Data Protection Officers

Do I need one and what do they do?

Winckworth Sherwood


COUNTER:
EXPORT
Q-DATA
LOGIC
BIN
OFF
UNDEFINED
RFID
VECTOR
EXPORTING DATA...
CONNECTING...

Introduction

The forthcoming EU General Data Protection Regulation ('GDPR') enters into force in May 2018 and requires, for the first time in the European Union, some organisations to appoint a Data Protection Officer ('DPO'). With regard to DPOs appointment currently, there is inconsistency across the EU. Some countries, such as Germany and Spain, mandate the appointment of a DPO in certain circumstances. Other countries permit organisations to voluntarily appoint DPOs, and in doing so reduce an organisation's obligations in other areas of data protection law (for example, by providing an exemption to notifying the organisation's processing activities to the data protection authority). For companies and organisations which operate internationally, the legal landscape is complex and peppered with trip wires. The aim of this guide is to de-mystify and simplify the available solutions.[1]

The mandatory obligation to appoint a DPO forms a key part of the strengthened accountability obligations found in the GDPR, alongside new obligations on organisations to carry out data protection impact assessments, implement the principles of privacy by design and by default, and to maintain internal records of their data processing activities.

The Article 29 Working Party[2] ("WP29") issued guidance on DPOs in December 2016 which underlines the importance of DPOs in the compliance programmes of organisations and provided that:

"Before the adoption of the GDPR, the WP29 argued that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses. In addition to facilitating compliance through the implementation of accountability tools (such as facilitating or carrying out data protection impact assessments and audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor.

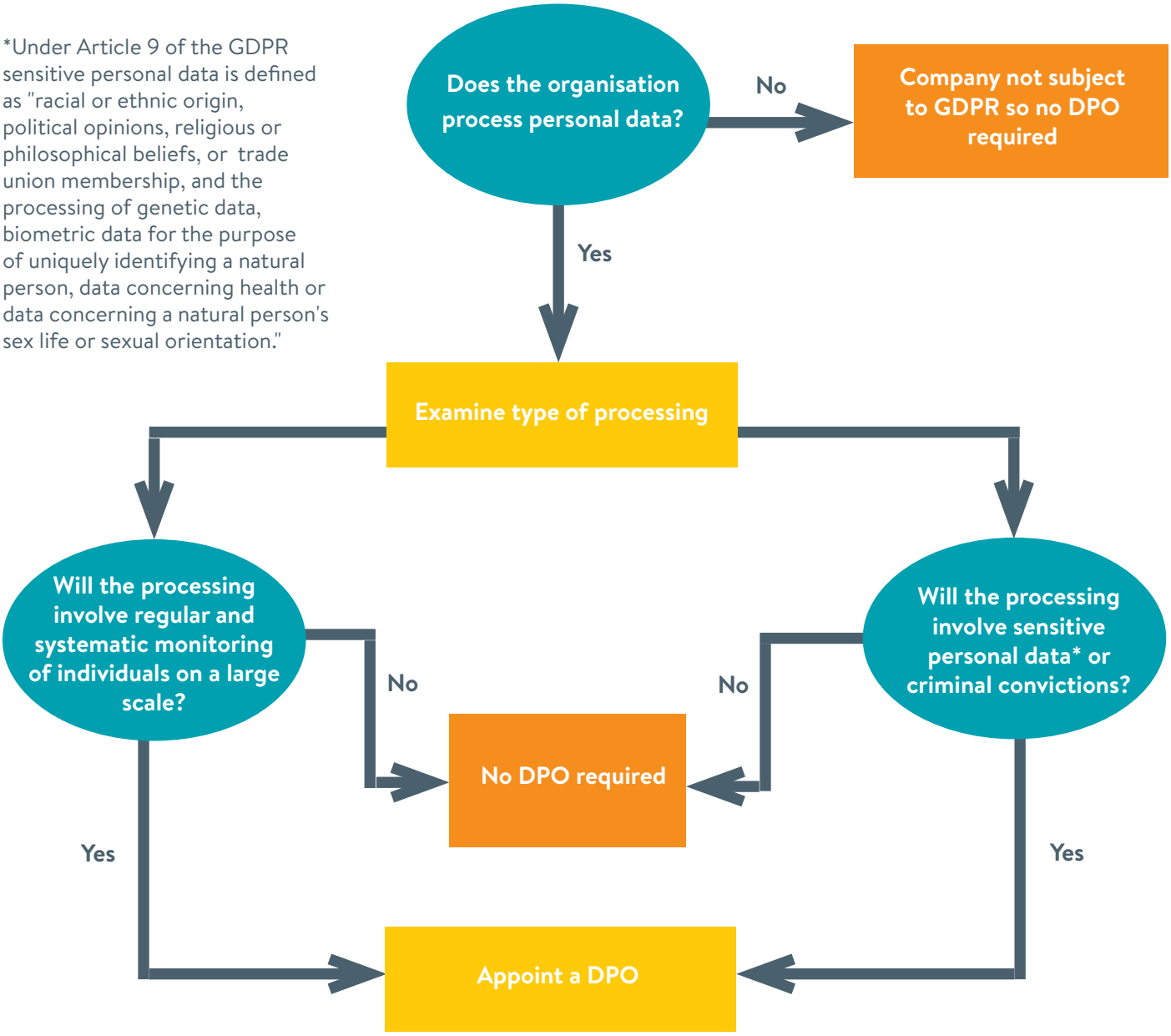
The controller or the processor also has a crucial role in enabling the effective performance of the DPO's tasks. Appointing a DPO is a first step but DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively."

