WERKSMANS
ATTORNEYS

REGULATORY

When the dispute relates to personal information – the discovery vault

7 November 2018 *7 min read*

by Ahmore Burger-Smidt, Head of Data Privacy Practice

A number of articles have been written and comments made in the media in relation to hundreds of Discovery Life's clients who had their personal information such as names, identity numbers and contact details disclosed in court papers. However, Discovery Life has moved swiftly to seal the document to contain a possible fallout.

The information was furnished as a supporting document to a court challenge that Discovery Life initiated against one of its former financial advisers who has left Discovery Life to join an independent brokerage. While insurers sometimes allow advisers to move their client books with them, Discovery Life stated that its clients' information had been taken without its permission and therefore it had to provide the data in question to the court to prove that theft of client information had taken place.

Discovery Life filed an urgent application in the Johannesburg High Court on 10 September 2018, asking the court to prohibit their former employee, De Meyer from "*contacting, enticing or soliciting away*" any of the clients listed in five annexures accompanying its notice of motion. The annexures list the names, identity numbers, landline and mobile numbers as well as e-mail addresses of the clients in question and effectively puts the information in the public domain. Court documents are in principle public documents and can be accessed by the public. In the urgent application, Discovery stated –

"*For this reason alone, we initiated urgent legal proceedings to protect the information he had stolen. Discovery applied to the Johannesburg High Court to interdict Mr Meyer [sic] from using any of this information and to ensure its return. Discovery is taking all reasonable and necessary steps to have this information returned, and to prevent its misuse in respect of the employment contract with Mr Meyer [sic], which is designed specifically for the protection of our clients.*"

"*To this end, as an additional precaution Discovery requested the Judge to seal the court papers – and it is now in the process of being sealed.*"

The Protection of Personal Information Act ("**POPIA**")[1] provides in section 11 that personal information may be processed where the processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

But what constitutes the "legitimate interest of the responsible party" in the current instance of Discovery Life?

In light of the fact that there is no existing jurisprudence to rely on from a South African perspective, it is submitted that one should consider the European legislation and experience for guidance.

LEGITIMATE INTEREST

Article 6(1)(f) of the GDPR[2] provides that personal data processing will be lawful for the purposes of the First Data Protection Principle where –

Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The 'legitimate interests' condition is somewhat ambiguous and controversial. The starting point here is the existence of a legitimate interest of the controller. There is no definition of "legitimate" in the GDPR. Recital 47 states that a legitimate interest could exist, for example, where the data subject is a client or in the service of a controller, and also acknowledges that the processing of personal data for direct marketing purposes may be regarded and carried out for a legitimate interest. This makes clear that business purposes, such as customer care or marketing, and staff purposes, such as wellbeing, can be legitimate interests. However, reliance on business purposes would justify more limited types of processing than a stronger interest, such as staff wellbeing.

The processing must be necessary for that legitimate interest, i.e. the interest that the disclosing may have in the processing, and this interest must be pursued by Discovery Life and requires that the interest must constitute a real and present interest. Also, to be considered legitimate, a purpose must be acceptable under any applicable law.

The GDPR, however, also states that the existence of a legitimate interest would need careful assessment, including whether a data subject i.e. a Discovery Life client, can reasonably expect at the time and in the context of the collection of the personal data that the processing for that purpose, in the current instance, High Court litigation by Discovery Life to interdict a previous employee from using the information, may take place.

It is acceptable in the European Union that the notion of legitimate interests could very well include a broad range of interests and that these interests should be balanced against the fundamental rights of the data subject.

The Recitals of the GDPR provide some non-exhaustive examples of situations in which legitimate interests could exist. These would include processing for the purpose of preventing fraud, ensuring network and information security, including preventing unauthorised access and enforcement of legal claims.

Also, the legitimate interests must not be overridden by the interests or fundamental rights and freedoms of the data subject, and a proportionality assessment is thus brought into play in which the legitimate interests of the controller or third party are to be weighed against the rights, freedoms and legitimate interests of the relevant individual whose data are being processed, in order to assess if the latter override the former.

The Court of Justice of the European Union ("CJEU") has considered the legitimate Interests processing condition, although its judgment was not particularly illuminating. In the case of *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas Pašvaldības SIA 'Rīgas satiksme'* (Case C-13/16), the CJEU held that *"there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest"*. In relation to *"balancing the opposing rights and interests at issue"*, the CJEU noted that this depended *"on the specific circumstances of the particular case"*.

In general, the following three factors should be considered when applying a balancing test –

1. the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;
2. the impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed; and
3. additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies, increased transparency, general and unconditional right to opt out, and data portability.

It is submitted that when considering civil litigation, the main risk, from a data Protection perspective, is more than likely disclosing irrelevant or unnecessary personal information. This risk can be mitigated by redaction. However, the definition of personal information means that redacting someone's name is unlikely, of itself, to be sufficient to remove all personal information from any given document. It depends of the document. Redaction has a place but it is neither a wholesale solution nor required in every instance.

The question to be considered in the current instance specifically relates to whether it was in the legitimate interest of Discovery Life to have processed the personal information and how should they have dealt with the security of the personal information.

It is submitted that Discovery Life can indeed put a case forward that it was in their legitimate interest to process the specific personal information. Whether they safeguarded the information appropriately, taking into consideration the timeline, could possibly be questioned.

Redaction of the personal information that formed part of the pleadings, would have rendered the above a mute debate.

[1] Act 4 of 2013.

[2] General Data Protection Regulations (EU) 2016/679.



Ahmore Burger-Smidt

Head of Regulatory

View Profile