DIFC and ADGM data protection and commercial litigation: data protection in disclosure

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

Peter Smith - Senior Associate - International Litigation Group / Litigation - Dubai International Financial Centre

In the November 2019 edition of Law Update, we explained the uses of data subject access requests ('DSARs') as tools in commercial litigation in the courts of the Dubai International Financial Centre ('DIFC') and the Abu Dhabi Global Market ('ADGM').

Since that article was published, the DIFC has introduced a new Data Protection Law (Law No.5 of 2020; the 'New Data Protection Law'). The New Data Protection Law substantially updated the DIFC's previous Data Protection Law (Law No.1 of 2007 as amended; 'Previous Data Protection Law'), setting out a new regime for governing data protection in the jurisdiction of the DIFC and the powers of the DIFC's Commissioner for Data Protection ('CDP'). In this second article in our series on the UAE's current data protection regimes as they apply in the UAE's common law jurisdictions, we look at considerations relating to data protection in the dispute resolution process and in the context of disclosure.

The disclosure or the 'discovery' of documents is a key part of any dispute resolution process. The DIFC and ADGM Courts have a default model of disclosure based on international arbitration norms, whereby in summary the parties: (a) provide documents in support of their claim or defence in a first phase known as 'standard' disclosure, upon which they will rely at trial; (b) make requests of their opponent for documents that are relevant and material to the outcome of the case (usually tabulated so that categories of documents relate to certain issues in the case); (c) respond to their opponent's requests and reply to their opponent's responses to their own requests; and (d) search for and provide copies of documents falling within categories of disclosure as ordered by the judge or the tribunal.

Parties engaging in disclosure must do so in ways which comply with the relevant and applicable data protection laws. From the outset of a dispute, documents will be exchanged between parties, in pre-action correspondence and then in the formal disclosure process described above. Indeed, the early exchange of some documents may solve a dispute before a formal dispute resolution process is engaged.

In many cases, the momentum of the dispute resolution will be in the claimant's favour, as the court or tribunal will presume (whether explicitly or not) that the claimant should have the opportunity to extract information from the defendant to investigate and/or prove its case. This is particularly true in the case of fraud, where the claimant may seek early disclosure through a pre-action disclosure process against the likely defendant or a third party, or even by way of disclosure ordered through an injunction.

Parties subject to disclosure obligations must ensure that their disclosure of personal data and particularly data falling within "special categories of personal data" (such as health data or data relating to religious beliefs, for example) is disclosed in a lawful manner. What does this mean? The disclosure of personal data to a third party is a form of processing of personal data that is captured by all data protection laws, and certainly by the New Data Protection Law in the DIFC and the 2015 Data Protection Regulations in the ADGM ('ADGM Regulations'). So disclosure of personal data in a dispute resolution process is caught and regulated by data protection laws.

Under the New Data Protection Law, the processing of special categories of personal data is unlawful

unless it is done in accordance with the general principles of personal data processing (Article 9), on a lawful basis under Article 10, and because a special reason under Article 11 applies. Article 11(f) expressly permits processing "necessary for the establishment, exercise or defence of legal claims (including, without limitation, arbitration and other structured and commonly recognised alternative dispute resolution procedures, such as mediation) or is performed by the [DIFC] Court acting in its judicial capacity". A similar provision exists at Article 3(1)(e) to the ADGM Regulations, which refers only to processing "necessary for the establishment, exercise or defence of legal claims".The New Data Protection Law begs a question: what is a "structured and commonly recognised" form of ADR? Some dispute resolution processes would manifestly fall within this definition, such as DIFC Courts litigation in the Court of First Instance, Court of Appeal or Small Claim Tribunal, as would arbitration under the DIAC or DIFC-LCIA Rules, for instance. But is an ad hoc negotiation a "structured and commonly recognised" process?