1 This guide does not, however, represent legal advice.

2 The "Article 29 Working Party" provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.

When am I obliged to have a DPO?

*Under Article 9 of the GDPR sensitive personal data is defined as "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."



Data controllers and data processors must appoint a DPO if they carry out processing involving the 'regular and systematic monitoring of data subjects on a large scale' or if they process sensitive personal data or data relating to criminal convictions and offences 'on a large scale'. Public authorities will also need to appoint a DPO. There is no definition in the GDPR of the terms 'systematic', 'regular', and 'large scale' and the rules relating to mandatory appointment of a DPO were amended throughout the negotiation process before the GDPR was finalised. Earlier drafts referred to a requirement that organisations should have a minimum of 250 employees or those organisations which process personal data relating to at least 5000 individuals (each year) must appoint a DPO. However these thresholds and criteria were removed in the final draft.

What does 'large scale' mean in practice?[3]

The GDPR does not define what constitutes large-scale processing. You should take into account these factors:

- the number of data subjects concerned – employees and customers
- the volume of data and/or the range of different data items being processed
- the duration, or permanence, of the data processing activity
- the geographical extent of the processing activity

Examples of 'large scale' processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

What does 'regular and systematic monitoring' mean?[4]

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, monitoring is not restricted to the online environment.

Examples of activities that may constitute a regular and systematic monitoring of data subjects:

- operating a telecommunications network or providing telecommunications services
- email retargeting

[3] Source: Article 37(1)(b) and (c) of the GDPR

[4] Source: Article 37(1)(b) of the GDPR

- data-driven marketing activities
- profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering)
- location tracking (e.g. by mobile apps)
- loyalty programs
- behavioural advertising
- monitoring of wellness, fitness and health data via wearable devices
- CCTV
- connected devices e.g. smart meters, smart cars, home automation, etc.

'Regular' means:

- ongoing or occurring at particular intervals for a particular period
- recurring or repeated at fixed times
- constantly or periodically taking place

'Systematic' means:

- occurring according to a system
- pre-arranged, organised or methodical
- taking place as part of a general plan for data collection carried out as part of a strategy

The GDPR also contains a provision allowing the EU or Member States to designate additional categories of controllers or processors that will also need to appoint DPOs. The number of organisations that must appoint DPOs is therefore likely to increase once additional organisations are designated. This could potentially lead to difficulties for organisations where there are disparate national and EU laws requiring the DPO appointment, particularly where the DPO's role is defined differently under national laws.

