



White Label  
Consultancy



# THE ROLE OF THE DATA PROTECTION OFFICER

May 2021

## Contents

1.	Introduction	3
2.	A few important terms	4
3.	The Purpose of the DPO	5
4.	When is a DPO required?	7
4.1	Mandatory designation	7
	European Union /	
	European Economic Area	7
	Brazil	8
	Egypt	8
	India	8
	Nigeria	9
	South Africa	9
	United Arab Emirates (Dubai International Financial Centre)	9
	United Arab Emirates (Abu Dhabi Global Market)	9
	United Kingdom	10
4.2	Voluntary designation	10
	Australia	10
	Bahrain	11
	Kenya	11
5.	Selection of the DPO	12
5.1	Qualifications of the DPO	12
5.2	Independence of the DPO	13
5.3	Reporting line for the DPO	14
6.	The outsourced DPO	16
7.	Business impact of the DPO	17
8.	Conclusion	18
9.	How can White Label Consultancy Help?	19
10.	Authors	20

## 1. Introduction

**T**he role of the Data Protection Officer (DPO) has arrived as a global profession. Although the practice of appointing a DPO has existed in several European Union countries, GDPR made it commonplace in Europe and now it has been introduced in many other jurisdictions.

In this white paper we intend to explain the role of the DPO to executive-level decisionmakers and legal and compliance stakeholders who are not privacy professionals, but who are increasingly faced with questions about privacy, including whether to appoint a DPO.



## 2. A few important terms

Before we start, here are a few important terms that will be mentioned throughout this paper:

- » **Accountability:** this 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 demonstrate what they did.
- » **Data controller:** this is the person or organisation 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 the control over purposes and processes, then they are considered joint controllers.
- » **Data processor:** this is the organisation who processes personal data on behalf of the data controller. They are instructed to process the data.
- » **Data subject:** the individual to whom personal data relates.
- » **Personal data:** this 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:** 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:** individual authorities established by countries or states to oversee compliance with a specific data protection regulation or law.

### 3. The Purpose of the DPO

According to the European Data Protection Supervisor, 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.”<sup>1</sup> But many non-privacy professionals will quite naturally ask: What does that mean?

Supervisory authorities understandably focus on the theme of compliance. This means they will recognise the role the DPO can play to help an organisation to demonstrate compliance with their local data protection regulation. For a non-privacy professional, it is important to make sure you are aware of the principle (or theme) of accountability that has been introduced by the GDPR, but also widely adopted elsewhere as a key data protection trend. 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, we can summarise what the DPO is tasked with doing in the following manner<sup>2</sup>:

- » Interpret local and international data protections 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,
- » Enable the free flow of data within and between organisations, including across jurisdictional borders,
- » Represent and advocate for the interests of data subjects inside and outside your organisation, and,
- » 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

ACCOUNTABILITY PUTS  
THE ONUS ON THE DATA  
CONTROLLER

<sup>1</sup> [Data Protection Officer \(DPO\) | European Data Protection Supervisor \(europa.eu\)](#)

<sup>2</sup> WLC Blog: [Responsibility of the DPO](#)

has been the subject of much discussion and debate? The answer is yes, but there are caveats that you need to consider very carefully. In short, you 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 of you will have policies and experience which you can leverage. This is likely to be a subjective assessment where you also leverage best practice guidance. If no apparent conflict exists today, it may also be 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 on the face of it seem like strong potential candidate, because they understand data and how it is being used. However, both would generally be

conflicted 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.

YOU MUST ENSURE THAT  
ANY OF THESE OTHER  
TASKS OR DUTIES DO NOT  
RESULT IN A CONFLICT OF  
INTEREST.

SENIOR LEADERSHIP SUPPORT AND PARTICIPATION WILL  
NEED TO BE ESTABLISHED, CULTURAL CHANGE WILL BE RE-  
QUIRED, AND NEW PROCESSES, POLICIES AND ACCOUNT-  
ABILITIES WILL NEED TO BE INTRODUCED.

## 4. When is a DPO required?

### 4.1 Mandatory designation

**D**eciding whether your organisation requires a DPO will involve a careful assessment of your local data protection regulations. 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.

