Guidelines on Data Protection Officers Adopted by Article 29 Data Protection Working Party

By Francesca Petronio, Marilena Hyeraci & Sara Schiuma

Introduction

On 13 December 2016, the Article 29 Data Protection Working Party¹ ("WP29") published three sets of guidelines among which its "Guidelines on Data Protection Officers" ("Guidelines"), where it specifically focused on the new subject introduced by the "Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" ("GDPR")², i.e. the Data Protection Officer ("DPO")³.

The GDPR entered into force on 25 May 2016 and its provisions will be directly applicable in all Member States from 25 May 2018, when it will replace national data protection laws⁴.

From a practical point of view, this means that the countdown for implementation has started. On the one hand, Member States have a two-year transition period to adapt their national legal systems to the requirements set forth by the Regulation; on the other hand, European companies and data subjects must start considering how to adjust their existing practices in order to comply with the new European rules coming their way.

In such a framework, experts have been working on possible ways to implement the Regulation’s provisions and to sketch guidelines and best practices.

The Guidelines of the WP29 aim at clarifying and shedding light on the relevant provisions of the GDPR in order to help controllers and processors to comply with the law, as well as to assist DPOs in their role.

Overview on DPO Provisions

The DPO is a brand new subject within the privacy legal framework of most European Member States. The GDPR identifies the DPO as a key player in the new data governance system and strictly regulates its appointment, position and tasks. The DPO’s role is considered important to the development of a data protection culture as well as in order to implement some essential elements of the GDPR, such as the principles of data processing, data subjects’ rights, data protection by design and by default, records of processing activities, security of processing, as well as notification and communication of data breaches. In other words, DPOs should act as intermediaries between relevant stakeholders (e.g., supervisory authorities, data subjects, and business units within the organization).

According to the GDPR⁵, the DPO’s appointment is mandatory whenever: (i) the processing is carried out by a public authority or body, except for Courts acting in their judicial capacity; (ii) 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 (iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of data.

Moreover, EU or Member States laws may require the designation of DPOs in further cases as well.

WP29 Guidelines

The WP29 Guidelines cover three main areas, namely designation, position and tasks of the DPO.

DPO’s Designation

Besides situations where they are clearly not required to appoint a DPO, WP29 recommends organizations which do not intend to designate one to document the internal analysis carried out to determine whether or not such a subject is to be nominated, in order to be able to demonstrate that the relevant circumstances have been properly considered.

If an organization does not expressly require appointing a DPO but, nonetheless, decides to do so on a voluntary basis, it will be subject to the same requirements and rules concerning the DPO’s designation, position and tasks expressly set forth by the GDPR.

It follows that, given the special status afforded to DPOs by the GDPR, if an organization chooses not to designate a DPO but instead decides to employ staff or outside consultants with tasks relating to the protection of personal data, it is strongly recommended to be clear as to whether such persons are DPOs or not: in other words, every organization should clearly state (e.g., in internal as well as external communications) that the title of such individuals or consultants is not “DPO.”

The Guidelines provide some useful indications to identify those cases where the appointment of a DPO is mandatory.

For instance, the Regulation does not define the notion of the “public authority or body” that has to appoint a DPO. WP29 suggests it should be determined under national laws. Therefore, such a term will typically include not only national, regional and local authorities, but also a range of other bodies governed by public law.

The Guidelines stress that public tasks are frequently carried out — and public authority exercised — not only by public authorities, but also by other natural or legal persons governed by public or private law, e.g., in sectors such as public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.

Even though there is no obligation in such cases, WP29 suggests, as a good practice, a) that private organizations carrying out public tasks or exercising public authority should designate a DPO, and b) that the DPO’s activity should also cover all processing operations carried out by the organization, including those not related to the performance of a public task or exercise of official duty (e.g., the management of employee database).

