Expert Q&A: DIFC Data Protection Law

by Katie Hewson and Alison Llewellyn, Stephenson Harwood, with Practical Law Data Privacy Advisor

Articles | Law stated as of 14-Sep-2020 | Dubai International Financial Centre

An Expert Q&A with Katie Hewson and Alison Llewellyn of Stephenson Harwood on the Dubai International Finance Centre (DIFC) Data Protection Law No. 5 of 2020 (2020 DPL), which entered into force on July 1, 2020, replacing the DIFC Law No. 1 of 2007 (2007 DPL). Organizations must comply with the 2020 DPL by October 1, 2020. This Expert Q&A discusses the key implications of the 2020 DPL for organizations, steps organizations should take to ensure compliance, and important changes from the 2007 DPL.

On July 1, 2020, the Dubai International Finance Centre (DIFC) Data Protection Law No.5 of 2020 (2020 DPL) took effect, replacing and significantly expanding the existing DIFC Law No.1 of 2007 (2007 DPL). The 2020 DPL aligns DIFC data protection law with international data privacy standards, including the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), and brings a major change in DIFC data protection law.

The DIFC Authority (DIFCA) Board of Directors has also issued new Data Protection Regulations (Regulations) that establish procedures for:

- Notifications to the DIFC Commissioner of Data Protection (Commissioner).
- Accountability.
- Record keeping.
- Fines.
- Adequate jurisdictions for cross-border personal data transfers.

Practical Law Data Privacy Advisor asked Katie Hewson and Alison Llewellyn of Stephenson Harwood to comment on the key implications for organizations of the 2020 DPL, steps organizations should take to ensure compliance, and important changes from the 2007 DPL.

Katie Hewson is a senior associate and data protection specialist with considerable data privacy experience across sectors including life sciences, financial services, and retail. Katie holds a Certified Information Privacy Professional Europe (CIPP/E) accreditation from the International Association of Privacy Professionals.

Alison Llewellyn is a data protection associate with broad experience advising on data privacy issues. Alison has delivered training on the GDPR and the 2007 DPL for the DIFC Academy of Law and contributed data protection commentary to the Laws of the DIFC Vol 2, for which she was named an 'Academy of Law Specialist in DIFC Data Protection Law'.

Alison and Katie have supported a substantial number of clients on extensive GDPR-remediation projects and are currently advising DIFC-based clients on compliance with the 2020 DPL.

Who does the 2020 DPL apply to?

The 2020 DPL applies to controllers and processors incorporated:

- In the DIFC that process personal data, regardless of where the processing takes place.
- Outside of the DIFC that process personal data as part of stable arrangements in the DIFC, other than on an occasional basis. The law will apply to those controllers and processors in the context of processing activity in the DIFC and not in a third country, including transfers of personal data out of the DIFC.

(Article 6(3)(a), (b), 2020 DPL.)

For the purposes of Article 6(3)(b), processing "in the DIFC" occurs when the means or personnel used to conduct the processing activity are physically located in the DIFC (Article 6(3)(c), 2020 DPL).

The 2020 DPL enhances privacy compliance requirements and imposes several direct legal obligations on processors, including in relation to accountability and data security.

When must organizations comply with the 2020 DPL?

Organizations subject to the 2020 DPL must ensure compliance with its requirements by October 1, 2020, following a three-month enforcement grace period. Organizations should immediately:

- Review their current data protection practices.
- Understand the impact of the changes on their business.
- Take any necessary action to ensure compliance by October 1, 2020.

How does the 2020 DPL differ from the 2007 DPL?

The 2020 DPL:

- Provides new standards and controls for personal data processing.
- Introduces a new concept of accountability with enhanced controls and requirements, including:
    - implementing compliance programs;
    - appointing a data protection officer in certain circumstances (see What does high risk processing activities mean? and Who can organizations appoint as a DPO?);
    - conducting data protection impact assessments when engaging in high-risk processing activities (see Who can organizations appoint as a DPO?); and
    - imposing contractual obligations to protect personal data.

    (See Who can organizations appoint as a DPO?.)

