Data Transfers

Charlotte Sutcliffe - Associate - Digital & Data
- Dubai International Financial Centre

The Dubai International Financial Centre ("**DIFC**") has issued a new Data Protection Law DIFC Law No. 5 of 2020 ("**DIFC DP Law**"). This law applies in the jurisdiction of the DIFC only.

In this article, we discuss an entity's obligations under the DIFC DP Law when it wishes to transfer personal data outside the DIFC.

There are many reasons an entity may wish to transfer personal data to another jurisdiction outside the DIFC. Namely, that entity may have a parent or subsidiary entity, or an affiliate outside of the DIFC (including in onshore UAE). It may require transferring personal data for administrative purposes, to analyse and monitor that data, for record keeping of employee, contractor and client data, and even to provide personal data to third parties for marketing purposes.

Regardless of why the entity is transferring personal data, it is very important that the relevant entity has systems and procedures in place to ensure that personal data is processed for the purposes or related purposes which the data subject expected, unless one of the exemptions outlined in the DIFC DP Law applies. Entities should ensure they understand what personal data is being transferred, where and for what reason. Controllers and processors must maintain written records of processing activities ("**ROPA**") for which it is responsible or carrying out as instructed. The ROPA must contain information that sets this out, and includes details of the technical and organizational measures that are applied to the processing.

Requirement for adequate level of protection

According to the DIFC DP Law, entities must ensure they protect and safeguard personal data. One primary factor that determines an entity's obligations under the DIFC DP Law is whether the outside jurisdiction receiving the personal data has a level of protection over personal data which is considered to be adequate or inadequate.

The adequate jurisdictions are set out in Appendix 3 of the DIFC DP Regulations and include transfers to: the United Kingdom, Europe and the Abu Dhabi Global Market. A jurisdiction which many house affiliates of many entities operating in the DIFC and is not considered an 'adequate jurisdiction is the United States'. The "Privacy Shield" replaced Safe Harbour in 2016, and is a mechanism recognised by the European Commission for transferring personal data between the European Union / European Economic Area and the United States of America. The DIFC does not recognise it for this reason, as DIFC has no such agreement in place for transfers of personal data from the DIFC to the United States of America. Therefore, Privacy Shield cannot be relied upon for transfers from the DIFC to the United States of America.

On this basis, the DIFC DP Law requires that entities implement safeguards for transfers of personal data to jurisdictions such as the United States

In addition, the Commissioner may determine that a jurisdiction outside the DIFC does have an adequate level of data protection, in its discretion, by taking into account factors including:

- the rule of law, the general respect for individual's rights and the ability of individuals to enforce their rights via administrative or judicial redress;
- the access of a public authority to personal data; and

- the existence of effective data protection law, including rules on the onward transfer of personal data to another jurisdiction.

Transfers in the absence of an adequate level of protection

If the Commissioner has determined that the third party jurisdiction does not have an adequate level of protection, a transfer may only take place under certain circumstances including that:

(A) The controller or processor in question has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards referred to in (a) above may be provided for by factors including:

- a legally binding instrument between public authorities;
- Binding Corporate Rules; and
- standard data protection clauses as adopted by the Commissioner in accordance with Regulations setting out a procedure for developing such clauses.

The Commissioner has provided a set of standard clauses to be applied to contractual or other arrangements that require the transfer of personal data outside of the DIFC. They are available on the DIFC website. The standard clauses may not be altered other than to complete basic information or provide additional commercial requirements. If any alteration to the standard clauses is contemplated by the relevant entity utilizing them, the Commissioner should be consulted first and such alterations agreed in writing.

OR

(B) A derogation applies, including:

- a data subject has explicitly consented to a proposed transfer, after being informed of possible risks of such transfer due to the absence of an adequacy decision or appropriate safeguards. Note: entities could attempt to bury the transfer in their terms and conditions or privacy policy, but this would not be acceptable here as the DIFC DP Law requires explicit consent. Though a Data Subject may give “explicit” consent, relevant entities cannot infer consent from non-response to a communication, for example from a customer’s failure to return or respond to a leaflet. The adequacy of any consent or purported consent must be evaluated. For example, consent obtained under duress or on the basis of misleading information will not be a valid;
- the transfer is necessary for the performance of a contract between a data subject and controller or the implementation of pre-contractual measures taken in response to the data subject’s request. Note: this could include the data subject’s employment contract;
- the transfer is necessary for the conclusion or performance of a contract that is in the interest of a data subject between a controller and a third party;
- the transfer is necessary for reasons of “Substantial Public Interest” (e.g. to conduct criminal and regulatory obligations);
- the transfer is necessary or legally required in the interests of the DIFC, including in the interests of the DIFC Bodies relating to the proper discharge of their functions;
- the transfer is necessary for the establishment, exercise or defence of a legal claim;
- the transfer is necessary in order to protect the vital interests of a data subject or of other persons where a data subject is physically or legally incapable of giving consent; and
- the transfer is necessary to comply with applicable anti-money laundering or counterterrorist financing obligations that apply to a controller or processor or for the prevention or detection of a crime.

Where a transfer could not be based on the safeguards or derogations set out above, such transfer may take place only if the transfer:

- is not repeating or part of a repetitive course of transfers;
- concerns only a limited number of data subjects;
- is necessary for the purposes of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights of the data subject; and
- the controller has completed a documentary assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of the personal data.

Data sharing

The DIFC DP Law also covers controller and processor obligations around data sharing (as distinct from data transfers). This occurs when a government entity requests the controller or processor to share personal data with it. It is common for government organizations or authorities to request data, including personal data, on demand for a variety of purposes. While the Commissioner encourages such sharing, the organization receiving such request still needs to consider what controls should be in place to govern the sharing and ensure that all parties involved will apply them. If the organisation deems a request too broad, it may ask for specificity or request appropriate, written binding assurances that the data will be ethically and responsibly managed.

Under the DIFC DP Law, where a controller or processor receives a request from any public authority the disclosure and transfer of any personal data, it should:

- exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of personal data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the requesting authority;
- assess the impact of the proposed transfer in light of the potential risks to the rights of any affected data subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the personal data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and
- where reasonably practicable, obtain appropriate written and binding assurances from the requesting authority that it will respect the rights of data subjects and comply with the relevant data protection principles.

Before personal data is shared in response to a request for information the relevant entity should consider:

- Is all of the information in the request necessary to share?
- Is it subject to another law or regulation, thereby limiting the decision about whether to share or not, i.e., for the prevention of crime or for reasons that could save an individual’s life or health?

The DIFC DP Law Guide suggests the creation of policies regarding sharing personal data with government entities. Examples are contained on the Commissioner’s website.

Conclusion

An entity may choose or be required to transfer personal data outside the DIFC for many reasons, including record keeping and third party marketing purposes. Under all circumstances, it is necessary for

the entity to scrutinise what personal data it is sending, to which third parties and for what purposes. Further, that entity should ensure it meets all requirements under the DIFC DP Law, depending on whether or not the third party jurisdiction has been considered to have an adequate level of protection in accordance with the DIFC DP Law.

For further information, please contact Charlotte Sutcliffe (c.sutcliffe@tamimi.com).