The following examples offer an insight into the evolving global regulatory landscape as it pertains to the DPO role:

#### European Union / European Economic Area

GDPR has taken the concept of the DPO from Germany and introduced it in Europe and now globally. The law has specified both the possibility of a voluntary appointment and the mandatory one.

Foremost, the GDPR<sup>3</sup> connects the mandatory designation to the way the controller or the processor uses personal data. When an organisation's core activity consists of the systematic monitoring of individuals on a large scale, or when the organisation on a large scale processes sensitive data, or data about criminal convictions, they must appoint a DPO. In addition, public authorities, excluding courts, must also ensure that they appoint a DPO.

The first thing that many decision-makers in jurisdictions - where the DPO role is new - will ask is what is meant by terms such as core activities, or 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.

#### Core activities

GDPR introduced a distinction between the processing of personal data that is central ("core") to an organisation's business objectives, and the processing that is ancillary or supporting what is considered core to the business. As such, a core activity of a security company might be the monitoring of locations. The provision of financial advice would be a core activity for a bank. They will however have also ancillary activities, such as people management, or accounting.

#### Large-scale processing

The term "large-scale" 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 universally 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.

#### Regular and systematic monitoring

The concept of "regular and systematic monitor-



ing" is also not specifically defined in the GDPR but has been interpreted to include 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.

## Brazil

The Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais or LGPD<sup>4</sup>) came into force in September 2020 and created a DPO position. Unlike the GDPR, the LGPD requires every data controller processing personal data to appoint a DPO. This is however subject to change based on future guidance by the National Data Protection Authority.

## Egypt

Unlike the GDPR, all data controllers and data processors need to appoint a DPO who must also be an employee of the organisation. Unlike most other jurisdictions, this role cannot be outsourced, which creates challenges, particularly for small businesses. The Law on the Protection of Personal Data (Resolution No. 151 of 2020)<sup>5</sup> lists the requirements that DPOs must comply

with and states that they may be personally liable and punished if non-compliance of the DPO legal requirements is caused by negligence. This includes fines for non-compliance with their statutory obligations.

Executive Regulations are expected in 2021 and will hopefully provide additional information about the registration process and role of DPOs in Egypt.

## India

Under the existing legal framework every corporate entity which is collecting sensitive personal information must appoint what is called a *Grievance Officer* to deal with complaints relating to the processing of personal information. They also need to respond to data subject access and correction requests.

New legislation: Personal Data Protection Bill (PDP) 2019<sup>6</sup> is however currently pending consideration by a Joint Parliamentary Committee. Although not enacted yet, it does contemplate the appointment of a DPO if that entity is deemed a Significant Data Fiduciary (SDF). A data fiduciary is defined as any entity that determines the purpose and means of processing of personal data (and hence a term that relates to the data controller in other jurisdictions), and the PDP indicates that a SDF would involve data processing that is related to significant risk.

4 [LGPD: L13709 \(planalto.gov.br\)](#)

5 [Unofficial bi-lingual translation: Egypt-Data-Protection-Law-English-Arabic.pdf \(sharkawylaw.com\)](#)

6 [4173LS\(Pre\).p65](#)



## Nigeria

The Nigeria Data Protection Regulation<sup>7</sup> read with the National Information Technology Development Agency's (NITDA) Implementation Framework<sup>8</sup> for the Nigeria Data Protection regulation, requires controllers to designate a DPO responsible for ensuring compliance with the Regulations and other applicable data protection directives. A controller may outsource data protection to a verifiably competent firm or person.

## South Africa

The Protection of Personal Information Act 4 of 2013 (POPIA)<sup>9</sup> came into effect on 1 July 2020. DPOs, referred to in POPIA as Information Officers, must be registered with the Information Regulator. The information officer's tasks include ensuring compliance with POPIA, responding to requests for support with investigations by the Information Regulator, and data subject requests made to the controller, a role which is referred to as the Responsible Party in POPIA.

## United Arab Emirates (Dubai International Financial Centre)

The DIFC's Data Protection Law<sup>10</sup> 2020 mandates that DPOs are required 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.

The DIFC permits a single DPO to be appointed for a company group, even if that DPO sits outside the DIFC. Beyond that, the DPO must be a UAE resident, can be outsourced, and an internal DPO can hold other roles.

## United Arab Emirates (Abu Dhabi Global Market)

A very recent 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 above by GDPR.

