Personal data regulation: New litigation frontiers

Jonathan Burns and Saeed Khunaizi of ZH Partners and Ellen Ray of Hourani & Partners discuss what businesses in KSA need to know with regard to personal data access rights under the new PDPL.

"Discovery" is the process by which parties involved in a legal dispute exchange information and evidence pertinent to their case. Although judicial intervention is available, discovery aims to be a voluntary and cooperative process between attorneys. While the concept of discovery exists in civil code legal systems, originating from continental European traditions, it is most commonly associated with common law legal systems, which derive from the British legal tradition.

For instance, in civil disputes under US federal jurisdiction, the Federal Rules of Civil Procedure predominantly dictate the discovery process. This process can encompass various tools, such as interrogatories (written questions that the opposing party must answer under oath), requests for admission (requiring the opposing party to confirm or deny specific facts), witness depositions and mental and physical examinations, and requests for the production of documents.

The overarching goal of discovery is to ensure that all parties have access to relevant facts and evidence, thereby promoting a fair, transparent, and efficient legal process. Pre-trial ascertainment of factual stipulations enhances trial efficiency by sparing the court's time and resources on litigating peripheral facts, and promotes amicable settlement of disputes by allowing the litigants to make an initial assessment on the strengths and weaknesses of their claims and defenses based on the evidence discovered.

Comparative law specialists largely concur that historical colonising powers have propagated three principal legal systems worldwide: the British common law tradition, the continental European civil code tradition, and the Islamic law (*Shari'a*) tradition, the latter being prevalent in The Kingdom of Saudi Arabia (**KSA**). Historically, neither *Shari'ah* in general nor KSA's legal system specifically has incorporated a formal legal discovery process, aligning more closely with the continental European civil code tradition in this regard.

KSA courts always had broad judicial powers, including to order discovery of evidence. Under the relatively new Law of Evidence (2021), KSA courts have been granted the express authority to do so. Even so, KSA courts rarely exercise this authority. Consequently, most evidentiary matters in KSA are addressed in real-time during trial, rather than through a voluntary or cooperative pre-trial exchange of evidence.

In practice, a disputant in KSA must substantiate its case solely with the evidence it possesses, or which is in the public domain, without expecting any cooperative or voluntary disclosure from the opposing party. However, the new Personal Data Protection Law (**PDPL**) and its implementing regulations (**IRs**) (together, the **Law**) is set to change this paradigm, which may mark the beginning of a new litigation frontier in KSA and larger shift towards British and European legal systems. Employers and companies doing business in KSA should prepare for these changes when the Law's grace period ends in September 2024.

OVERVIEW OF THE LAW

The recent enactment of the Law marks a significant shift towards modernising the handling and protection of personal data (**PD**) and reflects a growing recognition of privacy rights and data security. The Law sets out guidelines for data controllers

(**Controllers**) and processors on how PD should be handled, stored, and transferred. By establishing such standards for data management, the Law aims to safeguard individual privacy and integrate PD protection principles into the fabric of legal, HR, commercial, and other practices.

In addition to the foregoing, the Law introduces fundamental rights of the data subject (**DS**), which includes the DS's right of access to PD.

This development is particularly relevant to companies doing business in The KSA who have HR departments, manage employees, and deal with personal customers, suppliers, and other individuals, as litigation procedures in KSA may require them to cooperate with "pre-discovery" procedures relating to DS access rights to PD under the Law.

As a result, it is of paramount importance that companies doing business in the KSA review their current procedures and prepare for these upcoming changes when the Law's grace period ends in September 2024.

THE RIGHT OF ACCESS

In the context of legal proceedings, the right of access to PD could serve as a crucial mechanism for evidence gathering. This is particularly pertinent in cases where PD forms a central element of the dispute, such as breach of privacy, defamation, or contractual issues where PD is relevant to the evidence in question.

Although the DS's right of access to PD is not limited to a specific context, it is likely that a significant amount of access requests will be served upon employers in the context of employment disputes. For instance, where an employee alleges unlawful dismissal, access to the personnel file could reveal important information, such as performance evaluations, disciplinary files, and internal records

> "Given that the Law is still in a grace period, it remains to be seen whether the Saudi Data and Artificial Intelligence Authority (SDAIA) will be an aggressive regulator interpreting nuances in favour of access."

referencing the employee, which could be crucial in supporting the case.

However, while the Law grants access rights, it also recognises the competing interest in protecting sensitive information and the rights of others. This creates a balancing act for Controllers, where they are expected to navigate the legal obligation to provide access while safeguarding other confidential information. It might involve redacting sensitive portions of documents that achieve the same objective without compromising privacy. The specific implementation of these limitations will likely be shaped by future regulatory guidance.

