they comply.

Organisations can take a number of steps to help ensure and demonstrate compliance:

- ✓ Keep records of all data processing activities carried out.
- ✓ Implement (or review existing) technical and organisational measures for achieving compliance, e.g. data protection policies in relation to employee training and internal audits of processing activities.
- ✓ Undertake a data protection impact assessment ("**DPIA**") where controllers are engaged in "High

Risk Processing Activities", e.g. where new technology is being deployed. Controllers could prepare a DPIA policy/template document.

- ✓ Appoint a data protection officer ("**DPO**"), who may be a staff member of the controller or processor (or employed by a group company) or a third party appointed under a service contract. Under the New DP Law, this is a requirement where processors or controllers are engaged in High Risk Processing Activities on a systematic or regular basis. The DPO must reside in the UAE unless he is an individual employed within the organisation's group, performing a similar function for the group company on an international basis.
- ✓ Implement measures that meet the principles of data protection by design and by default, including data minimisation, pseudonymisation, transparency, and improving security features on an ongoing basis.

7 High Risk Processing Activities

The non-exhaustive list of "High Risk Processing Activities" identified by the New DP law as having a greater chance of making personal data vulnerable to unintended disclosure, and therefore requiring additional protections, covers:

- processing that includes the adoption of new technologies or methods that materially increase the risk to data subjects or renders it more difficult for data subjects to exercise their rights;
- processing of a considerable amount of personal data (including staff and contractor data) where such processing is likely to result in a high risk to the data subject (e.g. on account of the sensitivity of the personal data);
- systematic and extensive automated processing, including profiling, with significant effects on the natural person; or
- processing of a material amount of special categories of personal data.

Controllers are expected to take responsibility for complying with the New DP Law in all respects, even where they are carrying on high risk processing activities not referred to in the list.

8 Data breaches and fines for breaches

A personal data breach is a breach of security leading to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

There will be a new mandatory requirement for controllers to notify data breaches to the Commissioner where it is likely to compromise an individual's confidentiality, security, or privacy. Notifications must be made as soon as practicable in the circumstances - there is no set time limit for notifying. When a personal data breach is likely to result in a high risk to the security or rights of a data subject, the controller must also communicate the personal data breach to the affected data subject(s) as soon as practicable in the circumstances.

Failure to notify – in addition to the cost of the breach itself - can result in a fine in an amount considered by the Commissioner to be appropriate, but not exceeding USD $50,000.

The schedule of fines in the Current Law – setting out the maximum applicable fines with respect to certain specific contraventions - has been retained in the New DP Law. The maximum prescribed administrative fine will not exceed USD $100,000.

The Commissioner may also issue a general fine for a contravention of the New DP Law in an amount he considers appropriate and proportionate, taking into account the seriousness of the contravention and the risk of actual harm to any relevant data subject. There is no guidance available yet on the levels of such general fines but regulations may be issued. Data subjects may also bring claims for compensation to be awarded directly to them by the DIFC Courts. Controllers' potential liability may therefore increase, although it remains to be seen whether any upper limit set for general fines will be set as high as under the GDPR (the higher of €20 million or 4% of annual worldwide turnover).

Processors (like certain third party suppliers) will be directly responsible for informing their controller "without undue delay" after becoming aware of a personal data breach. Controllers may wish to make this obligation more onerous under their contracts with processors, for example requiring that the processor notifies them within 24 hours.

Controllers should ensure they have robust procedures in place to identify, assess, record and, where appropriate, notify data breaches. Controllers may also wish to revisit the protection from liability they obtain through indemnities in contracts with processors and any liability insurance.

9 Contracts with processors

The New DP Law places direct legal obligations on **processors** in relation to things like implementing appropriate data security measures and keeping a record of processing carried out on behalf of a controller. Controllers and processors, as well as processors and sub-processors, are also required to ensure their contracts contain certain minimum provisions, such as a description of the scope, nature and purpose of processing. This requirement extends to DIFC companies that outsource their data processing activities to companies outside the DIFC.

Controllers should review and update their contracts with processors to ensure there are

appropriate provisions in relation to the processor's new direct obligations and other relevant matters such as compliance, monitoring and reporting.

Liability and indemnity clauses in contracts should also be reviewed to ensure the risk allocation remains appropriate, given that processors now have direct legal obligations and since controllers and processors will have the same obligations in areas such as security. Processors will be directly liable for breaches under the New DP Law and so may consider seeking indemnities from controllers in relation to data protection fines, or claims for compensation by data subjects, caused by the controllers.

10 Joint Controllers

A further example of the requirement for self-regulation is in the context of Joint Controllers. Two or more Controllers who process personal data jointly must enter into legally binding written agreements that clearly define each of their responsibilities for ensuring compliance with their obligations under the New DP Law. There is nothing to stop Joint Controllers agreeing indemnities and other risk allocation provisions between themselves.

The key elements of this written agreement must be made available to affected data subjects to enable them to exercise their rights in respect of any breaches against each of the Joint Controllers.

If Joint Controllers are in breach of the New DP Law, the Commissioner has the power to apportion any administrative fines between the Joint Controllers in whatever manner it considers appropriate to take account of the parties' respective liability for the breach.

Contact us

Please get in touch with our experts to discuss how we can help your business with the New DP Law.

Kiersten Lucas
Partner, Dubai
T: +971 (0)4 407 3993
M: +971 (0)52 577 7731
E: kiersten.lucas@shlegal.com

Emily Aryeetey
Senior associate, Dubai
T: +971 (0)4 407 3942
M: +971 (0)52 120 3148
E: emily.aryeetey@shlegal.com

Naomi Leach
Partner, London
T: +44 20 7809 2960
M: +44 7769 143 367
E: naomi.leach@shlegal.com

Katie Hewson
Associate, London
T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Alison Llewellyn
Associate, London
T: +44 20 7809 2278
E: alison.llewellyn@shlegal.com