Unsurprisingly, the parameters of this exception have not been tested. But this puts parties in a quandary. On the one hand, they may wish to adopt a 'cards on the table' approach from the outset, disclosing documents as soon as possible in a bid to early dispute resolution. The DIFC Courts' Rules have no formal pre-action process (unlike the English Civil Procedure Rules), and this too raises the question of whether the exchange of documents (constituting the processing of special categories of personal data) falls under the protection of Article 11(f) when the parties make such disclosure with the intention or expectation that a party will engage in a structured and common recognised form of dispute resolution but has not yet done so. There are a number of steps parties can take if they are unsure of the lawfulness of their disclosure from a data protection law compliance perspective.

Firstly, parties may seek specific consent from people whose personal data will be disclosed. This may be appropriate and practical under certain limited circumstances. For instance, an employer may write to a former employee to seek consent for the limited disclosure of information in a dispute between the employer and a third party. However, the person whose consent is solicited may refuse to give it, and there will be logistical difficulties over the time taken and costs incurred to obtain consent, along with the potential that the consent may be withdrawn at some stage.

Secondly, redaction. Parties can redact personal data from documents by either taking a black marker to documents and neatly scoring out information, or (far preferably) using software to the same effect on screen. Some parties in disputes take this approach more fastidiously than others, e.g. by redacting all personal data relating to people not related to the dispute, for example where a bank is in a dispute with a client and the bank has processed the claimant's information in the same database as it has for third party clients. Agreement to make redactions should always be sought from the party to whom disclosure is to be made, and if such assent is not forthcoming, an application should be made in good time to the DIFC Court or tribunal for permission. It is invariably better to disclose redacted materials within time and to retrospectively secure assent or permission than to delay the whole disclosure process, and it is never a good idea to disclose unredacted materials and then to seek permission to redact the same documents.

Thirdly, a confidentiality club. Such clubs are agreements to restrict access to documents to certain entities, such as the parties' lawyers and their experts, but not the parties themselves. They are used most commonly when documents are disclosed which have confidential information in them, e.g. commercially sensitive information that may be taken advantage of by the opposing side. A confidentiality club can be used to restrict the dissemination of information and may tip the balance when providing the adequate safeguards for the processing of personal data as the data protection law requires. The existence of a club on its own and without any other legal measure would likely not provide a sufficient basis for processing and/or disclosure of information, but if the arrangement were to be approved by a Court order, then the Article 11(f) grounds may be established.

Finally, there are the legal concepts of privilege and 'without prejudice' communications. If parties have a genuine fear that the documents they are obliged to disclose may lead to liability under an applicable data protection regime, parties should consider whether they can claim privilege over the documents that are being sought. Privilege does not extend to documents merely because they contain personal data or

special categories of personal data, of course, but it is certainly worthwhile bearing privilege in mind. Alternatively, parties may also consider avoiding the possibility of documents ever being subject to publication by exchanging those documents through the mechanism of 'without prejudice' communications, in which the parties agree to open up a corridor for communications where neither the existence of the corridor nor the subject matter of the communications ever goes before a Court or tribunal. Because such communications could only be genuine attempts to negotiate or settle a dispute, they are arguably protected also by the grounds at Article 11(f) in the case of special data, or under Articles 33(3)(b) and 35(3)(b), which go to the ability to resist DSARs where personal data is needed for the establishment, exercise or defence of legal claims, and/or Article 35(3)(d), which allows the processing of data and resisting DSARs for a 'substantial public interest', which includes the administration of justice and the exercise of a function conferred by an applicable law.

Conclusion

Just as the Previous Data Protection Law was replaced with the New Data Protection Law in the DIFC, the ADGM Regulations are expected to be replaced in the near future with new regulations to make the ADGM's legal regime akin to the EU General Data Protection Regulations. Given the multiplicity of forms of dispute resolution in the region, it is conceivable that the interaction between the ADGM and DIFC data protection regulations and dispute resolution processes will be examined by a Court, and that further authoritative guidance may be provided to data protection and disputes lawyers.

For further information, please contact Peter Smith (p.smith@tamimi.com) orMartin Hayward (m.hayward@tamimi.com).