White Label Consultancy

White Paper

THE ROLE OF THE DPO IN GCC COUNTRIES

October 2023

Table of contents

1. Introduction

The role of the Data Protection Officer (DPO) has become a global profession. Although the practice of appointing a DPO previously existed in several countries around the globe, recently there have been major developments in Gulf Cooperation Council (GCC) countries.

For instance, the Federal Decree Law No. 45/2021 on the Protection of Personal Data made it a requirement in the UAE for public authorities and most companies processing personal data that meet certain criteria. The Executive Regulations, which were published in March 2022, provide more guidelines on the role of the DPO. However, the Law does not apply to public entities or free zones in the UAE with their own data protection legislation, including the Dubai International Financial Centre (DIFC) and Abu Dhabi General Market (ADGM). Similarly, the Saudi Personal Data Protection Law introduced the requirement that controllers must appoint a DPO, subject to the conditions outlined in the Implementing Regulations.

In this white paper, we intend to explain the role of the DPO in GCC countries for leadership, legal, and compliance stakeholders, who are increasingly faced with questions about privacy, including whether they should appoint a DPO.

2. Important concepts

Below there are some important terms that will be mentioned throughout this paper and are important to understand the functioning of this role:

- **Accountability** has become one of the key data protection principles. It means that data controllers are required to take responsibility for the way they process personal data. Accountability also requires organisations to put in place technical and organisational measures and to be able to prove their actions and demonstrate compliance.
- **Data controller** is the person or organization that determines the purposes and means of the processing of personal data. The data controller decides what to do with the data. If two or more data controllers have control over purposes and processes, then they are considered joint controllers.
- **Data processor** is the organisation that processes personal data on behalf of the data controller. They are instructed to process the data.
- **Data subject** is the individual to whom personal data relates.
- **Personal data** is information that relates to an identified or (and this is important) *identifiable* individual. If you can identify an individual directly from the information you are processing, then that information may be considered personal data. But if the individual is still identifiable indirectly, perhaps by combining that data with other data points, then that data can also be deemed personal data.
- **Processing of personal data** covers a wide range of operations which can be both manual and automated. Processing includes any operation which is performed on personal data. This essentially covers anything you do with data, including collection, storage, use, sharing and even erasure of data.
- **Supervisory authorities** are individual authorities established by countries or states to oversee compliance with a specific data protection regulation or law.

3. The purpose of the DPO

The primary role of the DPO is to ensure the organisation processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules. But what does that mean?

Supervisory authorities understandably focus on compliance. This means they will recognise the role the DPO can play to help an organisation demonstrate compliance with their local data protection regulation. It is important to make sure you are aware of the principle of accountability that has been adopted within your organisation. It requires organisations to take responsibility for the way they process personal data and comply with the other principles. It also emphasises the ability to demonstrate compliance. This is significant because previous iterations of data protection laws revolved more around obtaining permission, or even permits. Accountability puts the onus on the data controller to make decisions based on regulatory guidance, to be accountable for them, and to be able to demonstrate compliance. You can immediately see how the DPO function will play a pivotal role in the delivery of this enhanced focus.

Broadly, the tasks of a DPO can be summarised in the following manner:

- Interpret local and international data protection laws and regulations.
- Help design and then implement data protection best practices.
- Monitor compliance with data protection legislation and your organisation's privacy programme ambitions.
- Represent and advocate for the interests of data subjects inside and outside your organisation.
- Act as a contact point and organisational representative for supervisory authorities and data subjects.

Whether or not a DPO can simultaneously fulfil other tasks and duties beyond data protection has been the subject of much discussion and debate. The answer is yes, but there are caveats that organizations need to consider very carefully. In short, organizations must ensure that any of these other tasks or duties do not result in a conflict of interest. Most legal and compliance stakeholders, and senior business leaders, will be very familiar with the concept of a conflict of interest, and many organizations will have policies and experience which they can leverage. This is likely to be a subjective assessment where organizations also leverage best practice guidance. If no apparent conflict exists today, it may also be also prudent to consider whether any potential conflict of interest is likely to exist in future before making a final decision on who to appoint as DPO, and potentially to whom they should report.