However, although the GDPR is being closely followed as a best practice, and the ADGM aligns strongly with the ICO<sup>11</sup> in the UK, we are also seeing some innovative variations. The ADGM<sup>12</sup>

7 [NigeriaDataProtectionRegulation.pdf \(nitda.gov.ng\)](#)

8 [Nigeria Data Protection Regulation 2019 Implementation Framework.pdf \(taxtech.com.ng\)](#)

9 [Protection of Personal Information Act \(POPI Act\) - POPIA](#)

10 [Data Protection Law DIFC Law No. 5 of 2020 | Dubai International Financial Centre \(DIFC\)](#)

11 [Information Commissioner's Office](#)

12 [ADGM, Abu Dhabi's International Financial Centre](#)

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 said, indications are that all companies - regardless of their size - should carry out Data Processing Impact Assessments (DPIAs) to evaluate the risk of their processing activities. If this assessment shows that any of their processing activities are high risk, a DPO must be appointed.

## United Kingdom

Following Brexit, the UK Government has transposed the GDPR into UK national law creating the "UK GDPR". As it stands, and as with GDPR above, each data controller or data processor is required to appoint a DPO if it is a public authority and/or its core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; and/or processing of sensitive personal data on a large scale.

## 4.2 Voluntary designation

Even when the data protection regulation applicable to your organisation does not specifically require the appointment of a DPO, you may find it useful to appoint a DPO on a voluntary basis

to help facilitate compliance with the applicable data protection legislation, and act as an intermediary between the supervisory authority, data subjects, and cross-functional teams (perhaps on behalf of a group DPO as a local "data protection champion") within an organisation. This is particularly important in all cases where, in the exercise of processing activities, there are risks to the rights and freedoms of data subjects.

To differentiate between the mandatory role and the voluntary appointment, some organisations prefer to designate the voluntary role Data Protection Manager or similarly, rather than using the DPO-label. This is worth considering, as appointing a DPO may indirectly introduce requirements, that the organisation if opting for the voluntary data protection role may otherwise not be subject to.

## Australia

Australia's federal Privacy Act 1988<sup>13</sup> does not require organisations to appoint a DPO. However, the Privacy Commissioner has issued guidance recommending that organisations appoint a DPO as good practice.

---

13 [Privacy Act 1988 \(legislation.gov.au\)](https://www.legislation.gov.au)

## Bahrain

The Personal Data Protection Data Law No. 30 of 2018<sup>14</sup> asserts that data controllers may voluntarily appoint a DPO, although the Personal Data Protection Authority's Board of Directors can mandate that certain data controllers appoint a DPO.

## Kenya

The Data Protection Act, 2019 in Kenya<sup>15</sup> makes provision for the designation of a DPO, but this designation is not mandatory. DPOs can be members of staff and may perform other roles. A group of entities can also share a DPO. The contact details of the DPO must be published on the organisation's website and communicated to the newly established Office of the Data Protection Commissioner.

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.

14 <https://www.bahrain.bh/Portals/0/PDFs/PersonalDataProtectionLawNo30of2018.pdf> (bahrain.bh)

15 [TheDataProtectionAct\\_No24of2019.pdf](https://kenyalaw.org/kenya-law-library/the-data-protection-act-no-24-of-2019) (kenyalaw.org)

## 5. Selection of the DPO

The DPO is a challenging role in the EU but it is likely to be even more so in countries and/or organisations where the data protection/privacy regime, or DPO role, is new. 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 illegitimate data processing scenarios, and which ultimately can have business implications as well as consequences for business process owners who knowingly has been mishandling personal data.

It is also worth emphasising to readers that a DPO is not appointed to take accountability or to perform all operational duties related to 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.

### 5.1 Qualifications of the DPO

The GDPR provides that the DPO “shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil (his/her) tasks.”<sup>16</sup>

THE DPO PLAYS  
A CRITICAL ROLE IN THE  
SUCCESS OF ANY PRIVACY  
PROGRAMME.

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 EU and/or other national borders, particularly if you are established in, or sharing data with processors, in multiple jurisdictions - even more so if you need to ensure compliance with other national or industry data sovereignty or cy-

bersecurity obligations. By default, a DPO should therefore have expertise in national and international data protection laws and practices.