In such cases, organisations will need to decide whether to appoint multiple individuals to act in the different DPO roles, or whether to appoint a single DPO to fulfil all of the requirements.

I am only a processor, do I need a DPO?

The simple answer is yes. The GDPR requirements to appoint a DPO apply equally to controllers[5] and processors[6]. Depending on whether your organisation fulfils the criteria for the mandatory appointment of a DPO, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other).

[5] The 'controller' is defined by Article 4(7) as the person or body, which determines the purposes and means of the processing.

[6] The processor is defined by Article 4(8) as the person or body, which processes data on behalf of the controller.

Examples:

• A small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large scale', considering the small number of customers and the relatively limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out large-scale processing. The processor must therefore appoint a DPO. At the same time, the family business itself is not under an obligation to appoint a DPO.

• A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor must appoint a DPO under the GDPR provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to appoint a DPO.

The DPO appointed by a processor also oversees activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

What does a DPO do?

The GDPR sets out in detail the minimum responsibilities of the DPO role[7]. DPOs, among other duties, must monitor compliance with the GDPR. Recital 97 further specifies that DPOs 'should assist the controller or the processor to monitor internal compliance with this Regulation'.

The DPO duties include informing and advising the organisation and its employees of the obligations of the GDPR and other data protection law; monitoring compliance of the organisation, both its practices and policies, with the GDPR and other data protection laws; raising awareness of staff of data protection law; providing relevant training to staff; carrying out data protection-related audits; providing advice to the organisation, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the organisation's wider obligations with regard to DPIAs; and acting as a contact point for the organisation's regulator.

As part of these duties to monitor compliance, DPOs may, in particular:

- collect information to identify processing activities
- analyse and check the compliance of processing activities
- inform, advise and issue recommendations to the controller or the processor

[7] See Appendix 1

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.'[8] Data protection compliance is a corporate responsibility of the data controller, not of the DPO.

In addition to those tasks, the DPO will also need to act as a contact point for individuals. Individuals may elect to contact the DPO on all issues relating to the processing of their personal data, and may also exercise their rights under the GDPR (for example, to obtain subject access or object to processing) by contacting the DPO. The DPO will therefore have a clear 'internal' and 'external' aspect to their role, and it will be important to ensure that these do not interfere with one another.

The appointed DPO must at all times have regard to 'the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing.' This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the organisation's processing of personal data.

It will be important for organisations to properly delineate the role of the DPO, in accordance with not only the GDPR, but also with the organisations internal management structures, practices and culture. For example, some organisations may not wish for their DPOs to be in direct communication with the organisation's data protection regulator (in the UK, the ICO), but would rather such communication is handled by the in-house legal or compliance team. In some circumstances, there may be strong reasons for doing so, such as maintaining legal privilege of those communications.

The DPO should 'cooperate with the supervisory authority' and 'act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter'[9].

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/ confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.

Please note, under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'.

As the GDPR states that DPOs 'shall have at least the following tasks', it is open for Member States or other EU regulatory bodies to prescribe additional tasks for DPOs. Such additional rules could potentially lead to confusion for DPOs if they are subject to inconsistent obligations across the EU, perhaps hampering the ability for organisations to appoint a pan-EU DPO responsible for the role across an organisation's EU offices.

8 Article 24(1)

9 Article 39(1)(d) and (e)

DPOs and DPIAs

A data controller (and not the DPO) is required to carry out a data protection impact assessment ('DPIA') under the GDPR in certain circumstances.[10] The controller must 'seek advice' from the DPO when carrying out a DPIA. DPOs have the duty to 'provide advice where requested as regards the DPIA and monitor its performance'.

