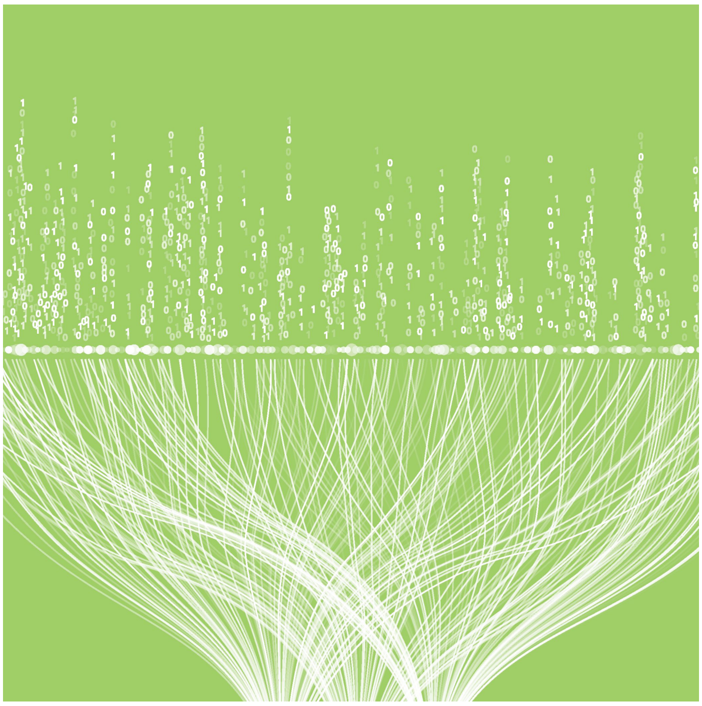
DIFC and ADGM Data Protection and Commercial Litigation: Data Subject Access Requests

Martin Hayward - Head of Digital & Data - Digital & Data
- Dubai International Financial Centre



Dispute resolution rarely runs in a straight line, from the raising of a pre-action complaint, to a substantive hearing on the claim, and a final judgment disposing of the action. Interim applications often disrupt this linear process, and issues such as disclosure and security for costs can spawn satellite dispute resolution processes that divert the parties from the main, underlying conflict.

Some ancillary measures are more useful than others in advancing the substantive dispute, however. A good example is the use of data protection law in commercial disputes. This phenomenon has been common in a number of jurisdictions for many years. The development of data protection legislation in the DIFC and ADGM and the maturation of the UAE's common law courts means that parties in commercial disputes are increasingly using data protection laws to further their position, primarily to flush out documents that would aid their case or undermine their opponent's. A similar trend is showing in relation to DIFC employment disputes.

This article is the first in a series that looks at two measures, data subject access requests and regulatory investigations, in that context.

What Is A Data Subject Access Request Under DIFC and

ADGM Law?

The DIFC Data Protection Law (Law No. 1 of 2007 as amended) governs data protection law in the jurisdiction of the DIFC. As a recap:

- the DIFC Data Protection Law focuses on information that allows the identification, directly or indirectly, of any natural living person, whether by reference to an identification number or to one or more factors specific to his/her biological, physical, biometric, physiological, mental, economic, cultural or social identity ('Personal Data');
- Personal Data identifies a natural person and is information which is processed by means of equipment operating automatically in response to instructions given for that purpose, is recorded with the intention that it should be processed by means of such equipment, or is otherwise recorded as part of a 'Relevant Filing System';
- the DIFC Data Protection Law provides that natural persons ('Data Subjects') have rights of access to Personal Data being held, processed or otherwise relating to them;
- Article 17 creates the right to a Data Subject access request ('DSAR'). It obliges a person (including a legal person) who controls such Personal Data ('the Data Controller') to provide, upon request, confirmation in writing as to whether or not Personal Data relating to that person is being processed and information at least to the purposes of the processing, the categories of Personal Data concerned, and the recipients or categories of recipients to whom the Personal Data are disclosed;
- the Data Controller should communicate to the Data Subject in an intelligible form the Personal Data undergoing processing including any available information as to the source of the Personal Data;
- the Data Controller should, as appropriate, rectify, erase or block the processing of Personal Data that is not processed in accordance with the DIFC Data Protection Law. All of this should be done within a "reasonable interval" and "without excessive delay or expense" by the Data Controller; and
- Article 18 of the DIFC Data Protection Law additionally provides the Data Subject with the right to object to the processing of his/her Personal Data on reasonable grounds relating to his/her personal situation Where there is a justified objection, the Data Controller may not process the material Personal Data in that way.