For example, a marketing lead or a CIO may seem a strong potential candidate to be appointed as a DPO because they understand what data is processed and how it is being used. However, both would generally incur in conflict of interest because they are directly involved in the processing of personal data and would likely find themselves at odds with the requirement to be an independent advocate or guardian of data subject matters on an operational level.

4. When a DPO is required?

Many laws recently enacted in GCC countries require organizations, in certain circumstances, to appoint a DPO.

In the following sections the conditions outlined in the relevant data protection laws will be addressed.

a United Arab Emirates (UAE)

Deciding whether your organisation requires a DPO will involve a careful assessment of the Federal Decree Law No 25 of 2021. You might also be processing and/or transferring data to multiple countries. If you are not familiar with some of the guidance and privacy terminology, this may

require that you to seek independent professional advice.

Similar to other legislation around the world, including the GDPR, if your organisation is a data controller or a data processor that meets any of the following criteria you will be required to appoint a DPO, cf. Article 10 of the Federal Decree Law:

- Where your processing activities involve using new technologies or technologies processing high volume of data and as a result there is a high risk to the confidentiality and privacy of the personal data of a data subject.
- In case your processing activities include a systematic and comprehensive evaluation of sensitive personal data, including profiling and automated processing.
- Where you are processing a large scale of Sensitive Personal Data.

The first thing that many decision-makers in the UAE will ask is what is meant by terms such as new technologies, large-scale processing or regular and systematic monitoring? These are important concepts and based on our experience we have attempted to set out below what these 3 terms mean in plain language.

The term **"new technologies"** refers to technologies which involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms (e.g., combining the use of fingerprint and face recognition for improved physical access control).

"Large-scale processing" relates to the amount of data that is processed by the organisation. It has never been clearly defined and no threshold exists that could be globally used. However, the number of individuals whose data is processed, the richness of the data set in question, the geographical extent of the processing operations and the duration of the processing are all factors that should be considered.

The concept of **"regular and systematic monitoring"** includes all forms of tracking and profiling. Monitoring has to do with some form of oversight of an individual's activity and includes both online and offline activities. To be regular and systematic it must not occur ad-hoc but should be planned and occur over time. Examples that are frequently mentioned include data-driven marketing activities, profiling and scoring for purposes of risk assessment, location tracking, behavioural advertising and monitoring of health data using devices like smart watches etc.

b Dubai International Financial Centre (DIFC)

The DIFC's Data Protection Law, Law No. 5 of 2020, requires to appoint DPOs for DIFC Bodies and data controllers or data processors performing high risk processing activities on a systematic or regular basis. A controller or processor could also be instructed by the Commissioner to appoint a DPO.

High risk processing activities include processing that includes the adoption of new or different technologies (such as AI or Blockchain), processing of a considerable amount of personal data, systematic and extensive automated processing and processing of special categories of personal data on a large scale.

This regime allows a single appointed DPO for a company group, even if that DPO is located outside the DIFC. Beyond that, the DPO must be a UAE resident, and can be outsourced, and an internal DPO may hold other roles.

In September 2023, the DIFC enacted the Regulation on Processing Personal Data Through Autonomous Systems. This regulation requires the appointment of an "Autonomous Systems Officer (ASO)" where deployers or operators use, operate, provide or make commercially available an autonomous system or semi-autonomous system to engage in high risk processing activities. The

Autonomous Systems Officer will have the same or substantially similar competencies, status, role and tasks of a DPO. This means that appointing a DPO could also be a beneficial choice when developing or using autonomous or semi-autonomous systems.

c Abu Dhabi Global Market (ADGM)

Another example of a data protection regulation which includes a DPO function is the ADGM's Data Protection Regulations 2021. The ADGM requires the designation of a DPO by a data controller and data processor in the same circumstances referred to by the GDPR.

However, although the GDPR is being closely followed as a best practice, there are some innovative variations. The ADGM is seeking to enhance data protection in their jurisdiction but also aims to support the development of a thriving technology hub and fintech community. Recognising the burden on start-ups and small enterprises, which are a key component of Abu Dhabi's business landscape, the ADGM has included an exception to the DPO obligations for organisations with fewer than 5 employees in ADGM - provided they do not perform high risk processing activities.

