Guidance on the General Data Protection Regulation: (3) Data Protection Officer

Guidance Note IR03/17

31st August 2017

Gibraltar Regulatory Authority
Information Rights Division
2nd Floor, Eurotowers 4, 1 Europort Road
Gibraltar
GX11 1AA
Telephone +350 20074636 Fax +350 20072166
Email: privacy@gra.gi
Web: http://www.gra.gi

Contents

Introduction

The General Data Protection Regulation (the "GDPR") will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

This is the third of a series of Guidance Notes that the Gibraltar Regulatory Authority ("GRA"), as the Data Protection Commissioner, will issue in the run up to the 25th May 2018.

This Guidance Note provides general advice on the GDPR's requirement for organisations to appoint a Data Protection Officer ("DPO").

Under the GDPR, it will be mandatory for some data controllers and data processors to appoint a DPO, for example, all public authorities (with some minor exceptions) and organisations which carry out regular and systematic monitoring of data subjects on a large scale.

The DPO requirement introduced by the GDPR is not a new concept. Although current data protection law under the EU Data Protection Directive 95/46/EC does not include a mandatory obligation for organisations to appoint a DPO, the practice of appointing a DPO has developed and been adopted by organisations throughout the EU to ensure compliance with data protection law. Prior to the GDPR, the Article 29 Working Party already considered the appointment of a DPO as a "cornerstone of accountability" that can facilitate compliance and also become a competitive advantage for business[1].

A DPO will act as an intermediary between its employer and relevant stakeholders, such as data subjects and regulators. Although appointing a DPO will facilitate compliance with the GDPR and its requirements, it is important to know that DPOs are not held personally responsible for non-compliance with the GDPR. It is clear, within the GDPR, that it is the data controller or the data processor who is required, at all times, to ensure and demonstrate that its data processing complies with the GDPR.

The GDPR recognises the DPO as an important player in the new data protection regime.

The aim of this guidance note is to provide advice on the GDPR's requirement relating to the appointment of the DPO and also assist DPOs in their role.

[1] Annex to Letters from Art. 29 Working Party to MEP Jan Philipp Albrecht and to Commissioner Věra Jourová in view of the trilogue <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf > Accessed 11 August 2017

1. Appointing a DPO

GDPR - Article 37(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.

As outlined above, the GDPR introduces a requirement for organisations to appoint a DPO in certain circumstances. These are described in 1.1 to 1.3 below.

1.1 Public authority or body

In the absence of a definition in law, all public authorities or bodies will be required to appoint a DPO. The Commissioner interprets "public authorities" to mean:

- government departments;
- a body or other person, that carries out functions of public administration;
- a body or other person, that exercises functions of a public nature; and
- a body or other person that provides public services.

It is important to note that a public function may be exercised not only by public authorities or bodies, but also by other natural or legal persons including private organisations. In such cases, a DPO will also be required.

1.2 Regular and systematic monitoring of data subjects

Article 37(1)(b) relates to circumstances that involve the regular and systematic monitoring of data subjects. The following summarises the Commissioner's interpretation of regular and systematic monitoring -

REGULAR		***SYSTEMATIC***
Interpreted to mean - • Ongoing or occurring at particular intervals for a particular period; • Recurring or repeated at fixed times; or • Constantly or periodically taking place.	+	Interpreted to mean – • Occurring according to a system; • Pre-arranged, organised or methodical;

	• Taking place as part of a general plan for data collection; or • Carried out as part of a strategy.

Examples of regular & systematic monitoring include - operating a telecommunications network; providing telecommunications services; 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, for example, by mobile apps; loyalty programs or CCTV amongst other things.

It is important to note that the requirement only applies to circumstances where –

- the organisation's regular and systematic monitoring of data subjects is an intrinsic part of its ***Core Activities***[2]. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Processing patient data is thereby considered part of a hospital's *Core Activities*; and

- the data processing is carried out on a ***Large Scale***. The Commissioner interprets this to mean a relatively significant data processing activity, taking account of the following factors:

    - the number of data subjects concerned - either as a specific number or as a proportion of the relevant population;

    - the volume of data and/or range of different data items being processed;

    - the duration, or permanence, of the data processing activity; and

    - the geographical extent of the processing activity.

