TAUIL | CHEQUER
MAYER | BROWN

BRAZIL'S PERSONAL DATA PROTECTION FRAMEWORK IN THE OIL AND GAS SECTOR

TAUIL | CHEQUER

MAYER | BROWN

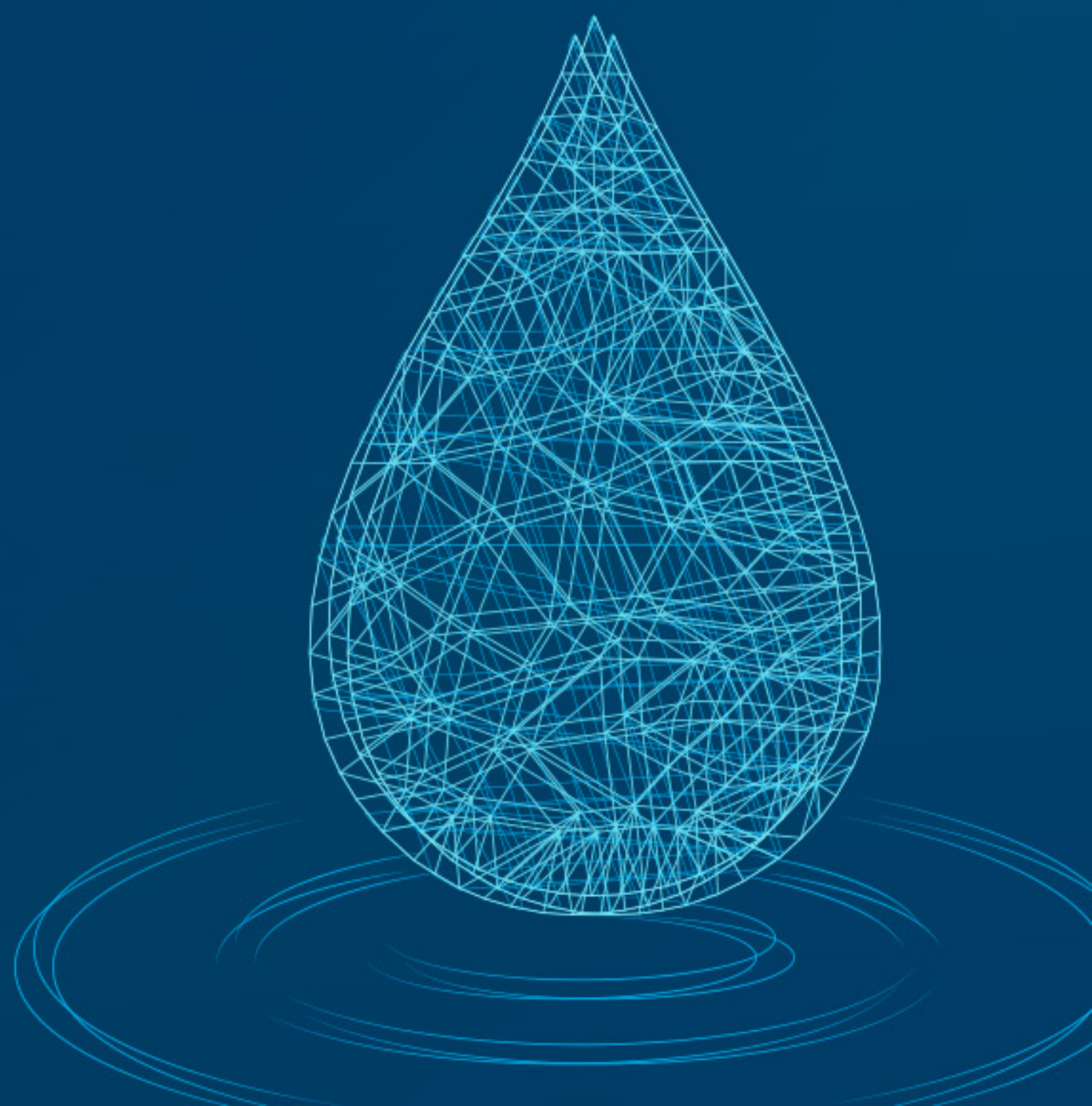
Law 13.709 of 2018, known as the **General Personal Data Protection Law (LGPD), has been fully applicable** since August 2021 and provides guidelines for the correct processing of personal data in all sectors.

The sectors may present different demands due to several factors, such as business model; sectorial rules; competent authorities; risks related to personal data processing activities, such as data volume and the use of artificial intelligence; and the best practices of the stakeholders involved in the sector and related to the companies' activities.