That being said, indications are that all companies -regardless of their size– should map their data processing activities and identify any possible high risk data processing activities. If this assessment shows that any of their processing activities are high risk, a DPO must be appointed.

d The Kingdom of Saudi Arabia

The Kingdom of Saudi Arabia has also enacted some laws regulating the requirements for the DPO.

The KSA's Personal Data Protection Law ("PDPL"), which was first published on September 24, 2021 in accordance with the Royal Decree M/19 of 9(2/1443H, is considered the country's first comprehensive national data protection law.

In March 2023, certain amendments were made to Saudi Data Protection Law. Those amendments were recently implemented through Royal Decree No. M147 of 5/9/1444H.

The PDPL has been published in the KSA Official Gazette and it entered into force on September 14, 2023. However, even though the law has entered into force, data controllers have a one-year grace period in order to comply with the PDPL (i.e., up until September 14, 2024).

The data protection law of the Kingdom of Saudi Arabia (KSA) has many similarities with the data protection laws of the UAE states. However, there are still some differentiating aspects. In accordance with KSA PDPL Implementing Regulations, Article 32, a DPO needs to be appointed in the following circumstances:

- Public entities that provide services involving the processing of personal data on a large scale.
- Organizations whose primary activities consist of processing operations that require regular and continuous monitoring of individuals on a large scale.
- Core activities of the organization consist of processing Sensitive Personal Data.

Among the responsibilities of the DPO, the Implementing Regulations establish that the DPO must monitor and update the records of personal data processing activities of the controller (Art. 32(3)(f) PDPL Implementing Regulations).

Another aspect to consider is that the regulations require only the controllers to appoint a DPO. This means that processors are, in principle, not required to appoint a DPO even if the processing activities fall within the circumstances previously mentioned.

The Competent Authority will issue rules for the appointment of the DPO and the circumstances or concrete cases under which a DPO will be appointed.

e The Kingdom of Bahrain

The Kingdom of Bahrain is one of the GCC states, that differentiates from the other data protection laws when it comes to the role of the DPO. Bahrain's Data Personal Data Protection Law No. (30) of 2018, does not mention "Data Protection Officer" or "DPO". Instead, Bahrain's data protection law introduces the "Data Protection Guardian". As will be seen below, the Data Protection Guardian has similar responsibilities, positions and roles to the DPO.

Article 10 of Bahrain's Personal Data Protection Law outlines the main duties and responsibilities of the Data Protection Guardians. The tasks of the data protection guardians are:

- Assist the controller in adhering to its duties as prescribed in the law.
- Act as an intermediary between the controller and data protection authority about certain data controller's obligations on data processing.
- Ensure that the controller is processing personal data in compliance with the data protection laws and, should there be any infringements, the Data Protection Guardian must bring them to the attention of the controller to eliminate those violations.
- Notifying competent authority when new evidence arises indicating that the controller has not eliminated violations after ten days from the moment Data Protection Guardian notified the controller of the infringement.
- Maintain the data processing register, which the data controller must notify to the competent authority.

Data Protection Guardians must be registered in the national register for one year, which may be renewed for similar periods (Art. 14 Order No. 46 of 2022, Regarding Data Protection Guardians).

It is important to note that the competent authority may issue a decision which requires certain categories of data controllers to appoint a DPO. This is in particular where the authority considers that the controller's type of work, the nature of the activity, the volume of processing that takes place, or the manner of processing personal data requires additional monitoring.

f The Sultanate of Oman

The Oman Personal Data Protection Law (PDPL) came into effect in February 2023 and it establishes new legal requirements for organizations processing personal data.

Similarly to other data protection laws, Oman's Personal Data Protection Law sets forth an obligation on controllers to appoint a DPO. The process of appointing a DPO must follow the selection controls and the criteria, which will be provided in the Executive Regulations of Oman's data protection law. Non-compliance with controls and selection criteria can result in a OMR 1,000 to OMR 5,000 fine.

g Qatar

Qatar enacted in 2016 Law No. 13, Concerning Personal Data Privacy Protection Law (the "PDPPL"). This law applies to the processing of personal data within the territory of Qatar, except for the Qatar Financial Centre (QFC) free zone. Controllers or processors incorporated or registered in the QFC must follow the QFC Data Protection Regulations.