PROCESS OWNERS WILL  
HAVE TO GUIDE AND  
SUPPORT THE VARIOUS  
DATA PROCESS OWNERS  
ACROSS THE ORGANISA-  
TION.

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 integ-

rity 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 the data protection expertise, and they 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.

## 5.2 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 GDPR specifically states that 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 in an independent manner. 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<sup>17</sup> - even in a jurisdiction like the EU with a relatively mature privacy regime:

- » 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, with the apparent exception being Egypt. That accountability will always remain with the data controller. This again underscores why selecting the right

individual is so critical. This is why, should you choose not to appoint a DPO, we would recommend that this decision be documented and then signed off by a senior leadership team member in your organisation.

### 5.3 Reporting line for 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.

However, the European Data Protection Supervisor (EDPS), does provide some guidance on the placement of the DPO in the organigramme<sup>18</sup> 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,
- » the 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 man-

<sup>17</sup> [The Difficult Role of the DPO | White Label Consultancy](#)

<sup>18</sup> [https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo\\_en](https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en)

agement, in the same way 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.

Some further guidance on the placement and the role of the DPO is offered in the Proximus-case<sup>19</sup>. In the case the Belgian Supervisory Authority, fined Belgium's largest telecommunications operator, Proximus, on the ground that the company had failed to protect its DPO from conflicts of interests in violation of the GDPR.

The authority ruled that the conflict arose from the fact that Proximus' DPO also fulfilled the function of director of audit, risk and compliance. The ruling accentuates that the DPO's role should not be undermined, but rather should be at the core of the organisational design.

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.

The DPO should have the authority to investigate. 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. The EDPS emphasises that for EU institutions DPOs are appointed for a period between three and five years, may be reappointed and can be dismissed only with the consent of the EDPS. For private organisations, some further flexibility must be expected, but contracts for internal employees of less than 2 years could be challenged. For external DPOaaS, contracts of less than 1 year duration with termination for convenience clauses could well be challenged by the authorities.

---

19 <https://www.dataguidance.com/news/belgium-belgian-dpa-issues-%E2%82%AC50000-fine-organisation-dpo>




## 6. The outsourced DPO

**T**he data protection regulations in Europe and other jurisdictions, like the ADGM and the DIFC in the UAE, and Nigeria, 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 orien-

tated 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.

A composite image featuring a hand clicking a computer mouse in the foreground, with a blurred cityscape at night in the background. A semi-transparent dark blue box with a white border is positioned on the right side, containing white text.

(DPOAAS) CAN BECOME  
A COMPELLING, PRACTI-  
CAL, AND COST-EFFEC-  
TIVE SOLUTION FOR MANY  
ORGANISATIONS.

## 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. The recent discussions on the use of various applications for Covid-19 tracking and tracing are an excellent example of the reaction to technology when solutions are implemented without the required level of digital trust having been established.<sup>20</sup>

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 have an expectation of privacy. The big technology companies realised this many years ago, but as more and more companies strive to become data driven, this focus on digital trust and privacy is applicable 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** - this 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** - this 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 since the GDPR came into effect and we have witnessed a global avalanche of regulatory data protection updates, including the requirement of the DPO as a mandatory or voluntary function.

