# Amicus


GDPR: The Role of the Data Protection Officer

# Introduction

The GDPR comes into effect across EU States on 25 May 2018, creating a level of fear and uncertainty that may perhaps be unwarranted, given that the General Data Protection Regulation (GDPR) is just another step, albeit a firm one, in the development of the personal data protection regime within the EU. Of course, there are a number of new concepts introduced in the Regulation, particularly at the institutional level: the creation of the European Data Protection Board ('the Board'), the Data Protection Officer and the extension of the obligation to protect personal data for both controllers and processors as well as the creation of safeguards for cross border transfers. These are all measures that aim to meet a key human rights obligation: the right to privacy under Article 8 of the EU Charter and its equivalent in the ECHR.

The right to privacy and, by extension, the protection of personal data is not an absolute right, but is, rather, a restricted right, provided that any violation or encroachment on the right is lawful, necessary and proportionate. The GDPR seeks to balance commercial interests with the right to privacy under Article 8 by strengthening the rights of individuals (data subjects) through a number of measures, which include clear and explicit consent, data portability and the right to erasure and harmonising its application across the EU to avoid the difficulties and challenges that had been created by the inconsistent implementation of the earlier Directive, EU 95/46/EC.

The aims of GDPR are, therefore, no different to the earlier EU Directive: the same principles are recognised as the bedrock: lawfulness, fairness, transparency, accuracy, security, data minimisation, data kept no longer than is necessary, appropriate safeguards for transfer and respect for the rights of the data subject.

In practical terms, what this does this mean for controllers & processors? Essentially it demands not just more accountability, but demonstrable accountability, by both controllers and processors (public and private, except for national security and crime prevention and detection, each of which falls outside the GDPR) through a risk based governance/ compliance regime. Accountability under GDPR has been achieved by setting out clear responsibilities for controllers & processors, and Article 5(2) states with clarity:

*'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)'*

The GDPR defines a controller as a person (natural or legal) who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed; whereas, a processor is a person (natural or legal) who carries out processing on behalf of the controller.

Recital 74 underlines this obligation:

- Responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established.

- The controller is obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities, including the effectiveness of the measures.
- The measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons (risk based approach).

The Regulation then sets out, in some detail, the measures controllers and processors must have in place by 2018; controllers and processors will need to assess the adequacy of the measures they currently have in place to ensure compliance with GDPR, and those that have no systems or processes in place, will need to conduct a risk assessment and design their policies, processes and systems accordingly. This paper will address just one of the compliance measures: the Data Protection Officer (DPO).

The idea and concept of a DPO is not a new one; it has been introduced by EU Member States in one of 3 ways:

- Sector specific DPOs: for example, in the UK, there is a health sector-specific DPO, the Caldicott Guardian; in Finland, DPOs have been in existence for social welfare and healthcare service and in Hungary financial institutions, public utility companies and telecoms companies must appoint a DPO.

- General DPOs: for example Germany and Croatia require a DPO or both public and private sector organisations, except for very small organisations.

- Voluntary DPOs: A number of Member States opted for voluntary DPOs and these include Netherlands, Luxembourg, Poland and Sweden.

The basic framework for DPO is set out in Section 4 (Articles 37 – 39) of the GDPR sets and now makes it mandatory for a certain category of controllers & processors to put in place DPOs. Article 37(4) gives Member States some latitude in extending the categories of organisations that must have DPOs, or any additional requirements.

## Who is Required to Have a DPO?

Under Article 37(1), the following are required to have a DPO:

1. All public authorities and bodies except courts acting in their judicial capacity (not defined by GDPR – it is a matter of national law. It should, however, also cover private companies performing a public function);
2. All other controllers and processors whose core activity is regular and systematic monitoring of individuals on a large scale (emphasis added); and
3. All controllers and processors that process special categories of personal data on a large scale or personal data (criminal convictions and offences).

In all other cases, a DPO is not required as a matter of law (i.e. the Regulation); however, the A29 Working Party (WP) recommends that consideration be given to the establishment of a DPO in any event. Where this occurs, the voluntary appointment of the DPO must for all intents and purposes meet the GDPR requirements: the fact that a DPO is mandated or voluntary is not relevant.