Similar provisions exist in ADGM law under the ADGM Data Protection Regulations 2015 , Articles 10 and 11.

How Can a DSAR be Used in Commercial Litigation?

It is important to note that a DSAR can only be made on behalf of a natural person and not a company. However, given that every company must have one or more humans at its heart, it is not usually difficult to see how a request based on Personal Data relating to a person can be usefully demanded from a prospective or actual counterparty in a dispute.

Parties in disputes usually want more information, particularly in the form of documents or other data and especially documents possessed by their adversary to which they do not have access. The Rules of the DIFC Courts and the ADGM Court Procedure Rules each have processes permitting parties to request documents before and during litigation, as do arbitral rules such as the DIFC-LCIA and ICC. However, DSARs may force the disclosure of documents, including hard copies and emails, which are relevant to a dispute but not captured within the dispute resolution process. This could be for a number of reasons, such as because the parties have not asked for them, because they do not fall within the scope of disclosure ordered by the court or tribunal, or because the Personal Data provide search terms which cast a wider net for searches.

Cost is a big issue as litigation and arbitration can be very expensive, particularly when fees for lawyers and IT disclosure platform providers are taken into account. DSARs can therefore provide a cheap and low risk form of pre-action disclosure or third party disclosure. The only real risk in a DSAR is if the Data Controller rejects or truncates the disclosure made in response to the request, in which case the Data Subject may need to engage the DIFC Commissioner for Data Protection ('CDP') or the ADGM Office of Data Protection ('ODP') for assistance. Even then, the statutory regulators may intervene on behalf of the Data Subject and make orders against the Data Controller. Ultimately, the Data Subject may need to apply to Court for an order, with or without the assistance of the statutory regulator. At all stages prior to an application to Court, the Data Subject's expended cost and his/her potential liability for the Data Controller's costs are low.

DSARs do not require an order from a court or tribunal, nor do they require Data Controllers to be added to litigation or arbitration for the purposes of a search and disclosure. They are freestanding rights of action that can be exercised at any time, whether or not proceedings are on footing. They are also easy to make and can be made in a number of formats. Both the DIFC and ADGM rules adopt European rules on data protection prior to the General Data Protection Regulation 2018, and particularly the scheme set out in the UK Data Protection Act 1998, but with variations. The DIFC Data Protection Policy Guidance published by the CDP notes that a DSAR must normally be in writing, but there is no specific format required. Unlike in the UK, DSARs in the DIFC should usually be free of charge unless the request results in high administrative costs or additional copies are required. DSARs generally oblige Data Controllers to respond in a timely fashion.

How Should a DSAR be Responded to?

As a rule, a Data Controller receiving a DSAR should respond promptly and efficiently upon receiving a DSAR. As the DIFC's Guidance notes, "Generally, controllers that hold or process personal data about an individual must confirm whether or not personal data concerning him or her are being processed, and, where that is the case, the controller must give the individual access to the personal data, with very few and limited exceptions." As such, large Data Controllers would be well advised to investigate appropriate information management technology that allows rapid searching across all of the organisation's functions captured by the DSAR scope. Data Controllers may wish to have information barriers in place so that data within the jurisdiction of the DIFC or ADGM is easily identifiable and searchable. If the DSAR is made for dispute resolution purposes, the litigation or arbitration team may not be aware that it has been made, and so good internal communications are necessary. External counsel should be advised if a DSAR has been made as it may have a bearing on the dispute.