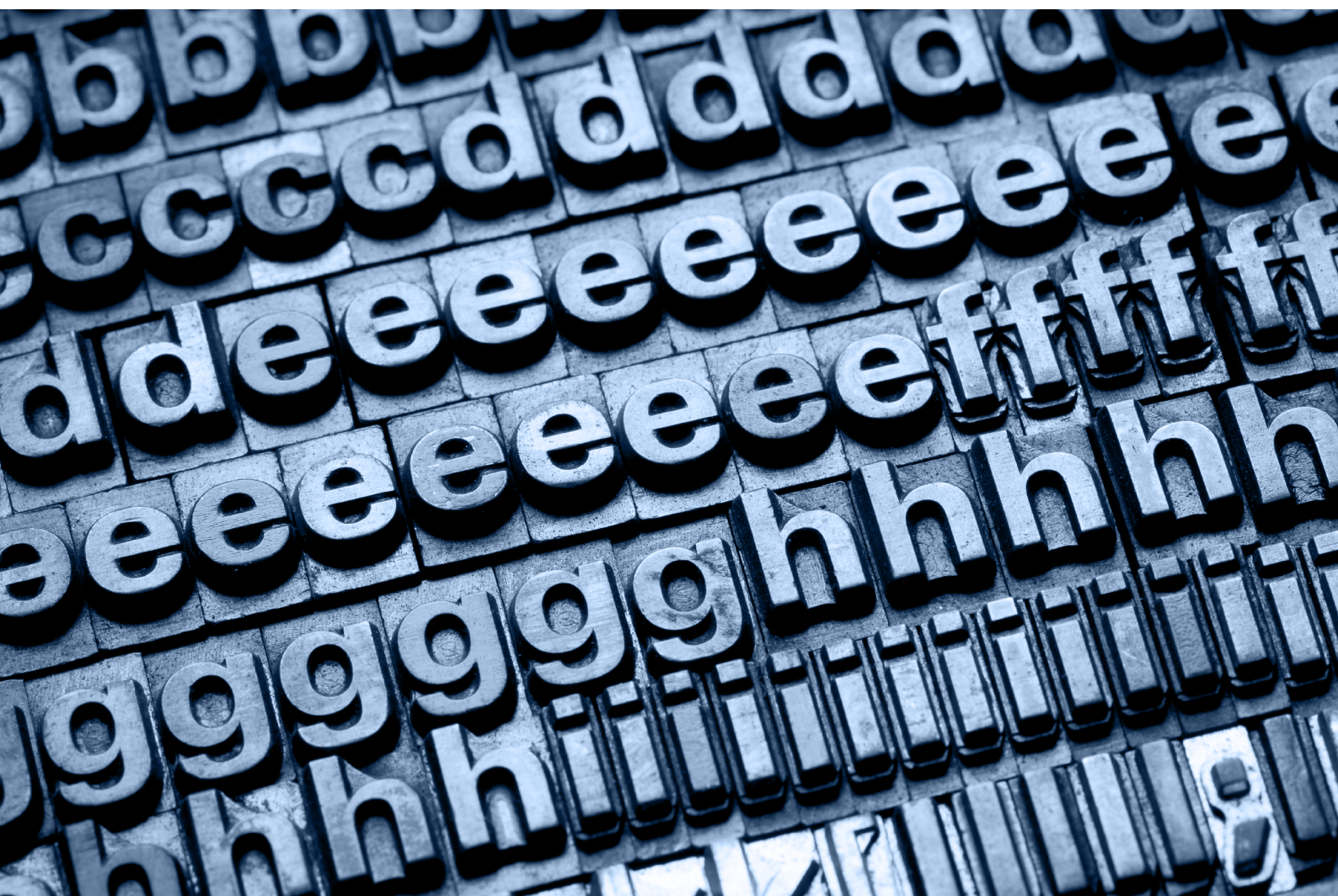
DIGITAL TRUST OFFERS  
CONSIDERABLE BUSINESS  
INFLUENCE IN AN INCREAS-  
INGLY DIGITAL ECONOMY.

## 8. Conclusion

**A**s 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, and 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?

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,
- » to manage communications with authorities, processors, and data subjects,
- » to assist in the development and maintenance of your record of processing activities,
- » to conduct the data privacy annual assessment,
- » to update, maintain and implementing compliant privacy policies and procedures,
- » negotiate privacy clauses in contracts with vendors,
- » monitor ongoing compliance with data protection requirements,
- » to assist the organisation in performance of data protection impact assessments.

## 10. Authors



Nicholai Pfeiffer

Managing Partner

[np@whitelabelconsultancy.com](mailto:np@whitelabelconsultancy.com)



Magdalena Goralczyk

Partner

[mg@whitelabelconsultancy.com](mailto:mg@whitelabelconsultancy.com)



Dale Waterman

Partner

[dw@whitelabelconsultancy.com](mailto:dw@whitelabelconsultancy.com)



Tomás Guedes de Figueiredo

Associate

[tgf@whitelabelconsultancy.com](mailto:tgf@whitelabelconsultancy.com)



## Contact information

Phone: +45 71 74 74 54

Email: [hello@whitelabelconsultancy.com](mailto:hello@whitelabelconsultancy.com)

Norway - Denmark - Poland - UAE