The various terms, in particular, under Article 37(1)(b) and (c) are not defined by the GDPR but some guidance has been offered by the Article 29 Working Party (WP) to mean as follows:

*'core activity'* is the primary function or an integral part of an entity's function e.g. hospitals whose core function is health care, but which nevertheless process data, or private company conducting surveillance of shopping centres – in the latter it is its primary function, whereas in the former, it is an integral function;

*'large scale'* : according to Recital 91 and the Article 29 WP organisations should use the following guidance by way of a working 'formula' in order to decide if it collects or processes data on a large scale:

1. Assess the number of data subjects concerned, which may either be a specific number or as a proportion of the relevant population;
2. The volume of data and/or the range of different data items being processed;
3. The duration, or permanence, of the data processing activity;
4. The geographical extent of the processing activity

The Article 29WP gives some obvious examples of *'large scale':* hospitals (patient data), travel cards, personal data for behavioural advertising by a search engine and store loyalty cards. Given the somewhat vague description, the threshold for amounts to *'large scale'* will be kept under review by the Article 29 WP as the GDPR embeds.

*'regular and systematic'*: Recital 24 (which is primarily aimed at extending the GDPR to controllers and processors not based in the EU) provides a partial steer in the following terms:

*'it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.'*

In short, it is all forms of tracking and profiling on the internet (or otherwise), including that for the purposes of behavioural advertising.

Examples of activities that fall within the definition of 'regular and systematic' include:

- operating a telecommunications network;
- providing telecommunications services;
- email retargeting;
- 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, for example, by mobile apps;
- loyalty programs;
- behavioural advertising;
- monitoring of wellness, fitness and health data via wearable devices;
- closed circuit television;
- connected devices e.g. smart meters, smart cars, home automation, etc.

**Practical note for organisations**

At the outset, an organisation will need to decide if it must appoint a DPO; in order to do so, it must assess:

1. If the organisation falls within the 3 categories set out in Article 37(1); if it does, a DPO is required.

2. If it is not caught by Article 37(1), it will need to check if its national law requires the appointment of a DPO in any event; if so, then one should be appointed.

3. If none of the two criteria above apply, it should nevertheless consider whether a DPO should be appointed on a voluntary basis. If an organisation comes to the view, taking into account the nature, scope and risks of the organisation, that a DPO is not required and should not be appointed, the decision (including reasons) must be fully documented and recorded.

## Skills and Expertise of the DPO

For obvious reasons, the GDPR cannot set out the qualifications for a DPO; it is a matter for each organisation (controller and/or processor) to appoint an individual (internal or external) who is well suited and qualified to carry out the functions and discharge the responsibility that goes with it.

The key function of the DPO is to monitor implementation of the GDPR and create a culture of GDPR compliance across the organisation; it, therefore, follows that the DPO should be familiar with organisation (its work and technical structures), data subjects, terminology etc., and be capable of implementing GDPR (direct reporting and access to senior management)

Article 37(5) provides that the DPO '*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'.

A DPO should have necessary expertise which is commensurate with the sensitivity, complexity, scale and amount of data an organisation processes in order to be capable of understanding the data protection issues within the organisation. According to the Article 29 WP, the DPO (at a minimum) must have an understanding of:

- national and European data protection laws and practices;
- an in-depth understanding of the GDPR;
- the business sector and of the organisation of the controller;
- the processing operations including information systems, data security and data protection needs of the controller, and in the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.

**Practical note for organisations**

Once a decision has been made that a DPO should be appointed (mandatory or voluntary), organisations may wish to consider:

1. Should the DPO be an internal or external (company or individual) post?
2. Who will appoint the DPO? Controller, processor or both.
3. Number of DPOs: depending on the size and structure of its operations, a single data protection officer may be appointed to act for a group of companies or for a group of public authorities provided the DPO is 'easily accessible from each establishment' to the data subjects, the supervisory authorities and internally within the organisation.
4. Location of the DPO: as the GDPR is concerned with safeguarding the interests of EU citizens, it would be both logical and sensible for the DPO to be located within the EU even if controller and processor are located elsewhere.
5. Provide the details of the DPO (name and contact details) to the national supervisory authority: Article 37(7).
6. Publish the contact details of the DPO on the organisation's website. Although there is no requirement to publish the name of the DPO, it should be considered particularly for ease of access by data subjects.

