information commissioner
Barrantagh Fysseree

Data Protection Officer

The General Data Protection Regulation

Important

This document is part of a series, produced purely for guidance, and does not constitute legal advice or legal analysis.

All organisations that process data need to be aware that the General Data Protection Regulation may apply directly to them.

The responsibility to become familiar with the GDPR and comply with its provisions from 25th May 2018 onwards lies with the organisation.

Legal advice, if required, should be sought from a Manx advocate.

Index

Overview

Articles 37 to 39 make provision for the designation, position and tasks of the Data Protection Officer (DPO). These provisions are set out in full in Annex A.

The fundamental role of the DPO is explained in Recital 97 as:-

> *" …a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance …"*

The DPO is not a new concept and has existed in other jurisdictions for some time, for example in Germany where it is mandatory for a company engaged in automated data processing and employing more than nine employees to have a DPO.

Under the GDPR it is mandatory for certain controllers and processors to designate a Data Protection Officer (DPO). This obligation applies to the public sector irrespective of what data they process, and controllers and processors that regularly and systematically process personal data on a large scale.

The Article 29 Working Party* has previously expressed the view :-

> *"The DPO is a cornerstone of accountability … they should be considered as the "compliance orchestrator" and the intermediary between all relevant stakeholders (e.g. supervisory authorities, data subjects, business partners)."***

and has formally adopted and published "Guidelines on Data Protection Officers."

This note summarises the guidelines

which can be found at :

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

* The body established by Article 29 of EU Data Protection Directive 95/46/EC and consisting of a representative from each of the 28 EU member state data protection authorities, the European Data Protection Supervisor and the European Commission. Under the GDPR, the Article 29 Working Party becomes the European Data Protection Board (EDPB).

** http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

1. The role of the DPO

Article 38(1) states:-

"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."

The DPO should be seen as an important contributor to any group dealing with data processing activities within the organisation. Ensuring that the DPO is informed and consulted from the outset will facilitate compliance and promote a privacy by design and default approach, as required by Articles 24 and 25, and, as such, should become a standard procedure in an organisation's governance processes.

The DPO, or his/her team, should be involved from the earliest stage possible in all issues relating to data protection, including, for example:-

- regular participation in senior management meetings,
- any decision with a data protection implication, and
- provided with all relevant information in a timely manner.

Due weight must be given to the DPO's opinion and, in case of disagreement, the reasons for not following the DPO's advice should be documented.

There are other provisions in the GDPR which specifically require the DPO's involvement, including data protection impact assessments and data breach notification.

2. The tasks of the DPO

Article 39 (see Annex A) sets out the minimum tasks of the DPO. In summary these are:-

- monitor and audit compliance with the GDPR and related policies;
- inform and advise the controller or processor of their obligations;
- awareness-raising and training of staff;
- provide advice with regard to data protection impact assessments;
- act as the contact point for the supervisory authority; and
- cooperate with the supervisory authority.

Provided there is no conflict, a DPO may be assigned other tasks, or the tasks may be specified in more detail. It is recommended that an organisation clearly sets out, for example in the DPO's contract, the precise tasks of the DPO and these tasks should be conveyed to other staff.

2.1. Monitoring compliance

The DPO should assist the controller or the processor to monitor compliance and, in doing so, may:-

- 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.

2.2. DPO and data protection impact assessments

The obligation to carry out a data protection impact assessment (DPIA) under Article 35 and to comply with the principle of data protection by design and default set out in Article 25 rests with the controller and not the DPO. However, the DPO has an important role in assisting the controller with a DPIA and Article 35(2) specifically requires the controller to seek advice from the DPO.

The DPO's advice should be sought on:-

- 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 it,
- what 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 DPIA 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 .

2.3. Cooperation with the supervisory authority

The DPO is the contact point for the supervisory authority and has responsibility for cooperating with the supervisory authority on behalf of the controller or processor. The DPO is expected to facilitate the supervisory authority's access to documents and information and the exercise of the supervisory authority's investigative, corrective, authorisation, and advisory powers.

