DIFC DP Law: data subject rights

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

The Dubai International Financial Centre ('DIFC') issued a new Data Protection Law DIFC Law No. 5 of 2020 ('DIFC DP Law'), redacting the DIFC Law No. 1 of 2007.

This legislation, modelled on the gold standard General Data Protection Regulation ('GDPR'), provides enhanced standards and controls for the processing and free movement of personal data by controllers and processors and protects the fundamental rights of data subjects. This includes how such rights apply to the protection of personal data in emerging technologies.

In this article, we focus on the obligations controllers (i.e .entities that control the processing of personal data) and processors (i.e. entities under the direction of a third party to process personal data) have to data subjects (i.e. the individuals from whom personal data is collected) when gathering personal data, and the rights of data subjects to object to the processing of personal data relating to them.

At a high level, there is a global discussion on the importance of an individual's right to privacy, and to what extent this needs to be protected or even compensated. All around the world, individuals are handing over their precious data ('the oil of the 21st Century') to technology companies without exact knowledge of how and why the data is processed. In some cases, companies use the data for direct marketing, and at times, in profiling activities.

Privacy regimes such as the DIFC DP Law attempt to create a framework that understands the importance and value of data to various entities, in their quest for a more innovative world, whilst also protecting an individual's privacy. Data rights give individuals an autonomy over their data, which effectively, in the 21st Century, means autonomy over their private lives, and the ability for those private lives to be tracked and recorded into the future.

Individual rights

Articles 32 to 38 of DIFC DP Law set out the data subject rights, which include:

- data subject having the right to withdraw consent at any time through notifying the controller;
- the data subject's right to access, rectification and erasure of personal data;
- under certain circumstances, the data subject's right to object to the processing of personal data;
- the data subject's right to restrict the processing;
- the data subject's right to data portability; and
- the data subject's right to object to any decision based solely on automated processing, including profiling.

These rights are generally comparable to those outlined in the GDPR.

Right to withdraw consent

Overall, the DIFC DP Law identifies three bases for what constitutes "lawful processing" which include:

- consent,
- necessity (the processing is necessary to perform certain specified tasks), and
- legitimate interest.

In the same manner as provided in the GDPR, the processing can be justified by a “legitimate interest” only if the interest of data controller is not overridden by the rights or interests of the data subject.

Consent with regards to the subject matter of data protection can be defined as the specific and informed indication of the data subject that is unambiguous in nature, through either a statement or some action that can denote agreement of the processing of personal data.

The right to withdraw consent is the basic right of the data subject to request the termination of processing the data and it is the duty of the Controller to comply with the same.

In order for the right to be enforced:

- the data subject must make a request to the controller (in writing or verbally) for the cessation of processing of data;
- the request can be made through the forums of contact that have been provided by the controller such as the telephone number or email. If the organisation has a website, a free source of contact will be mentioned and can be utilised for this right; and
- the controller has one month to process the request and cease the use of data as well as delete all data securely.

Right to access, rectification and erasure

The right to access is as its name suggests, the right of an individual to obtain information from the controller in regards to the personal data. The information that can be obtained includes:

- whether the personal data of the data subject is being processed;
- for what purpose the data is being processed; and
- what are the categories under which the personal data falls and the categories of persons who would be receiving this data.

In order for the data to be accessed, the data subject must make a subject access request. This request is made to a controller, usually in writing, but the same is not a requisite mandated by law and can be done in any form, for example verbally through a telephone call. The controller has a month to respond to the same and may not charge anything in that regard unless in exceptional circumstances, where there may be high administrative or documentation costs involved.

Objection to processing

The law provides for the right to object to the processing of personal data, but this is not an absolute right and can be denied.

A data subject can object at any given time on personal data processing relating to him or her. The objection of the same can be raised by the data subject on reasonable grounds. This objection can be raised on the understanding that processing of data is carried out on the grounds that:

- it is considered to be a necessity with regards to performing a task in the name of public interest; and

- there are legitimate interests of a controller or a third party involved.

Apart from raising an objection, a data subject is conferred with an important right of objection in regards to being informed by the controller:

- the right to be informed when personal data is being disclosed to third parties for the first time or used in the process of direct marketing; and
- when direct marketing is looked at, an express right to object is conferred upon the data subject. This right of objection can be used at any time and even with regard to profiling.