Neither do the Qatari Law No. 13 of 2016, Concerning Personal Data Privacy Protection, nor the QFC Data Protection Regulations expressly require controllers or processors to appoint a DPO. However, the guidelines on Data Protection Impact Assessments state that the DPIA should be conducted by a person/s with a sufficient understanding of the PDPPL requirements and data protection concepts and practices, and this will often be provided by a data protection officer.

This implies that even if there is no express obligation, the appointment of a DPO is highly recommended in cases where the processing activities entail high risks for individuals.

h Kuwait

In 2021 Kuwait's Communication and Information Technology Regulatory Authority (CITRA) issued the Data Privacy Protection Regulation ("DPPR"). The DPPR establishes regulatory obligations on Communications and Information Technology Service Providers and organizations that collect and process personal data through various means, such as websites, applications, etc.

Kuwait's DPPR does not explicitly require companies to appoint a DPO. There are also no specific provisions about data protection officers. However, in case there is a data breach, the company must provide Kuwait's Communication and Information Technology Regulatory Authority with all the communications with the data protection officer and the records of processing activities must include, if appointed, the name and contact details of the DPO.

5. Selection of the DPO

The role of the DPO is challenging. It is likely to be even more so in countries and/or organisations where the data protection/privacy regime, or DPO role, is new, such as in the UAE or KSA. Senior leadership support and participation will need to be established, cultural change will be required, and new processes, policies and accountabilities will need to be introduced. This may cause a certain degree of disruption and result in organisational pushback. Consider a scenario where an internal test and development team has historically been using the personal data of customers to train a machine learning algorithm without the consent (for that purpose) of the data subject, or a marketing team passing data to a processor for analytical purposes, but without a valid legal basis. The DPO would need to address these prohibited data processing scenarios, which ultimately can have business implications as well as consequences for business process owners who have been using personal data differently in the past.

It is also worth emphasising that a DPO is not appointed to take accountability or to perform all operational duties related to the processing of personal data, but rather to guide and support the various data process owners across the organisation who are now accountable, and then to independently monitor compliance with legal obligations and internal policies.

a Qualifications of the DPO

The GCC countries' data protection laws in general require that the DPO have sufficient skills and know-how about personal data protection. It is therefore necessary that you appoint a DPO based on their professional qualities, experience, and expert knowledge of data protection law, not because they happen to have some bandwidth available as an existing employee.

The DPO's experience should generally be proportionate to the type of processing that your organisation is carrying out, considering the sensitivity, complexity and amount of data. For

example, your risk would typically be elevated if your organisation systematically transfers data beyond the national borders, particularly if you are established in, or sharing data with processors, in multiple jurisdictions. By default, a DPO should therefore have expertise in national and international data protection laws and practices.

It is also extremely important to look beyond professional qualities and expert knowledge to assess an ability to fulfil the tasks expected of a DPO from a personal perspective. As noted above, the DPO is not only playing a second line compliance function, he or she also needs to integrate closely with the business and other compliance and legal stakeholders to ensure that the organisation is able to deliver on the objective of privacy by design. This is a demanding role because the DPO will need to evangelise and advocate for privacy, work with and train colleagues, have an ability to accurately assess risk and make decisions, report regularly to senior management, and represent the organisation externally with supervisory authorities and data subject requests.

This requires an assessment of their personal qualities, including maturity in relation to integrity and ethics, their knowledge of your industry and the strategic business objectives and strategies, and their position or standing within the organisation. One might argue that they need a certain amount of gravitas inside your organisation. Recognising this, does the candidate you have in mind have the ability to influence stakeholders from across the functional areas of the business? Does he or she have the personality and maturity to collaborate with colleagues in challenging circumstances? Can he or she deal appropriately with disputes while preserving the objectivity and strict independence of the DPO role, including any potential conflicts of interest?