2.4. Risk-based approach

Article 39(2) states:-

> *"The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.*

Article 39 advocates a common sense approach where the DPO prioritises activities and focuses upon issues that present higher risk. This does not mean, however, that a DPO should neglect monitoring compliance of other lower risk processing.

A pragmatic approach should help a DPO identify processing operations to devote more time and resources to, identify areas that should be subject to an internal or external audit and what training should be provided to staff.

2.5. DPO and record-keeping

Under Article 30 the controller or processor is required to maintain a record of processing activities.

The task of maintaining such records could be assigned to the DPO as they are relevant to the DPO's monitoring task and, in any event, are necessary to provide an overview of the processing activities being undertaken.

2.6. DPO and data protection policies

Under Article 24(2) a controller must implement proportionate and appropriate data protection policies.

Providing advice and monitoring compliance with these policies are tasks of the DPO. The DPO could be specifically assigned the task of ensuring these policies remain appropriate and up to date.

3. Designation of a DPO

3.1 Voluntary designation

The guidelines recall that a controller and processor must be able to demonstrate compliance with all obligations under the GDPR and suggest a DPO should be designated as a matter of good practice.

Where a DPO is designated on a voluntary basis then Articles 37 to 39 will apply to that person.

3.2 No DPO designation

The guidelines emphasise that where a DPO is not designated then it will be a matter for that controller or processor to demonstrate to the supervisory authority in accordance with its accountability responsibilities why it was not obliged to do so. It is suggested that this may be best achieved by documenting the analysis that was undertaken that led to the decision not to designate a DPO.

When changes to processing occur the guidelines recommend that a review is undertaken.

(A controller or processor may be required to demonstrate to the supervisory authority how, in the absence f a DPO, it is meeting all of its obligations under the GDPR.)

3.3 Mandatory designation

While any controller or processor may voluntarily designate a DPO, Article 37(1) sets out when it is mandatory to do so.

3.3.1 Public Sector

Article 37(1) states:

> *"The controller and the processor shall designate a data protection officer in any case where:*
>
> *a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;*

All '*public authorities or bodies*' that process personal data must designate a DPO. The GDPR does not define what constitutes a '*public authority or body*' but it should be taken to mean all Government Departments, Statutory Boards, Offices, Local Authorities and other bodies established by statute.

Any natural or legal person that carries out a public function or service including for example water and energy supply, public service broadcasting, public housing or disciplinary bodies for regulated professions should also designate a DPO.

3.3.1.1 DPO for more than one public body

Article 37(3) states:-

"Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size."

3.2.2 Private Sector

Article 37(1) states:-

> *"(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or*
>
> *(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."*

The nature of processing undertaken by a controller or processor therefore determines when a DPO must be designated in the private sector.

3.2.2.1 What are 'core activities'?

'Core activities' are the key operations to achieve the controller's or processor's objectives.

These include activities where the processing of personal data forms an inextricable part of the activity. For example, processing Know Your Customer/ Customer Due Diligence data as required by Anti Money-laundering legislation, is a core activity.

Supporting activities, for example, paying employees is an example of a necessary support function and in most cases is an ancillary function rather than a core activity.

(*An obvious exception would be a payroll company where processing pay is a core activity*)

3.2.2.2 What does 'regular and systematic monitoring' mean?

Regular and systematic monitoring is not defined in the GDPR.

The guidelines interpret ***'regular'*** as meaning one or more of the following:

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

and ***'systematic'*** as meaning one or more of the following:

- 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

Examples of activities that may constitute ***regular and systematic monitoring*** include:

- 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); operating a telecommunications network; providing telecommunications services;
- data-driven marketing activities;
- location tracking, for example, by mobile apps;
- loyalty programs;
- behavioural advertising;
- monitoring of wellness, fitness and health data via wearable devices;
- closed circuit television;

3.2.2.3 What is 'large scale' processing?

The GDPR does not define what constitutes large-scale processing. The guidelines recommend some factors to be considered when determining whether the processing is carried out on a large scale. These are:-

- the number of data subjects concerned
- 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 customer data in the regular course of business by an insurance company or a bank
- processing of data (content, traffic, location) by telephone or internet service providers
- processing of real time geo-location data of customers
- processing of personal data for behavioural advertising by a search engine

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

3.2.2.4 What are 'Special categories' of data

Special categories of data include:-

- health,
- sex life or sexual orientation,
- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
  or
- the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person.