It is recommended that controllers should seek the advice of the DPO on the following issues:
- Whether or not to carry out a DPIA
- What methodology to follow when carrying out a DPIA
- Whether to carry out the DPIA in-house or whether to outsource what it safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.

Role Checklist

- ☒ Raising data protection awareness within the organisation, and advising on GDPR compliance
- ☒ Ensuring the implementation of the appropriate documentation to demonstrate GDPR compliance
- ☒ Monitoring the implementation and compliance with policies, procedures and GDPR in general
- ☒ Handling of data breaches, including notification to the ICO and data subjects
- ☒ Liaising with the ICO, the employees' representatives and with the data subjects
- ☒ Monitoring Data Protection Impact Assessments
- ☒ Cooperating with and acting as the contact point for the ICO 'on issues relating to processing'

[10] For more information about DPIAs including a template assessment checklist, please contact us.

Data controllers and processors should ensure that:

- ☒ The DPO is invited to participate regularly in meetings of senior and middle management
- ☒ The DPO's name and contact details are provided to the supervisory authority (in the UK, the ICO)
- ☒ The DPO is present when decisions with data protection implications are taken
- ☒ All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice
- ☒ The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice
- ☒ The DPO must be promptly consulted once a data breach or another incident has occurred

Who should be your DPO? Selecting the right person

When appointing a DPO, organisations must make their selection on the basis of their 'professional qualities', on their 'expert knowledge of data protection law' and ability to perform the role of DPO. There is no requirement for a specific qualification and so it is not clear what level of knowledge of data protection law a DPO will require. It is likely that common standards will be developed in the future, possibly including EU-wide certification programs for individuals to demonstrate they have the appropriate knowledge of data protection law to perform the role of DPO.

Organisations are not limited to members of staff when considering candidates for the DPO role, but may choose to appoint an outside contractor to perform the role on the basis of a service contract. Where an external DPO is selected, it will be important for organisations to ensure that the DPO is able to form productive relationships with internal stakeholders and colleagues in order to perform the DPO role adequately.

On the other hand, an external DPO perhaps has an additional façade of independence which an internal DPO may not be able to demonstrate, particularly if the chosen individual already has close working relationships with the stakeholders whose actions they will be required to monitor.

Where an employee is chosen as the DPO, there is nothing to prevent that individual from also performing other roles at the organisation, such as a Head of Legal or Chief Compliance Officer role, provided such roles do not affect his or her ability to adequately perform the role of DPO. Internal DPOs will also have to manage issues which might arise regarding confidentiality and it will be important for organisations to put in place policies which deal with any conflict of interests between the DPO role and other responsibilities to shareholders, regulators and other stakeholders. Groups of organisations may appoint a single DPO for the whole group, provided that the DPO is accessible from each of the organisation's EU establishments.

The DPO needs to fulfil a dual role – that of the 'trusted adviser' on data protection, and also 'policing' and supervising correct compliance with data protection rules.

What are the professional qualities that the DPO should have?

The DPO should be selected on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil his or her tasks. The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.

Relevant skills and expertise

• Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
• Understanding of the processing operations carried out
• Understanding of information technologies and data security
• Knowledge of the business sector and the organisation
• Ability to promote a data protection culture within the organisation

Personal qualities

A DPO has to gain the confidence of senior executives at board level and be a trusted advisor and point of contact. Our suggested list of personal qualities includes:
• A good communicator who can article complex legal and technical issues in an easy to understand manner
• Someone with gravitas, whose advice will be followed
• Experience of managing upwards at board level
• A good networker who can liaise internally in an organisation and externally with other DPOs
• The ability to generate trust so that employees are more likely to report matters
• A solution orientated pragmatist who has the ability to apply discretion and make well balanced decisions taking into account the needs of the organisation and the rights of individuals

Resources

The DPO must have the resources necessary to be able to carry out his or her tasks. Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:
• Active support of the DPO's function by senior management
• Sufficient time for DPOs to fulfil their tasks
• Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
• Official communication of the designation of the DPO to all staff
• Access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
• Continuous training