TAUIL | CHEQUER
MAYER | BROWN

Regarding the **oil and gas** sector, it encompasses several activities, from refining to offshore oil extraction, carried out by both public institutions and private companies.

It is also a highly regulated sector, with many actors, resulting in a very specific framework.



TAUIL | CHEQUER
MAYER | BROWN

Although the sector has specific regulations, coming from the National Petroleum Agency (ANP), to date, t**he ANP has not issued rules specifically on the protection of personal data**. So far, the agency has left the regulation of this matter exclusively to the National Data Protection Authority (ANPD). However, the LGPD does not prevent, in the future, cooperation between ANPD and the agency responsible for the sector.

It is also important to note that the Securities and Exchange Commission (CVM) has specific rules on the reporting of information security incidents that must also be considered by companies in the sector subject to CVM regulation.

TAUIL | CHEQUER
MAYER | BROWN

In view of the sector's activities, which are essentially of a B2B nature, the main point of concern turns out to be the collection and processing of data from employees, outsourced workers and suppliers.

Oil and gas companies, for example, are subject to a series of specific regulations, arising from the Regulatory Norms of the Ministry of Labor and Social Security, in particular, Regulatory Norm (NR-37) on safety and health on oil platforms, that require the companies to perform a series of personal data processing operations.

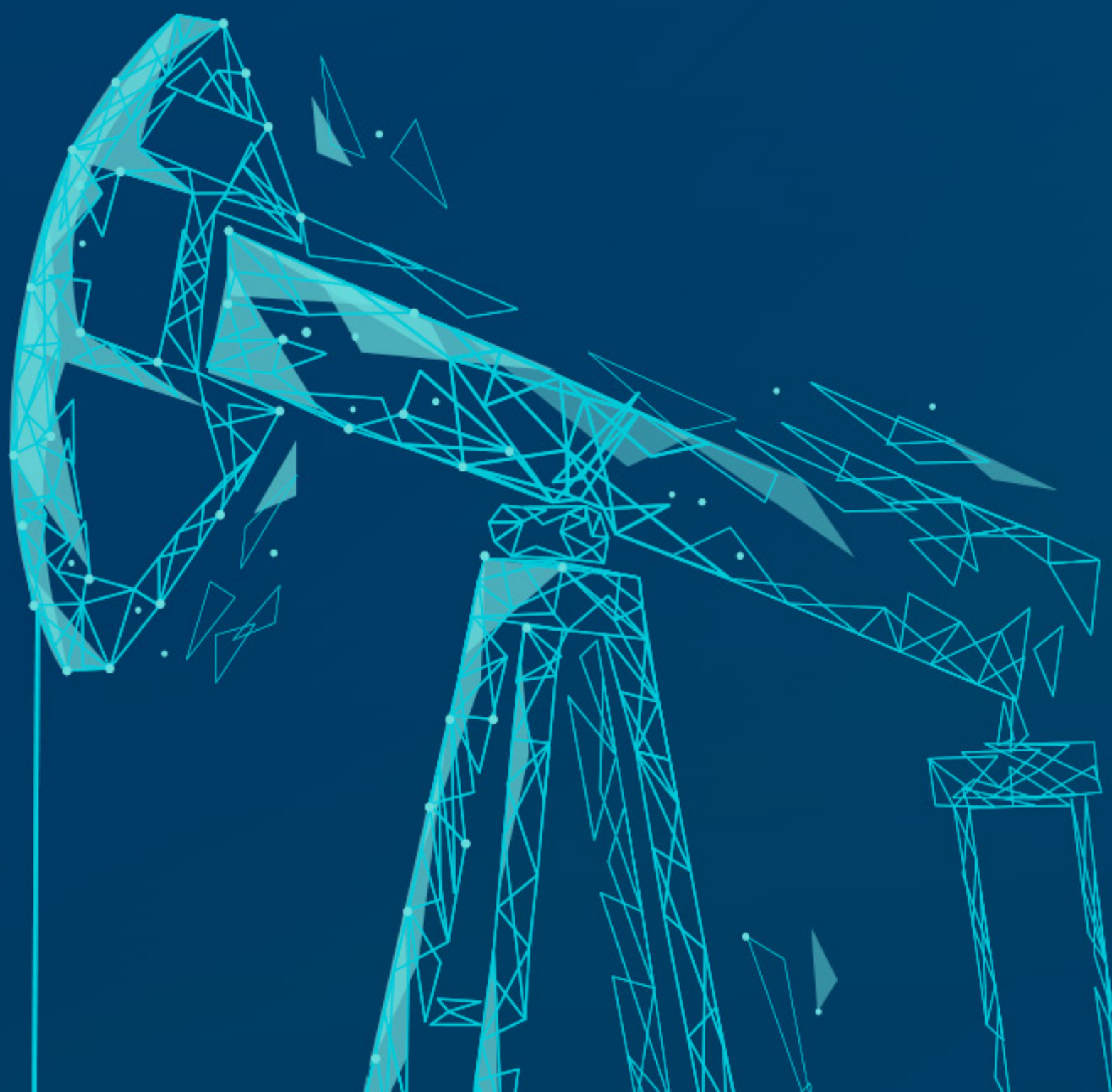
NR-37 and others—such as NR-33 on safety in work in confined spaces, NR-30 on waterway work for off-shore operations and NR-29 on port work for on-shore operations—require a series of sensitive data collections to ensure the health of employees, contractors and suppliers, as well as to maintain a healthy work environment.