There are a number of principle grounds for resisting the scope of a DSAR:

First, objections to the scope of search including proportionality of searching for material data. English case law (which is persuasive in the DIFC and ADGM) has established that a Data Controller is obliged only to carry out a reasonable and proportionate search in response to a DSAR. The ground of proportionality alone will rarely be a sufficient reason to justify the recipient of a DSAR failing to attempt even to carry out a search. However, if a Data Controller believes that a search would be genuinely disproportionate, a clear record should be kept of the basis upon which this conclusion was reached, including estimates of the time the search would take and the costs it would incur. Data Controllers can engage with the Data Subject to reduce and clarify the scope of DSARs as far as possible, such as by requesting further information about when the data was processed and for what it was processed.

Second, objections on the grounds of privilege and confidentiality. Under European data protection law (the General Data Protection Regulation ('GDPR') and the related UK 2018 Data Protection Act) legal professional privilege and confidentiality are exemptions to the Data Controller's transparency requirements, allowing a Data Controller to refuse to provide Personal Data if it were legally privileged or if it were information in respect of which a duty of confidentiality was owed by a professional legal adviser to a client. However, neither the DIFC Data Protection Law nor the ADGM Data Protection Regulations contain these explicit exemptions. Given the logic of both exemptions, and the closeness with which the DIFC and ADGM schemes follow English law, it is likely that, upon invitation, the DIFC Courts and ADGM Courts could develop their own jurisprudence on the issues. As a result, Data Controllers should generally satisfy themselves that the relevant documents really are legally privileged or confidential in the traditional sense because, if they not, they will need to be disclosed. Even if the legal privilege and confidentiality exemptions apply, a search cannot be completely avoided, and suitable processes should be in place to identify potentially privileged and confidential material and separate it for further consideration. If in doubt, a Data Controller should apply a presumption of non-disclosure and seek the views of the appropriate statutory regulator.

Finally, the Data Subject's motive in making the DSAR, and particularly his/her timing in so doing. An early English Court of Appeal decision (Durant v Financial Services Authority [2003] EWCA Civ 1746) established the principle that a DSAR is not an automatic right, such as for employees to access all personal data held about them by their employer for the purposes of litigation. The purpose of the request could be considered too. However, in Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74, the Court of Appeal rowed back from that position, holding that the motive behind the making of the DSAR was irrelevant to whether or not the employer should comply with it. The individual was entitled to make a DSAR even if the collateral purpose in doing so was to aid litigation. There is nothing in the DPA that limits the purpose of a DSAR or places a requirement on an individual to explain what they want the information for, and the existence of an ulterior motive did not vitiate the rights of the Data Subject. The DIFC and ADGM regulators and Courts respectively may develop an analysis of the Data Subject's motivation in future, when considering whether to order a Data Controller to respond to a DSAR.

What Is the Future of the DSAR?

Given the advent of the GDPR, regulators around the world are re-thinking their data protection regimes. In the DIFC, the CDP published Consultation Paper No. 6 in June 2019 with a proposed new data protection law for the DIFC. Similar changes are expected in the ADGM. The proposed new DIFC data protection law contains provisions that require Data Subjects to be provided with information and specify the required information and conditions of the presentation and delivery of the information. The proposed right of access to Personal Data remains an absolute right, subject to limited exceptions created by the law. The list of individual remedies suggested is an increase on the existing rights under the current DIFC Data Protection Law.

Perhaps, in both the ADGM and the DIFC, the biggest change to the DSAR regime will be a widening in the scope of information that a Data Controller must provide. Pre-GDPR, the Data Controller had to provide a copy of the Personal Data and confirm whether it is processing them. Now, the Data Controller must also provide additional information including the purposes of processing, the categories of Personal Data concerned, the recipients or categories of recipients of the Personal Data, notice of the existence of the right to request rectification, erasure or restriction, information about the source of the data when not obtained directly from the Data Subject, and the existence of automated decision-making such as profiling. This has the potential for greatly increasing the time and cost for a Data Controller in managing a DSAR and, as a result, may well make the use of DSARs a more potent litigation tool.

Al Tamimi & Company's TMT team and International Litigation Group are experienced in advising data subjects and data controllers alike on making and responding to data subject access requests, and adversarial proceedings before the statutory regulators and Courts in the DIFC and ADGM. For further information, please contact Martin Hayward (m.hayward@tamimi.com) or Peter Smith (p.smith@tamimi.com).