Avoiding conflicts of interests

The GDPR permits organisations to allow DPOs to 'fulfil other tasks and duties' but requires that the organisation must ensure that 'any such tasks and duties do not result in a conflict of interests'. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests and they must at all times act independently. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as Chief Executive, Chief Operating Officer, Chief Financial Officer, Chief Medical Officer, Head Of Marketing, Head of Human Resources or Head of IT) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interest may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

Some commentators have suggested a Head of Legal is not an appropriate role to be combined with a DPO because of the inherent conflict of interest which may arise particularly with regard to disclosures to regulators. However, Heads of Legal frequently deal with conflicts of interest and often in regulated sectors have lines of communication with other regulators. It therefore should be possible to avoid these two roles being in conflict.

Appointment checklist

- A DPO can be an employee of the organisation or a third party service provider
- A DPO may also have other parallel roles – although a DPO must not be conflicted to act in the full performance of the DPO duties
- The ideal candidate must be able to combine a sound knowledge of data protection law with a robustness of character and the ability to articulate complex issues at board level
- The DPO should have at least a dotted line into the highest levels of management in the organisation and ensure that data protection is a board agenda item

A proposed DPO job specification can be found in Appendix 2.

Should I appoint one, even if I don't want to?

Organisations may voluntarily elect to appoint a DPO if they are not required by law to do so. Many organisations currently appoint DPOs voluntarily. In particular, data processors may find it easier to demonstrate their commitment to compliance with the GDPR by voluntarily appointing a DPO. This appointment provides both an indicator to an organisation's customers, and regulators, that the organisation takes its data protection obligations seriously, and is committed to building an effective and accountable privacy programme.

Once a DPO has been selected, there is no requirement to register his or her appointment with the relevant regulator. However, the appointing organisation is required to publish the contact details of the DPO, including in its privacy information notices, and to communicate the DPO's name and contact details to its regulator.

Is the DPO akin to an independent whistle-blower?

The GDPR contains a number of rules relating to the role of the DPO aimed primarily at ensuring the independence of DPOs, and in ensuring they have adequate resources to allow them to effectively perform the role.

Firstly, the GDPR requires the organisation to ensure the DPO is involved 'properly and in a timely manner' in all data protection related issues. In addition, the organisation must provide resources to the DPO to enable him or her to carry out the DPO's assigned tasks, and to maintain his or her expert knowledge of data protection law. The DPO will need to be involved in all data protection-related issues affecting the business. The level of responsibility, and accordingly the level of resources needed to adequately perform the role, will therefore vary significantly by organisation.

A large organisation with multiple EU operations that focusses on processing personal data collected from multiple sources will require a more well-resourced DPO than a smaller domestic based organisation with only minimal exposure to personal data. The GDPR is not prescriptive as to the resources to be made available to the DPO, and again what is appropriate will depend largely on the organisation in question. Resources are likely to include, amongst other things, a budget for the DPO and (potentially) their office, training materials and legal resources, access to outside legal counsel, IT and other technical resources, allowances to visit conferences and other learning opportunities.

Perhaps the most important aspect of the DPO's role is that the DPO must be independent of the management of the organisation, and that the DPO must not 'receive any instructions regarding the exercise of those tasks'. The DPO must also report directly to the 'highest management level' of the organisation. It is not clear whether this means directly to the Chief Executive Officer, or to some other part of the management of the organisation. In practice, this is likely to mean that the DPO will need to report into the board of the organisation, most likely via the organisation's Chief Compliance Officer or Chief Legal Officer, depending on the management structure of the organisation.

For organisations whose main business is the processing of personal data, it may be that the DPO has a direct position on the board. In any event, reporting lines should be 'true' reporting lines that enable the DPO to report to individuals who have the power to make binding decisions and real changes to the organisation's privacy practices, particularly after a specific incident of non-compliance.