Due to these regulatory standards, it is worth noting that the Ministry of Labor and Social Security is responsible for carrying out audits, as provided for in Decree No. 4,552 of 2002. An interesting question then arises: **Would there be concurrent competence of the Ministry of Labor and Social Security and the ANPD, from the perspective of the correct treatment of health data, for example?**

TAUIL | CHEQUER

MAYER | BROWN

In the oil and gas sector, given that the main concern in light of personal data protection falls on the personal data of employees, contractors and suppliers, the following challenges arise for companies in this segment:



TAUIL | CHEQUER

MAYER | BROWN

1

Large-scale handling of sensitive data that ends up requiring a very robust and documented infrastructure of controls aimed at information security, with well-defined access management and implemented security incident response plans. An important example is the recent Law No. 14,289 of 2022, which further reinforces the need to preserve secrecy about the condition of people living with HIV infection, chronic hepatitis, leprosy and tuberculosis. These are data capable of causing high discrimination against the user and, therefore, their confidentiality must be high, including limiting their access by internal teams.

2

Tracking individuals is always a controversial issue when it comes to employees, contractors and suppliers. What are the limits of this monitoring? What are the permitted uses for the information obtained from the control mechanisms? On this point, it is worth noting, among other aspects, the purpose of this monitoring, as well as the intrusiveness of this monitoring.

3

Background check for the most diverse purposes and in the different stages of the employment contract, especially during the recruitment phase. Carrying out any assessment in this sense is delicate and requires a specific understanding of each situation that arises, verifying holders, relevant data, volume, sources, purposes of checking, level of transparency, feasibility of possible oppositions, among other aspects.

TAUIL | CHEQUER
MAYER | BROWN

4 **Indiscriminate use of health checks among different categories of employees** Parameterizing, by the most conservative norm—the testing of all individuals who work for a particular company, especially in a scenario where there are employees on board the ship off-shore and others who work only in offices, many of them working from home—can be a delicate practice and should be handled with great caution in light of the needs of each company. In general, treating more data than necessary goes against LGPD guidelines.

5 **Creating a uniform data protection culture** across functions that are so different and with peculiarities that need to be taken into account. A strong culture on data protection to be developed by companies in the oil and gas sector must reach all employees. It is crucial, therefore, that this culture encompasses the entire manufacturing sector, including employees who work offshore, although they do not always have access to a company's internal awareness practices (via intranet, emails, campaigns, etc.), primarily adopted during in-office activities.

6 **Compliance with various regulations for the protection of personal data and privacy around the world**, given that a good number of companies in the sector have international operations or are linked to foreign headquarters. Therefore, policies and practices must respect local standards, without impeding a cross-border flow of personal data and a global integration of activities.

TAUIL | CHEQUER
MAYER | BROWN

Although most companies in the sector are dedicated to B2B activities, some companies also operate **in the direct-to-consumer distribution sector – B2C**, especially automotive fuels. In this scenario, the regulatory and legislative range, as well as the authorities responsible for inspection and sanctioning, expands significantly. The risk certainly increases as, for example, the Consumer Protection Code (CDC) becomes applicable to the relationship with the holders, which brings the possibility of action by consumer protection bodies, such as Procons and Senacon, which have even been very active in enforcing the LGPD guidelines.

TAUIL | CHEQUER

MAYER | BROWN

Another major source of obligations related to the protection of personal data, and which inevitably impact the framework applicable to companies in the oil and gas sector, are the contracts signed by them with the most diverse commercial partners. In general, with the increasing maturity of Brazilian companies in the field of personal data protection, many require submission to specific agreements and/or clauses on the matter, which, in turn, impose audit rights, notification and collaboration obligations, in addition to commitments aimed at the accountability of the parties involved. It is important, however, that the requirements made are consistent with the legal and regulatory framework to which the company is subject.

TAUIL | CHEQUER

MAYER | BROWN