Restriction of processing

A data subject also has the right to request to restrict the processing of data by a controller in certain circumstances. Similar to the right of objection, this is not an absolute right. The purpose of such a right is to restrict the way a party can utilise their personal data. This right is considered to be an alternative to the right to erasure or the right to be forgotten.

The circumstances in which such a right can be enforced are as follows:

- when the data subject questions the accuracy of the personal data that is being processed. This allows the controller a period to check the accuracy of such data;
- the personal data that is being processed is deemed unlawful and the data subject would rather restrict such data than erase it;
- when the controller no longer has use for the data but the data subject requires this data for the legal claims in regard to either establishing such claims, exercising such claims or a defence to such claims;
- when a data subject objects to the processing of personal data, if legitimate alternative grounds exist for the controller to override the data subject.

Data portability

The data subject also has the right to obtain the information that was provided by him or her to the controller in a structured, commonly used and machine readable format. This is possible when:

- the data subject consented on the processing through the performance of a contract;
- it is done by automatic means
  - is even possible, at the request of the data subject.to transmit the personal data directly from one controller to another; and
  - this right is subject to certain exceptions and that is such that transmission would affect the rights of another natural person.

Automatic processing

The data subject possesses the right to object to decisions that have taken place as a result of any automated processing. This includes profiling or anything that could have serious legal or consequential effects on the data subject.

Like most rights, this is not an absolute right and comes with certain exceptions and they include:

- the data processing is needed for the performance of a contract between a data subject and controller;
- the data processing is authorised by the law to which the controller is subject; and
- the data subject provided explicit consent.

Right of non-discrimination

The DIFC DP Law introduced an original data subject right: "Right of Non-Discrimination" under Article 39. As the DIFC DP Law includes the right of non-discrimination against a data subject who exercises his or her privacy rights under the DIFC DP Law (in circumstances where the data subject is denied goods or services, or charged more for them). This Article states a Controller may not discriminate against a data subject who exercises any rights under the DIFC DP Law, including by:

- denying any goods or services to the data subject;
- charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- providing a less favourable level or quality of goods or services to the data subject; or
- suggesting that the data subject will receive a less favourable price or rate for goods or services or a less favourable level or quality of goods or services.

From a global standpoint, the new stance of the DIFC DP Law is different to many around the Gulf, as the Right of Non-Discrimination is still yet to be incorporated into the GDPR. Like The California Consumer Privacy Act ('CCPA'), the clause allows controllers to offer financial and other incentives to data subjects for their willingness to allow the controller to use personal information about them.

The CCPA provides data subjects with a right to non-discrimination when they exercise other privacy rights under the law, such as the right to access, delete, or opt out of the sale of their personal information. However, the meaning of "non-discrimination" and the exceptions to this prohibition provided in the CCPA and proposed regulations are among the more confusing aspects of California's privacy law.

Data Breach Notification

The new DIFC DP Law includes comprehensive provisions on an entity's obligations regarding data breach notification. Similar to the GDPR, the legislation distinguishes notifications to be provided to the Commissioner of Data Protection from notification to be provided to the data subjects.

The notification to data subjects is triggered only when the breach "is likely to result in a high risk to the security or rights of a data subject". In this case, there is also no maximum timeframe for making the notification. It would be "as soon as practicable in the circumstances", or "promptly" when there is "an immediate risk of damages".

Compensation

Like the GDPR, the DIFC DP Law contains provisions which allow for data subjects to make compensation claims in relation to breaches of the DIFC DP Law. Therefore, under the DIFC DP Law, court proceedings can be initiated by the Commissioner of Data Protection as well as by data subjects.

Conclusion

The DIFC DP Law applies to the processing of personal data by a controller or processor incorporated in the DIFC, regardless of whether the processing takes place in the DIFC or not. Entities must ensure they are respecting the rights of data subjects in accordance with the DIFC DP Law, including filling in all gaps between the DIFC DP Law and the GDPR, and the DIFC DP Law and previous DIFC data protection law (DIFC Law No. 1 of 2007) as applicable.

For more information on how we can help, please contact Charlotte Sutcliffe (c.sutcliffe@tamimi.com).