Remember!
Although DPOs will be at the heart of the implementation of GDPR, the controllers and processors remain entirely responsible for data handling under Article 24(1).

## Position of the DPO within the organisation

Article 38(1) requires the controller and the processor to ensure that the DPO is '*involved, properly and in a timely manner, in all issues which relate to the protection of personal data'*. This includes:

- Mandatory early engagement with DPO on all data protection issues.
- In relation to data protection impact assessments (DPIAs) the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.
- DPO are included as key personnel in any working groups, participate in meetings for middle and senior management etc. relating to DP issues.
- Where the advice of DPO is not followed, a detailed record should be made setting out the reasons for not doing so
- In the event of a data breach, the DPO must be notified immediately.

## Resources for DPO

Article 38(2) requires the organisation to support its DPO by '*providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.'*

The DPO must, therefore, be provided with sufficient resources to carry out the function, tasks and responsibilities of the DPO, which include:

- Adequate resources: financial, infrastructure (premises, facilities, equipment) and staff;
- Active support for DPO at the most senior level (Board etc.);
- Sufficient time should be given to DPO to carry out the functions and tasks, particularly where the DPO has another role in the organisation, or if it a part-time function or dealt with by an external individual/entity;
- It is important that the DPO profile and contact details are made known within the organisation;
- DPO should have easy and unhindered access to other departments (IT, legal etc.) that are relevant to DPO function;
- Regular and continuous training for DPO;
- Where necessary (e.g. large organisation) set up a DPO team with clear lines of responsibility and appoint a lead DPO.

In addition, Article 38(3) requires organisations to put in place safeguards and guarantees for DPO. These are:

- A sufficient degree of autonomy from controller and/or processor in carrying out DPO duties;
- Protection from dismissal or penalty in performance of the DPO tasks.

- Direct reporting to the highest management level within the organisation (controller/ processor) in order to ensure GDPR compliance.

As the DPO may perform other functions within an organisation, a safeguard that is of particular significance is the need for controllers or processors to ensure that '*any such tasks and duties do not result in a conflict of interests*' (Article 38(6))**.** In practice, this means that a DPO should not hold a position within the organisation (controller) that is required to decide the purpose and means of data collection and processing; to do so puts the DPO in a difficult position and is a clear 'conflict of interest'. Ideally, therefore, a DPO should not hold senior positions (e.g. chief executive, head of marketing department, Head of Human Resources etc.) which are likely to put the DPO in conflict with the duties and functions of DPO.

The Article 29 WP has given some steer and suggests the following approach based on good practice:

- Identify the positions which would be incompatible with the function of DPO.
- Draw up internal rules and guidance on COI (this should be the case in any event as part of the governance framework).
- Make it known that the DPO has no conflict of interests which also helps to raise wider awareness of the requirement.
- Ensure that any notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests.
- Be alive to real or apparent COI issues, particularly when considering the appointment of an external DPO.

## What are the functions of the DPO?

Having established a DPO, an organisation will then need to decide the tasks and functions of the DPO. Article 39 identifies 5 key tasks (as a minimum); however, it is a matter for each organisation to decide if the tasks of the DPO should go beyond those 5 main tasks.

The key tasks include:

1. Inform and advise the controller or processor (and their employees) of their obligations under GDPR, national law and the law of other Member States;

2. Monitor compliance:
    a. with GDPR, other Union and Member State data protection provisions
    b. of the organisation's policies & procedures in relation to protection of personal data, training and awareness raising programmes in place of staff responsible for processing, the allocation of responsibilities and audits.