- Enhances and clarifies data subject rights (see Does the 2020 DPL introduce any changes to data subject rights?).
- Provides more detailed requirements for certain legal bases for processing, such as legitimate interests and consent (see Does the 2020 DPL change the requirements for valid consent?).
- Introduces fines for serious breaches of the 2020 DPL in addition to or instead of administrative fines (see What are the penalties for non-compliance?).
- Increases maximum fine limits (see What are the penalties for non-compliance?).
- Removes the permit process for cross-border data transfers and processing of special categories of personal data (see Does the 2020 DPL implement any changes regarding cross-border data transfers? and Does the 2020 DPL implement any changes regarding processing special categories of personal data?.)
- Permits organizations using new technologies like artificial intelligence (AI) and blockchain to manage potential conflicts with data subjects' rights by implementing safeguards, such as providing data subjects with enhanced information at the outset.
- Provides for appropriate data sharing structures between government authorities, signifying a key step forward in data sharing standards within the United Arab Emirates and the DIFC.

What steps should organizations take to ensure compliance with the 2020 DPL?

Organizations should begin by performing a data audit as an initial step towards satisfying the 2020 DPL's new accountability requirements and to identify other remediation steps.

The 2007 DPL implicitly required businesses registered in the DIFC to understand what personal data they held and how they held that personal data. The 2020 DPL makes this explicit, requiring controllers and processors to document details including:

- The categories of personal data processed.
- The purposes for personal data processing.
- Who the controller or processor shares the personal data with.

To comply with this new requirement, organizations should perform a data audit covering:

- The categories of personal data processed.
- The purposes for processing personal data.
- The legal bases for processing personal data.
- The source of the personal data processed.
- How the organization stores the personal data.
- Where the organization stores the personal data.

- Data retention periods.
- Who has access to the personal data.

Organizations should also:

- Review and update existing privacy notices to ensure they meet the 2020 DPL's enhanced information requirements (see What does the 2020 DPL's new concept of accountability mean and how can organizations comply?).
- Review existing policies and procedures considering the increased penalties available for 2020 DPL violations (see What are the penalties for non-compliance?).
- Review the legal bases for personal data processing relied on, including for special categories of personal data.
- Ensure existing data subject access request procedures comply with the new shorter timeframes for responding to requests (see Does the 2020 DPL introduce any changes to data subject rights?).
- Understand the new and enhanced data subject rights and review and update existing policies and procedures to reflect the relevant changes (see Does the 2020 DPL introduce any changes regarding data breach notification requirements?).
- Review and update existing procedures to ensure they reflect the new mandatory requirement to report data breaches to the Commissioner (see Does the 2020 DPL introduce any changes regarding data breach notification requirements?).
- Review third-party service provider agreements to ensure compliance with the new requirements for contracts (see Does the 2020 DPL impose any specific requirements for data processing agreements?).
- Review existing third-party service provider contracts and consider initiating negotiations with existing third-party service providers over the extent of their liability for 2020 DPL breaches and any indemnities required.
- Familiarize themselves with the new Regulations issued by the DIFCA Board of Directors that establish procedures for:
    - notifications to the Commissioner;
    - accountability;
    - record keeping;
    - fines; and
    - adequate jurisdictions for cross-border personal data transfers.

What does the 2020 DPL's new concept of accountability mean and how can organizations comply?

The 2020 DPL includes a new accountability principle which requires organizations to:

- Comply with the data protection principles.
- Demonstrate how they comply.

(Article 9, 2020 DPL.)

To ensure and demonstrate compliance, organizations should:

- Keep records of all data processing activities.
- Review, update, or implement appropriate technical and organizational measures to achieve compliance, such as data protection policies in relation to employee training and internal audits of personal data processing activities.
- Perform a data protection impact assessment (DPIA) when engaged in high-risk processing activities, such as where new technology is deployed.
- Develop and implement a DPIA policy and template document.
- Appoint a DPO where necessary.
- Implement data protection by design and by default measures, including data minimization, pseudonymization, transparency, and regularly reviewing and improving security features on an ongoing basis.
- Familiarize themselves with new data protection regulations issued by DIFCA that establish procedures for accountability and record keeping.

Do organizations need to review their existing privacy notices?

Yes, controllers should review and update existing privacy notices to ensure they comply with the 2020 DPL's new information requirements. The 2020 DPL enhances the 2007 DPL's fair processing information requirements and requires controllers to communicate additional information to data subjects, including:

- The purposes of and legal basis for processing personal data.
- Data retention periods or the criteria for determining data retention periods.
- Information about data subjects' rights including individuals' right of complaint to the Commissioner.