Conclusion

The role of the DPO has become increasingly important over the last several years for data protection compliance and risk management, and with the introduction of the DPO obligation under the GDPR, this trend is set to continue.

While the GDPR contains detailed provisions as to the selection, position and tasks of DPOs, there are still significant and challenging practical questions regarding how the role will work on a day-to-day basis. Although the GDPR will enter into force in 2018, there are a number of steps that organisations can take now to begin their preparations, which are set out on the next page.

DPO Action Plan

1. Take action now. Confirm whether your organisation will have to appoint a DPO. If so start thinking about the best way to do it.
2. If you are going to make an internal appointment, consider whether training and/or a suitable qualification is required.
3. Define a specific data protection budget including the costs of the DPO, his/her training and staff.
4. If you have operations in several jurisdictions, define the rationale for allocating local and specific data protection responsibilities.
5. Define whether an internal DPO will work better for your corporate structure, or whether an external service provider is a better option.
6. If an internal employee is more appropriate, define your risk appetite for having an internal DPO with multiple parallel functions.
7. Conduct a data protection audit to assess any gaps that the DPO will have to resolve.
8. Consider what the right job specification is for the DPO in your organisation (and don't ask your selected candidate to draft this!).

Appendix 1

Text of the GDPR relating to DPOs

Art 38 - Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Appendix 2

DPO Role Profile & Job Description

- **DPO details**

Name of organisation	[Insert name]
Name of DPO	[Insert name]
Reports to	[Insert name and/or position]
Full time/part time	[Insert]
Details of any other roles held within the organisation	[Insert details of any other roles held within the firm]
Date appointed	[Insert date]

- **Role summary**

To ensure systems and controls are in place to enable the organisation, including its managers and employees, to comply with their obligations under UK [AND/OR global] data protection legislation.

- **Responsibilities**

a) Strategic data protection management

i) Be the focal point for all activity within the organisation relating to data protection.

ii) Support and co-ordinate senior management focus on and promote a culture of awareness of data security throughout the firm.

iii) Develop and manage the organisation's data protection strategy [in the UK AND/OR globally].

iv) Oversee the organisation's systems and controls in relation to data protection.

b) Compliance

i) Ensure the firm organisation's entry on the Register of data controllers maintained by the Information Commissioner is kept up to date and accurately reflects the organisation's processing activities.

ii) Implement systems and controls to ensure compliance with relevant [UK AND/OR global] data protection legislation and regulation, to include drafting, maintaining and implementing data protection policies and procedures, systems and controls.

iii) Monitor and prepare for implementation of the EU General Data Protection Regulation (GDPR).

iv) Identify all circumstances in which personal data is transferred outside the EU and implement procedures to ensure compliance with relevant requirements relating to international data transfer.

v) Implement procedures to deal with subject access requests.

vi) Undertake periodic data protection audits, including all relevant manual filing systems, computerised filing systems, any outsourced processes, archived systems and back up data, to assess the organisation's compliance with data protection requirements. Ensure any deficiencies identified as a result of an audit are addressed.

vii) Inform and train staff on the requirements of the [UK AND/OR global] data protection regime and the care and handling of personal data.

viii) Respond promptly to any reasonable request for information made by the Information Commissioner or any other relevant regulator or law enforcement agency.

ix) Ensure data processing agreements are in place with third parties handling personal data.

x) As necessary, advise on and conduct privacy impact assessments and monitor their effectiveness.

xi) Monitor compliance with [UK AND/OR global] data protection requirements and with the organisation's policies and procedures, including in relation to:

(1) the assignment of responsibilities
(2) awareness-raising and training of staff involved in processing operations
(3) any related audits

xii) Liaise, as required, with the organisation's [insert details of any other relevant compliance officers, e.g. Head of Compliance, Head of Risk] to ensure appropriate sharing of information and consistency of approach.

c) *Risk*

i) Conduct [firm OR organisation]-wide risk assessments on data protection compliance at appropriate intervals, but at least [insert frequency, e.g. annually].