Examples of large scale processing: Processing of patient data by a hospital; processing of travel data of individuals using a city's public transport system (e.g. tracking via travel/ID cards); processing of real time geo-location data of customers for statistical purposes by a processor specialised in providing these services; processing of customer data in the regular course of business by an insurance, bank, or gambling company, processing of data (content, traffic, location) by telephone or internet service providers.

[2] Article 37(1)(b) and (c) of the GDPR refers to the '*core activities of the controller or processor'*. Recital 97 specifies that the core activities of a controller relate to '*primary activities and do not relate to the processing of personal data as ancillary activities*'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.

1.3 Special categories of data and data relating to criminal convictions and offences

This provision requires organisations that handle the following types of personal data to appoint a DPO:

- Special categories of data[3]: examples of organisations that process this type of personal data are organisations that provide medical/health services, unions and providers of biometric technology/services.
- Processing of personal data relating to criminal convictions and offences: this condition primarily concerns law enforcement organisations, but will capture any other organisation that process data concerning criminal convictions and offences.

This requirement is also conditional on the data processing being an intrinsic part of the organisation's ***Core Activities*** and being on a ***Large Scale***.

[3] This includes personal data revealing 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 shall be prohibited.

2. The requirement applies to Controllers and Processors

It is important to note that the requirement to appoint a DPO in Article 37 of the GDPR applies to both controllers[4] and processors[5].

Depending on who fulfils the criteria, in some cases only the controller may be required to designate a DPO or only the processor. In other cases, both the controller and the processor may be required to designate a DPO - under such circumstances, the DPOs should cooperate with each other. It is important to note that a processor is not required to appoint a DPO simply because the controller fulfils the criteria, although it may still be good practice to do so.

Example: 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 CCTV surveillance and security. 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 involving regular and systematic monitoring of data subjects. The processor i.e. the CCTV provider, must therefore designate a DPO under Article 37(1)(b). At the same time, the family business itself is not under an obligation to designate a DPO.

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

[5] Similarly, Article 4(8) defines a processor as a person or body, which processes data on behalf of the controller.

3. The role of the DPO

In this section, guidance is provided on key aspects of the DPO's role under the GDPR. In summary, these are –

- the *tasks* that the DPO should perform as part of their role;
- the DPO's *involvement* in data processing operations;
- the *qualities* that the DPO should have;
- the *resources* that the DPO should have;
- the *independence* of the DPO;
- preventing *conflicts of interest*;
- assigning a DPO for a *group* of undertakings or public authorities;
- safeguarding the DPO from penalisation for performing their tasks;
- *subcontracting* the DPO; and
- *publication* of contact details.

Each of the above are explained further in the following.

3.1 The tasks that the DPO should perform as part of their role

Article 39 of the GDPR details specific tasks for the DPO, which can be summarised as follows:

- to provide advice to the organisation on the GDPR's requirements;
- to monitor the organisation's compliance with the GDPR[6];
- to implement awareness-raising and training for staff;
- to provide the organisation with advice on Data Protection Impact Assessments ("DPIA") and monitor their performance[7];

[6] This task may involve - identifying processing activities; analysing their compliance; and, issuing recommendations.

[7] In relation to DPIA, amongst other things, the DPO could advise on - whether or not to carry out a DPIA; what methodology to follow when carrying out a DPIA; identifying safeguards (including technical and organisational measures) that could be applied to mitigate any risks to the rights and interests of the data subjects; whether to carry out the DPIA in-house or whether to outsource it; and,

- to cooperate with the regulator; and

- to act as the regulator's point of contact.

The above are the tasks that, as a minimum, the DPO should perform according to Article 39 of the GDPR. However, the DPO's role may include other tasks to support the controller or processor's compliance arrangements to meet their obligations under the GDPR. It is a matter for the controller or processor to determine what additional tasks, if any, may be given to the DPO, taking into account their organisational structure and compliance arrangements. However, other tasks that the DPO could have and/or be involved in are:

- creating and managing a register of processing operations in accordance with Article 30 of the GDPR;

- implementing an effective data breach notification process in accordance with Articles 33 and 34 of the GDPR;

- implementing an internal data protection audit programme;

- implementing policies and procedures for "data subject right requests"[8];

- implementing data protection complaint procedures;

- complaint handling;

- identifying and managing any relevant data protection certification;

- implementing/reviewing policies and procedures in accordance with the requirements relating to data protection by design and by default; and

- developing and/or reviewing data protection related policies and procedures.