(Article 29(1), 2020 DPL.)

Organizations should ensure that privacy notices are:

- Concise.
- Transparent.
- Intelligible.

- Easily accessible.

Controllers relying on data subject consent should ensure that the consent meets the 2020 DPL's requirements for valid consent (see What are the DPL 2020's requirements for valid consent?).

What are the 2020 DPL requirements for valid consent?

To be valid, consent to personal data processing must be:

- Freely given.
- Specific and informed.
- Unambiguous.
- Capable of being withdrawn at any time.

Organizations should:

- Obtain positive opt-in consent. Consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent. Implied consent based on silence, pre-ticked boxes, or inactivity is not sufficient.
- Ensure requests for consent are not bundled together with other terms. The request for consent must be clearly distinguishable from other matters to be sufficient.
- Review existing consents to determine if they meet the requirements for valid consent under the 2020 DPL or if the organization can rely on other, more appropriate legal grounds for processing.
- Consider if new consent mechanisms are required to comply with the 2020 DPL.
- Consider the potentially significant operational impact of data subjects' right to withdraw consent at any time, if the organization can comply with this right or whether it should rely on an alternative legal basis for processing personal data.
- Recognize that obtaining valid consent in the employment context is difficult due to the imbalance of power between employers and employees. Controllers should look for a different legal basis for processing in the employment context.

Does the 2020 DPL introduce any changes to data subject rights?

Yes. The 2007 DPL granted certain rights to data subjects, including a right of access to personal data and a right to object to certain data processing. The 2020 DPL makes significant enhancements and additions to existing data subject rights, including:

- The right to rectify, restrict, or erase data in certain circumstances.
- A new and specific right to non-discrimination for exercising any data subject rights.
- New rights to address the impact of emerging technologies, including:

    - the right to object to automated decision-making, including profiling, in certain circumstances and require controllers to manually review such decisions; and
    - a data portability right to request the transfer of certain personal data to a different controller.

- More stringent data subject access request requirements, including:
    - allowing verbal data subject access requests, in addition to written requests;
    - reducing the time for complying with a data subject access request to one month;
    - removing the ability to charge a fee for a data subject access request;
    - requiring controllers to provide data subjects with reasons for refusal of a request which it considers unfounded or excessive (Article 33(8), 2020 DPL); and
    - requiring controllers to provide at least two methods that data subjects can use to exercise their rights, for example, post, telephone, email, or online forms.

The 2020 DPL permits organizations to refuse data subject rectification or erasure requests in certain circumstances, including if it is not technically feasible to comply with the request, subject to review and approval by the Commissioner or Director of Data Protection.

Organizations should review and update their policies and procedures to comply with these new and enhanced rights.

Who can organizations appoint as a DPO?

The 2020 DPL requires the appointment of a DPO where organizations perform high-risk processing activities on a systematic or regular basis (see What does high risk processing activities mean?). Organizations may appoint an employee, a group company employee, or a third party appointed under a service contract as a DPO. The DPO must reside in the UAE unless the DPO is employed by the organization's group company performing a similar function for the group company on an international basis. (Articles 16, 17, 18, and 19, 2020 DPL.) DPO's must assess the controller’s processing activities annually.

What does high risk processing activities mean?

The 2020 DPL establishes a non-exhaustive list of high-risk processing activities which are considered to pose a greater risk of exposing personal data to unintended disclosure and therefore require additional protection. High-risk processing activities include:

- Processing that includes the adoption of new technologies or methods that materially increase the risk to data subjects or renders it more difficult to exercise data subject rights.
- Processing large volumes of personal data where the processing is likely to result in a high risk to the data subject because of the personal data's sensitivity.
- Systematic and extensive automated processing, including profiling, with significant effects on individuals.
- Processing large volumes of special categories of personal data.

(Schedule 1, Article 3, 2020 DPL.)

Controllers are expected to comply with the 2020 DPL in all respects even where they are carrying on high-risk processing activities not referred to in the list.

Does the 2020 DPL implement any changes regarding cross-border data transfers?

Yes. The permit process for cross-border data transfers which existed under the 2007 DPL no longer applies.