3. Provide advice to controllers on Data Protection Impact Assessments (DPIA) and monitor its performance pursuant to Article 35. Although strictly a task for the controller, the Article 29 WP recommends that a controller should seek the advice of

the DPO in the following instances (in any event the role of DPO in DPIAs should be set out clearly):

a. whether or not to carry out a DPIA;
b. what methodology to follow when carrying out a DPIA;
c. whether to carry out the DPIA in-house or whether to outsource it;
d. what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;
e. 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.

4. Co-operate with the supervisory authority.

5. Act as the main contact point for the supervisory authority for prior consultation in relation to DPIA.

In addition, the DPO may also:

1. Act as the main contact point between the various stakeholders (within the organisation and data subjects).

2. Assist in providing accountability: Although it is the duty of the controller/processor to maintain records of the processing activities under Article 30, there is nothing that prevents a controller/processor from assigning this to the DPO. In a large organisation, this may also help the DPO with the monitoring function (and address any shortcomings/gaps as they arise) as well give the controller, processor or supervisory authority an overview of all the personal data processing activities being carried out.

## Penalties

Under Article 83(4), a breach of Section 4 (Articles 37 – 39) attracts an administrative fine of up to EUR 10,000,000, or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

## Concluding Comments

Data collection, storing and processing are today an integral part of any organisation (public or private), with the need to protect robustly the personal data of data subjects having come into sharp focus in recent times through the various cyber security breaches and hacks. Compliance with GDPR is just another step towards meeting that obligation and ensuring the right to privacy is maintained.

## Practical note for organisations

Some steps organisations should consider (on a wider basis) are:

1. Have a clear understanding of your operations and how it interacts with GDPR.
2. Identify the measures that you have in place and their adequacy.
3. Identify the new measures, such as DPO, that need to be put in place to ensure compliance and what steps you need to take – they may not be as onerous and burdensome as you think! The ICO has drawn up a list of 12 steps to assist organisations in the UK, some of which you may find useful.
4. Identify the information you deal with: does it include 'sensitive data'
5. Different measures of protection may be required across the same organisation (e.g. HR may handle 'sensitive data', whereas marketing may hold data on clients etc.).
6. Do the operations go beyond EU/EEA? If so, data transfer mechanisms need to be addressed.
7. Have in place appropriate security and systems across the organisation.
8. Need to train staff (including temporary staff) to not only understand the legislative framework, but also the human rights framework that underpins it (this helps to make it more personal and meaningful to the staff as their own personal data is also held by other controllers and processors).
9. At a senior and board level, it is valuable to conduct 'crisis avoidance' exercises in order to work through the potential consequences of failure for both the individual and the wider organisation (including financial penalties, market loss and reputational tarnishing).

---

# Arvinder Sambei, Director

T: +44 7949 553060
E: a.sambei@amicuslegalconsultants.com

Arvinder Sambei is a former Senior Crown Prosecutor with the Crown Prosecution Service of England & Wales with established experience and expertise spanning various areas involving criminal justice. She was engaged in numerous high-profile extradition, counter-terrorism, transnational and war crimes cases in the UK.

Arvinder was the Head of the Criminal Law Section at the Commonwealth Secretariat from 2005 to 2008, where she was primarily responsible for the daily running of the Section and the design and delivery of training programs/courses. Prior to that Arvinder was the Legal Adviser to the Permanent Joint Headquarters (PJHQ) providing real-time operational advice and guidance to Iraq and Afghanistan theatre forces.

Arvinder has published widely and in addition to a wide range of papers, she is the co-author of the *Extradition Law Handbook* (Oxford University Press, 2005) and *Counter-Terrorism Law & Practice: An International Handbook* (Oxford University Press 2009). She was also a contributing author to *Extradition and Mutual Legal Assistance Handbook* (Oxford University Press, 2010).

Arvinder is an experienced facilitator and trainer, and has been engaged in designing & delivering workshops for a number of years. She facilitates and leads training workshops on behalf of international organisations, law firms and the private sector on anti-corruption, AML/CFT, counter-terrorism, dawn raids, and corporate governance.