In summary, candidates need data protection expertise and have a clear compliance function, but they also need to be able to garner the support of colleagues and leadership teams and build a reputation as a business enabler. This is particularly true in organisations where the data protection programme is relatively new and undeveloped. The DPO will need to maintain their independence and provide guidance (and ensure compliance) based on the privacy interests of internal and external data subjects.

b The independence of the DPO

Independence is consequently a key element of the DPO role. This dictates that the DPO role demands a senior position, where the leadership team will need to trust and respect the expertise and judgment of the appointed individual, particularly as they should not interfere with the opinion or attempt to influence the position of the DPO. The DPO should not receive any instructions regarding the exercise of his or her tasks and should be able to perform their duties and tasks independently. To ensure autonomy and objectivity, and an ability to represent data subjects effectively, the DPO role is afforded a level of job security. The DPO cannot be dismissed or penalised for performing his or her duties.

The selection of the right individual for the DPO role is therefore critical for the success of any privacy programme. Our experience at White Label Consultancy, based on years of implementing privacy management programs, has identified the following common challenges DPOs are facing:

- Opposition from the rest of the organisation towards privacy work.
- Overwhelming workloads.
- The independence of the DPO being challenged.
- Resistance from senior management to make the necessary changes to address

the various programmatic challenges faced by the DPO.

Lastly, although we would be hard-pressed to exaggerate the importance of the DPO role, it should be mentioned that the DPO is not personally liable for any non-compliance. That accountability will always remain with the data controller. This again underscores why selecting the right individual is critical. For this reason, should you choose not to appoint a DPO, we would recommend that this decision be well-documented and then signed off by a senior leadership team member in your organisation.

c Reporting line of the DPO

Another frequently discussed topic regarding the role of the DPO is the placement and reporting line of the role in the organisation. Different approaches have been taken by various organisations, and little case law exists so far.

The European Data Protection Supervisor (EDPS), does provide some guidance on the placement of the DPO in the organigramme as they highlight several assurances guaranteeing this independence:

- A DPO should not also be a controller of processing activities (for example, if she is head of HR) – as this would allow the DPO to influence the processing activities, that she at the same time is to oversee and monitor,
- A DPO should not be an employee on a short or fixed-term contract, as this could create an incentive to be less critical towards possible infringements of data protection requirements,
- A DPO should not report to a direct superior (rather than top management) as this potentially can make it difficult for the DPO to voice concerns to senior management and it can impede the DPO in focusing on the organisational matters where the need is the highest.
- A DPO should have responsibility for managing her own budget so that the DPO does not have to seek budget approval each time an activity is required.

In addition, the organisation must offer staff resources and budget to support the DPO to carry out her duties. In this respect, DPOs can be supported by an assistant or deputy DPO and can rely on data protection coordinators in each section of the organisation.

For instance, DPOs need to have immediate access to all personal data and data processing operations. Those in charge are also required to provide information in reply to questions from the DPO.

A minimum term of appointment and strict conditions for dismissal must be set out by the organisation for a DPO post. In the EU, for example, the EDPS emphasises that for EU institutions DPOs are appointed for a period.

6. The outsourced DPO

Data protection laws, including in GCC countries, permit organisations to assign the DPO responsibility to an external party. This can be an attractive option for organisations with limited data protection experience. Trying to find a suitable, well-qualified, business-oriented DPO with the location, language, and experience requirements to hire in-house is bound to be very difficult. Consequently, DPO-as-a-Service (DPOaaS) can become a compelling, practical, and cost-effective solution for many organisations.

Many smaller entities will also not require a full-time role making DPOaaS a suitable option.

7. Business impact of the DPO

Leadership teams should be clear that a privacy or data protection programme is not just about compliance, even if that might be a default reaction to another new regulation presented to the Boardroom.

The DPO will not only be responsible for a "tick box" paper governance compliance exercise. In a world where access to data increasingly requires meaningful consent, it is difficult to exaggerate the importance of digital trust for the adoption of new services and how it can nurture an increased willingness by users to share information with a data controller.

Digital trust offers considerable business influence in an increasingly digital economy – from customer loyalty to customer spending. It will connect companies more intimately to their customers, and it will make customers more likely to be loyal to brands that live up to their expectations. Privacy has become a key element of that digital trust equation and customers increasingly expect privacy. Big tech companies made the first steps in this field many years ago, but as more and more companies strive to become data-driven, this focus on digital trust and privacy applies to every business. Business partners and governments, recognizing this, are also expecting organisations to provide adequate privacy safeguards.