ii) Maintain a central register of data security reports in a form that allows the DPO and the organisation to:

(1) monitor and assess the effectiveness of the organisation's data protection systems
(2) identify any data security report that may be linked
(3) adequately respond to requests for information
(4) identify any training needs within the firm

iii) Actively participate in the organisation's [state name of any internal group whose remit includes information security, e.g. Information security group or Risk management group].

iv) Create and deliver data protection content for risk workshops.

d) *Advice and guidance*

i) Advise on the appointment and use of data processors and ensure appropriate contracts terms are included in any data processing agreement.

ii) Inform and advise the organisation and any employees who process personal data of their obligations pursuant to [UK AND/OR global] and international requirements.

iii) Advise the organisation on any transfers of personal data outside the EU.

iv) As required, provide input on the data protection implications of the organisation:

(1) projects
(2) business development/marketing strategy
(3) proposed mergers, acquisitions and disposals

v) Provide advice and guidance to members of staff in respect of any data protection questions, issues or developments that may arise from time to time, e.g. in relation to the development of new IT systems and procedures, drafting data protection notices, obtaining consent from data subjects and in the operation of the organisation's HR function.

vi) Provide advice and guidance on subject access requests.

vii) At least [insert frequency, e.g. annually], submit a report to the [board OR senior management team OR [other] which:

(1) assesses the effectiveness of the firm's data protection arrangements, and
(2) makes appropriate recommendations for improvement

e) Incident management

i) Devise and implement an internal system for reporting actual or suspected data security breaches (data security reports).

ii) Respond to and manage (including liaising with the ICO and any other regulator) any:

(1) data security breaches
(2) data security reports
(3) communications received from or enforcement action initiated by the ICO or any other relevant regulator
(4) complaints or communications relating to data protection and/or security received:

(a) from other professional representatives (e.g. [insert description, e.g. solicitor acting for the other side in a dispute])
(b) directly from clients and other members of the public

f) Horizon scanning

i) Monitor and prepare for implementation of the EU General Data Protection Regulation.

ii) Keep abreast of any regulatory or other changes relating to data protection that may affect the organisation and, as necessary:

(1) inform the organisation in good time of any actions that need to be taken
(2) amend existing policies and processes and/or devise and implement new policies and processes
(3) train staff

iii) Keep abreast of emerging technologies/communication channels that are relevant to data protection.

iv) Monitor ICO guidance, enforcement actions and policies.
v) Network with data protection and information security professionals outside the [firm OR organisation] to gain insight into good practice across the [sector OR industry OR profession].

- **Relationship between the DPO and senior management**

a) The DPO has the authority to act independently of senior management in carrying out their responsibilities.

b) The DPO shall directly report to the highest management level of the organisation.

c) Senior management will ensure the DPO has:

i) their active support
ii) adequate resources (including appropriate staff, technology and arrangements to apply in their absence)
iii) independence of action, and
iv) access to personal data processing operations and relevant business information

d) Where the DPO has any other tasks or duties, the organisation shall ensure this does not result in a conflict of interests.

OUR GDPR TEAM

TONI VITALE

HEAD OF REGULATION, DATA & INFORMATION

020 3735 1934
tvitale@wslaw.co.uk

JON BALDWIN

PARTNER, REGULATION, DATA & INFORMATION

020 7593 0384
jbaldwin@wslaw.co.uk

ANDREW YULE

PARTNER, EMPLOYMENT

020 7593 5089
ayule@wslaw.co.uk

ROBERT PAYDON

PARTNER, DISPUTE RESOLUTION

020 7593 5022
rpaydon@wslaw.co.uk

LOUISE LAWRENCE

SENIOR ASSOCIATE, EMPLOYMENT

020 7593 5082
llawrence@wslaw.co.uk

THERESA KERR

SENIOR ASSOCIATE, EDUCATION

020 7593 5154
tkerr@wslaw.co.uk


G

Winckworth Sherwood