4. The position of DPO

4.1 Professional qualities and expert knowledge

Article 37(5) states:

"The data protection officer 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 the tasks referred to in Article 39."

The guidelines emphasise that the necessary level of expert knowledge required of the DPO 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 particularly sensitive data is involved, the DPO may need a higher level of expertise and support.

Relevant skills and expertise include:

- knowledge of the business sector and the organisation;
- understanding of the processing operations carried out;
- ability to promote a data protection culture within the organisation;
- understanding of information technologies and data security;
- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR.

4.2 Shared DPO

Article 37(2) states:-

"A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment."

Accessibility refers to the DPO as a contact point with respect to data subjects, the supervisory authority and within the organisation. In order to ensure that the DPO is accessible, whether internal or external, their contact details must be made available.

The DPO, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authority.

4.3 External DPO

Article 37(6) states:

" The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract."

The DPO can be external with the tasks fulfilled under a service contract.

When the DPO function is undertaken by an external provider, a team of individuals working for that provider may carry out the DPO tasks, under the responsibility of a designated lead contact.

The allocation of tasks and lead contact should be clearly set out in the service contract.

4.4 Conflicts of Interest

Article 38(6) states:

"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."

The DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of processing of personal data. Conflicting positions within the organisation may include senior management positions such as:-

- Chief Executive Officer,
- Chief Operating Officer,
- Chief Financial Officer,
- Chief Medical Officer,
- Head of Marketing Department
- Head of Human Resources
- Head of IT
  or
- Any other role that leads to the determination of purposes and means of processing.

A conflict of interest may arise in other scenarios; for example if an external DPO represents a controller in a matter before a Court relating to a data protection issue.

4.5 Independence

Article 38(3) states:

" 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 tasks. The data protection officer shall directly report to the highest management level of the controller or the processor."

A DPO must be able to perform their tasks with sufficient autonomy. A DPO must not be instructed how to deal with a matter, how to investigate a complaint or whether to consult the supervisory authority nor must they be instructed to take a certain view, for example, a particular interpretation of Data Protection legislation.

A DPO cannot be dismissed or penalised for performing their tasks. This strengthens a DPO's autonomy so they can act independently and provides sufficient legal protection to do so.

Penalties could be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient if they are intended to penalise the DPO for performing their tasks.

However, this autonomy does not mean that a DPO has decision-making powers extending beyond the tasks set out in Article 39.

If a controller or processor makes a decision that is contrary to the DPO's advice, the DPO must be able to make their position clear to the highest management level. Direct reporting ensures that senior management, including the board of directors, are aware of the DPO's advice and recommendations.

4.6 Resources

Article 38(2) states:

"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."

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
- Training including refresher training and CPD

4.7 Contact details

Article 37(7) states:-

" The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority,"

While Article 38(4) states:

"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."

The intention is to ensure that a data subject (either inside or outside an organisation) and the supervisory authority can easily and directly contact the DPO without having to contact another part of the organisation.

The contact details of the DPO should include:

- a postal address,
- a dedicated telephone number, and/or
- a dedicated e-mail address.

When appropriate, other means of communication could be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organisation's website.

Whilst it may be a good practice to do so, the published contact details do not need to include the name of the DPO. However, as the DPO is the controller or processor's contact point, the supervisory authority must be advised of the DPO's name.

4.8 Confidentiality

Article 38(5) states:

"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."

The DPO is bound by confidentiality in the performance of their tasks.

This obligation of confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority as Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.

ANNEX A

Chapter IV Section 4
Data Protection Officer

Article 37

Designation of the Data Protection Officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

Article 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 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.

Article 39

Tasks of the Data Protection Officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the 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.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Blank


information
commissioner
Barrantagh Fysseree