In the performance of their tasks, the GDPR requires DPOs to have due regard to the risks of the data processing. The DPO should thereby adopt a risk based approach and prioritise matters that have a higher data protection risk[9].

It is important to note that data protection compliance is a corporate responsibility of

whether or not the data protection impact assessment has been correctly carried out and whether its conclusions.

[8] Data subjects have rights to make requests under the GDPR e.g. see Articles 15, 16, 17. 18, 20, and 21.

[9] See Article 39(2) of the GDPR

the data controller, not of the DPO[10]. The DPO is not personally responsible where there is an instance of non-compliance.

3.2 The DPO's involvement in data processing operations

GDPR - Article 38(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.

The DPO should be involved in all issues relating to data protection from the earliest stage possible. The DPO is to be seen as the "go to person" within the organisation for all matters relating to the protection and processing of personal data and that they take part in relevant working groups within the organisation.

The following are examples of measures that an organisation should take to ensure that the DPO is appropriately involved:

- invite the DPO to participate regularly in meetings of senior and middle management;
- have the DPO present where decisions with data protection implications are taken, and ensure that all relevant information is passed on to him/her in a timely manner in order to allow him/her to provide adequate advice;
- always give due weight to the opinion of the DPO and in case of disagreement, document the reasons for not following the DPO's advice; and
- consult the DPO promptly in the event of a data breach or other incident.

3.3 The qualities that the DPO should have

GDPR - Article 37(5)

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.

DPOs are required to have appropriate professional qualities for the role. Organisations should use the following guidance to determine the qualities required:

[10] See Article 24(1) of the GDPR

- Expertise relative to the data processing: The level of expert knowledge required for the DPO should be determined according to the data processing operations carried out including the protection required for the personal data being processed. Factors to be considered include the complexity of the processing, the nature of the data being processed (e.g. sensitive), the amount of data being processed, and whether data is systematically transferred outside the European Union.

- Knowledge: Knowledge of national and European data protection laws and practices including the GDPR[11]. Knowledge about the relevant sector and the organisation's technical and organisational arrangements including its security and data protection needs would also be appropriate.

- Abilities: Appropriate qualities to fulfil their tasks, such as integrity and high professional ethics.

3.4 The resources that the DPO should have

GDPR - Article 38(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.

The GDPR requires organisations to support the DPO by providing the resources necessary to carry out their tasks and maintain their knowledge. Organisations should consider the following:

- Active support of the DPO's function by senior management (such as at board level).

- Sufficient time for DPOs to fulfil their duties. This is particularly important where the DPO is appointed on a part-time basis or where the employee carries out data protection in addition to other duties. Conflicting priorities could result in the DPO's duties being neglected.

- It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.

[11] A number of organisations offer courses on data protection. A list of courses known to the GRA are provided on our website (www.gra.gi/data-protection/training). However, please note that the GRA does not endorse any particular course.

- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.

- The necessary access to other services, such as human resources, legal, IT, security to be readily available to the DPO.

- Continuous training for DPOs to stay up to date with regard to developments within data protection.

- Setting up a DPO team where the size and structure of an organisation, requires it.

3.5 The independence of the DPO

GDPR - Article 38(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.

The GDPR requires DPOs to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers/processors are required to ensure that the DPO 'does not receive any instructions regarding the exercise of [his or her] tasks.' Recital 97 adds that DPOs, 'whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner'.

The DPO should always be given the opportunity to make his or her opinion clear to the controller or processor.

3.6 Preventing conflict of interests

GDPR - Article 38(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.

Controllers and processors are to ensure that there are no conflict of interests between the DPOs role and any other tasks and duties that they perform. The absence of conflict of interest is linked to the concept of the DPO working in an independent manner.