Receiving access requests

The Law does not currently detail what does and does not qualify as a valid access request. Until further regulatory guidance is issued, this lack of clarity places an additional burden on Controllers to have vigilant monitoring systems in place to ensure all communications having the potential of a valid access request are properly received and processed. Given that the Law is still in a grace period, it remains to be seen whether the Saudi Data and Artificial Intelligence Authority (**SDAIA**) will be an aggressive regulator interpreting nuances in favour of access.

Responding to access requests

In any event, a valid access request crystallises an obligation upon the Controller to verify the requester's identity and respond to the access request within a maximum of 60 days. The response may be an acceptance and disclosure of the PD requested, a rejection of the request, or a combination of both.

First, the Controller may reject an access request if it is repetitive, manifestly unfounded (e.g., the requester's identity could not be verified vis-à-vis the PD requested), or requires disproportionate effort. However, if so, the Controller still must notify the requester accordingly.

Secondly, if the request is valid and requires granting access to the PD, the Law states that access must be granted in a "readable and clear format".

While there is no extensive regulatory guidance on this matter as yet, the requirement for accessible data to be "readable and clear" suggests that the disclosure should include relevant contextual information. For example, if there is a full paragraph of text, and the DS's PD only appears in one sentence of the paragraph, then, so long as the full paragraph does not contain any other non-disclosable content, the full paragraph (and not just the single sentence containing the PD) should be made accessible to the DS.

Tools and limitations for controllers

Controllers have several tools at their disposal when confronted with a valid request for access to PD that the Controller has an interest in not disclosing. This is typically managed through permanent redaction techniques or software tools.

For instance, access might be denied if it could compromise crime detection efforts, hinder effective criminal procedures, or adversely affect intellectual property rights.

Another exception repeated frequently in the Law (indicating the degree of regulatory importance) is that access rights do not prejudice the privacy rights of others. This means that, in providing the requester access to the requester's own PD,

the Controller cannot, at the same time, disclose the PD of another person. This is important because SDAIA established in one of the first pieces of regulatory guidance issued (*Guide to the Saudi Personal Data Protection Law: For Controllers & Processors; v1.0, Dec. 2023*) that "opinions" and "inferences" can qualify as "personal data" if an individual can be identified therefrom (p. 11).

In the context of litigation where the requester may be simultaneously formulating a legal case to file against the Controller or a related party, the ability to redact "opinions" and "inferences" of third parties within the organisation (such as line managers and HR staff) on the basis that the information qualifies as PD could offer an additional layer of protection to the Controller and legal basis to withhold potentially crucial evidence from disclosure to the DS.

Notably, the Law contains neither a robust nor express legal privilege exception for Controllers. The principle of "legal privilege" is that communications between lawyers and their clients are confidential and protected from interception or forced disclosure, even if it involves PD of a third-party DS. Therefore, in the previous example, if the employer (Controller) sought legal advice from legal counsel in relation to the termination of the employee (DS), those communications with the legal counsel, and the PD intertwined therewith, would normally be protected from any disclosure requirement.

Although not expressly stated as an exception to access in the Law, IRs Art. 5 cross-references to PDPL Art. 16 which, in turn, vaguely states that "Disclosure" of PD is forbidden where it would violate professional obligations (subparagraph 7) or a "procedure" (subparagraph 8). Arguably, these provisions could be cited by the Controller as a basis for withholding access to certain PD in the context of legal privilege when a request is made.

In alignment with Saudi Arabia's Vision 2030 objectives to align legal standards with international norms, additional regulatory guidance on the above-mentioned exceptions and other exceptions is anticipated in the future.

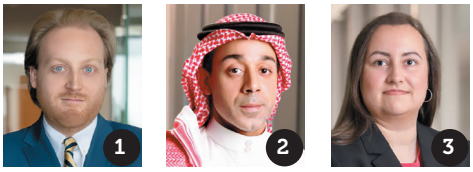
PENALTIES

Penalties under the Law are both general and specific. Where a DS is unsatisfied with the response (or lack thereof) of the Controller following a duly served access request, the first step is to lodge a complaint with SDAIA within 90 days. Then, SDAIA can decide whether or not to investigate and, if SDAIA finds that the Controller violated the law, SDAIA can apply penalties ranging from a mere warning to a fine of up to SAR5 million.

CONCLUSION

In conclusion, "discovery" has historically been a rare occurrence in KSA, and only available by judicial order. But new PD access rights under the new PDPL and IRs introduce a new form of "pre-discovery" available to individuals. This introduces new obligations and risks upon companies and employers doing business in The KSA and a basis on which they must review their current data management practices in preparation for the end of the Law's grace period in September 2024.

The authors would like to thank Anas Akel, partner (Jeddah), for contributing valuable and scholarly insight into this article.



Text by:
1. JONATHAN BURNS, *senior associate, ZH Partners*
2. SAEED KHUNAIZI, *associate, ZH Partners*
3. ELLEN RAY, *associate, Hourani & Partners*