The 2020 DPL generally restricts cross-border personal data transfers to jurisdictions outside of the DIFC. However, it permits cross-border data transfers outside the DIFC to jurisdictions that:

- Provide an adequate level of personal data protection (Article 26(1), 2020 DPL). Appendix 3 of the Regulations sets out the list of countries deemed adequate.
- Do not provide an adequate level of personal data protection, provided:
    - the controller or processor provides appropriate safeguards, including standard data protection clauses adopted by the Commissioner or binding corporate rules, and the recipient jurisdiction provides enforceable rights and effective legal remedies for data subjects' rights (Article 27(1)(a), (2)); or
    - an exemption applies (Article 27(3), 2020 DPL).

The Commissioner applies the same adequacy standards as the European Commission and the standard data protection clauses are based on the European Commission standard contractual clauses (EC SCCs). The Commissioner has confirmed that existing contracts incorporating the EC SCCs remain valid as an appropriate safeguard.

Absent an adequacy decision, appropriate safeguards, or an applicable exemption, the 2020 DPL permits a controller to transfer personal data cross-border in certain limited circumstances (Article 27(4), (5), 2020 DPL).

Does the 2020 DPL implement any changes regarding processing special categories of personal data?

Yes. There is no longer a permit process for processing special categories of personal data. Instead, controllers must identify a lawful basis for processing special categories of personal data listed in the 2020 DPL (Article 11, 2020 DPL).

Does the 2020 DPL introduce any changes regarding data breach notification requirements?

Yes. The 2020 DPL introduces a new mandatory requirement for controllers to notify the Commissioner of data breaches which are likely to compromise an individual's confidentiality, security, or privacy (Article 41(1), 2020 DPL). The 2020 DPL does not specify a timeframe for notifying, however, controllers must notify the Commissioner of any breaches as soon as practicable in the circumstances. The controller must also communicate the personal data breach to the affected data subjects as soon as practicable when a personal data breach is likely to result in a high risk to the security or rights of a data subject.

In addition to the cost of the breach itself, failure to notify can result in a fine amount determined by the Commissioner, but not exceeding $50,000.

The 2020 DPL imposes a direct obligation on processors to inform controllers of a data breach without undue delay. Controllers should consider making this obligation more onerous in data processor agreements, for example, by requiring the processor to notify 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 from indemnities in contracts with processors and any liability insurance.

Does the 2020 DPL impose any specific requirements for data processing agreements?

Controllers, processors, and sub-processors must ensure their data processing agreements contain certain minimum mandatory provisions, such as a description of the scope, nature, and purpose of processing (Article 24(1), 2020 DPL). This requirement extends to DIFC companies that outsource their data processing activities to companies outside the DIFC.

Controllers should also review and update their data processing agreements 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. Controllers should also review any liability and indemnity clauses in agreements to ensure the risk allocation remains appropriate, considering:

- Processors' new direct legal obligations.
- Controllers and processors have the same legal obligations in areas, such as security.

Processors are directly liable for breaches under the 2020 DPL and may consider seeking indemnities from controllers in relation to potential fines or compensation claims by data subjects caused by the controllers.

Are organizations still required to register with the Commissioner?

Yes. However, the 2020 DPL requires organizations to provide more information to the Commissioner as part of the registration process compared to the 2007 DPL's requirements. Controllers and processors must register with the Commissioner, irrespective of whether the organization processes personal data. No fee is payable applies if the organization does not process personal data. Failure to register with the Commissioner may result in enforcement action, including fines of up to $25,000.

What are the penalties for non-compliance?

The 2020 DPL retains the schedule of fines set out the 2007 DPL, which specifies the maximum applicable fines for specific violations (Schedule 2, DPL). The maximum administrative fine for the most serious violations has increased from $25,000 under the 2007 DPL but will not exceed $100,000.

The Commissioner may also issue a general fine for a serious violation of the 2020 DPL based on what the Commissioner considers appropriate and proportionate, considering the seriousness of the violation and the risk of actual harm to data subjects. The Commissioner has wide discretion to issue general fines, for which there is no prescribed maximum level.

Data subjects may also initiate court proceedings for compensation claims.

Controllers' potential liability may therefore increase under the 2020 DPL, although it remains to be seen whether any upper limit set for general fines is set as high as under the GDPR, which provides for fines of up to EUR €20 million or 4% of annual worldwide turnover, whichever is greater.

END OF DOCUMENT