Although a DPO can carry out other functions within the organisation, it is important to note that they can only be entrusted with tasks and duties that do not interfere or give rise to conflict of interests.

Subject to the circumstances of each case, it follows that a DPO should generally not hold a position within the organisation that leads him or her to determine the purpose and means of the processing of personal data[12].

The following is some guidance on the measures that could be adopted to prevent conflict of interests:

- before designating a DPO, the controller or processor should identify the positions that would be incompatible with the function of DPO;

- draw up internal rules to avoid conflict of interests that include a general explanation about conflict of interests; and

- declare that the DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement.

3.7 Assigning a DPO for a group of undertakings or public authorities

GDPR - Article 37(2)
A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

GDPR – Article 37(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.

The GDPR allows for a group of undertakings to designate a single DPO. Equally, a single DPO can also be appointed for several public authorities or bodies.

Amongst other requirements such as having sufficient resources, the appointment of a single DPO for several organisations must comply with the following:

- Accessibility: The DPO must be accessible from each establishment. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data

[12] Examples of roles, which could create conflict of interests when shared with the DPO role are - chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of human resources or head of IT departments) 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.

subjects[13], the supervisory authority[14], but also internally within the organisation[15]. The contact details of the DPO must also be available as per Article 37(7) of the GDPR.

- Communication: The DPO must be in a position to efficiently communicate with data subjects[16] and cooperate[17] with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned.

In the context of a single DPO being appointed for several organisations, it is important to reiterate that the DPO is bound by confidentiality concerning the performance of his or her tasks[18].

3.8 Safeguarding the DPO from penalisation for performing their tasks

GDPR - Article 38(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.

Under the GDPR, organisations are not allowed to dismiss or penalise DPOs for performing their tasks. This requirement helps ensure that they act independently and enjoy sufficient protection in performing their tasks.

Penalties may take a variety of forms such as absence or delay of promotion; prevention from career advancement or denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is enough, as long as the threat is being used to penalise the DPO on grounds related to his/her activities.

[13] Article 38(4) of the GDPR states that data subjects may contact the DPO

[14] See Article 39(1)(e) of the GDPR states that the DPO shall be the point of contact for the supervisory authorities

[15] See Article 39(1)(a) of the GDPR requires the DPO to inform and advise the controller and the processor and their employees

[16] See Article 12(1) of the GDPR

[17] See Article 39(1)(d) of the GDPR

[18] See Article 38(5) of the GDPR

The GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, as a normal management rule and as it would be the case for any other employee, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for example, in cases of theft, physical, psychological or sexual harassment or similar gross misconduct).

3.9 Subcontracting the DPO

The function of the DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's/processor's organisation.

Under the circumstances when a service contract is made with an organisation or group of individuals, it is essential that each member of the organisation exercising the function of the DPO fulfils all relevant requirements set out in section 4 of the GDPR.

In circumstances where an organisation acts as the DPO on the basis of a service contract, it is recommended that clear allocation of tasks be assigned to individuals, and that a single individual within the organisation acting as the DPO is assigned as a lead contact and person 'in charge' for each client.

3.10 Sharing the contact details of the DPO

GDPR - Article 37(7)

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

The DPO will need to be easily, directly and confidentially contacted without having to contact another part of the organisation.

The contact details of the DPO should be communicated to the relevant supervisory authorities and also published so that both supervisory authorities and data subjects can contact the DPO easily. An example of relevant contact details are:

- Postal address
- Dedicated phone line
- Email address

Although it may be good practice, the published contact details need not include the name of the DPO.

Furthermore, it is advisable that the contact details of the DPO are shared throughout the organisation.

Important Note

This document is purely for guidance and aims to supplement the Article 29 Working Party's Guidelines on the Data Protection Officer[19]. The document does not constitute legal advice or legal analysis. All organisations that process data need to be aware that the GDPR will apply directly to them. The responsibility to become familiar with the GDPR and comply with its provisions from 25th May 2018 onwards therefore lies with the organisation.

Where necessary, the GRA will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR, the GDPR will take precedence.

[19] Article 29 Working Party, 'Guidelines on Data Protection Officer ('DPOs')' (13 December 2016)