Leadership teams should recognize that a strong privacy program will deliver:

- Improved data governance will allow the organisation to obtain enhanced and increasingly relevant insights from the data it holds, allowing the company to offer more relevant and advanced services to customers.
- Strengthened customer-focused business practices relating to the use of data will increase customer trust towards the organisation, build your brand and offer a competitive advantage.
- Improved data management will reduce the risk of unforeseen incidents and the non-compliant use of data, with a subsequent reduction in overall business risk.

The DPO plays a critical role in the success of any privacy programme. The role has taken on an elevated status in the last few years and it is yet to evolve in the regions that update their regulatory data protection frameworks, making the DPO a mandatory role.

But also organizations operating in jurisdictions where the appointment of a DPO is not mandatory, such as Qatar and Kuwait will benefit from appointing a DPO. This is because a DPO:

- Provides dedicated and ongoing support in privacy matters.
- Acts as the point of contact with competent authorities and individuals.
- Provides access to specialist and tailored knowledge.
- Provides valuable insights into best practices and actionable recommendations.

8. Conclusion

As we have set out above, a successful DPO needs to be very carefully selected. The role requires a high level of subject matter expertise, strong leadership team support, the elements of seniority and strong independence, an ability to positively influence and collaborate with colleagues, being comfortable delivering training, good risk management and judgement qualities, while objectively representing the interests of data subjects and interacting externally with supervisory authorities.

An outsourced DPO can become an attractive and effective option for many organisations, either as a designated DPO, or potentially as a back-office function offering your DPO access to expertise or added bandwidth.

9. How can White Label Consultancy Help?

While data protection laws in GCC countries are still to enter into force or entered into force very recently, it is reasonable to expect that the measures to be taken to adjust business practices to the new regulatory regimes will be time-consuming and will demand coordination between all parts of the business.

White Label Consultancy DPOaaS allows you to put your privacy compliance and organisation's reputation into the safe hands of experienced and senior privacy professionals. Being a boutique data protection and privacy consultancy with highly specialised privacy professionals, White Label Consultancy has vast experience implementing privacy management programs across several large multi-nationals, working in both in-house and consultancy roles.

We combine excellent legal proficiency with deep technical knowledge and significant operational experience to offer a made-to-measure, proven, and functional approach to solving the issues that organisations face.

We can assist organisations with their DPO needs and fast track the data protection journey towards the desired level of maturity and compliance.

Each organisation is different, but a DPOaaS offering can be tailored to the needs of the organisation, both in terms of support offered and the time allocated. Based on the individual needs of the organisation, White Label Consultancy can offer:

- An on-demand team of privacy professionals to manage your privacy matters,
- An independent resource with no conflict of interest,
- Obtaining ongoing support for daily privacy tasks and complex projects,
- A data privacy assurance service,
- Drafting and implementing key policies and procedures.
- Training your employees and raising privacy awareness in your organisation.
- Supporting you with data subject access requests and data breaches.
- Acting as your appointed DPO.
- Training and ongoing back-office support for your designated DPO.
- Managing communications with authorities, processors, and data subjects,
- Assisting in the development and maintenance of your record of processing activities.
- Conduct the data privacy annual assessment.
- Updating, maintaining, and implementing compliant privacy policies and procedures.
- Negotiating privacy clauses in contracts with vendors.
- Monitoring ongoing compliance with data protection requirements.
- Assisting the organisation in the performance of data protection impact assessments.

Check the complete version of our DPOaaS offer here

*Please reach out to us at White Label Consultancy here with any questions or using **hello@whitelabelconsultancy.com***

Authors

Nicholai Pfeiffer
Managing Partner
White Label Consultancy
np@whitelabelconsultancy.com

Magdalena Goralczyk
Partner
White Label Consultancy
mg@whitelabelconsultancy.com

Federico Marengo
Senior Consultant
White Label Consultancy
fma@whitelabelconsultancy.com

Norman Aasma
Junior Associate
White Label Consultancy
noa@whitelabelconsultancy.com

White Label
Consultancy