As mentioned above, the GDPR also requires the appointment of a DPO whenever the core activities of the controller or processor concerns: (1) processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or (2) processing on a large scale of special categories of data.
Thus, the identification of the core activities of the controller or the processor is crucial in order to determine whether the appointment of a DPO is mandatory. In this respect, WP29 stresses the importance of encompassing in the notion of "core activities" also those activities where the processing of data forms a fundamental part of the controller's or processor's performance (e.g., hospitals cannot provide healthcare safely and effectively without processing patients' health records; processing these data should be considered among hospitals’ core activities, thus hospitals should designate DPOs).

The Guidelines list some relevant factors which must be taken into consideration in determining what constitutes large-scale, e.g., the number of data subjects concerned; the volume of data and the range of different data processed; the duration, or permanence, of the data processing activity; or the geographical extent of the processing activity7.

Eventually, the last case of mandatory designation concerns "regular and systematic monitoring" and WP29 gives several useful examples to determine the scope of the rule8.

With regard to DPOs’ expertise and skills, the Regulation does not identify which professional qualities should be considered when designating the DPO. WP29 recommends DPOs to have expertise in national and European data protection laws and practices as well as an in-depth understanding of the GDPR; knowledge of the controller's business sector and organization is also an asset. Possibly, DPOs should also have a sufficient understanding of the processing operations carried out, as well as of the information systems.

As for the level of expertise, it is not strictly defined but it must be adequate to the sensitivity, complexity and amount of data processed by the organization. For example, where a data processing activity is particularly complex, or a large amount of sensitive data is involved, WP29 considers it important for the DPO to have a higher level of expertise and support.

With regard to the DPO's ability to fulfill its tasks, in WP29's opinion, it should be interpreted as both referring to its personal qualities and knowledge, and also to its position within the organization. Personal qualities should include, for instance, integrity and high professional ethics.

**DPO's Position**

With regard to the position of DPOs, the GDPR focuses on three main areas, namely: (i) their independence within the organization, (ii) their involvement in all issues relating to the protection of personal data, and (iii) the resources that they should be provided with to perform their activities.

The GDPR defines some basic guarantees to ensure DPOs are independent in the performance of their tasks, specifying that they should not receive instructions concerning the exercise of such tasks. In WP29's advice, this means that DPOs must neither be guided on how to deal with a matter, nor suggested to take a certain view of an issue related to data protection law, e.g., a particular interpretation of the law.

Moreover, the GDPR takes into account potential conflicts of interest of those DPOs that also fulfill other tasks and duties within the organization. On a case-by-case reasoning, it is up to the organization to ensure that “any such tasks and duties do not result in a conflict of interests.”9 In other words, DPOs are allowed to perform other functions, but they can only be entrusted with different tasks and duties provided that these do not give rise to conflicts of interest.

As a rule of thumb, WP29 suggests that controllers and processors identify the positions incompatible with the DPO's functions and draw up internal rules to avoid conflicts of interest. For
instance, according to the Guidelines, conflicting positions may include, not only senior management positions (such as CEO, COO, CFO, head of marketing department, head of human resources, head of IT) but also other subjects operating in the organizational structure, if such positions or roles lead to the determination of purposes and means of processing of personal data.

As per the DPO’s involvement in issues relating to the protection of personal data, the GDPR states that controllers and processors should ensure that the DPO be “involved, properly and in a timely manner, in all issues which relate to the protection of personal data.” In this respect, WP29 highlights that a crucial point is the DPO’s involvement in all issues relating to data protection from the earliest stage possible.

In compliance with such provisions, from a more practical perspective, WP29 recommends that the DPO be a part of the working groups dealing with data protection issues, as well as a discussion partner on such topics within the organization. According to WP29, the preferable involvement can be achieved by ensuring, for example, that the DPO is invited to participate in meetings of senior and middle management, that it is present when decisions with data protection implications are taken, and that it is consulted without delay once a data breach or another incident has occurred.

Furthermore, Article 38 GDPR states that organizations should support their DPOs by providing them with access to personal data and processing operation. The Guidelines highlight that such a support necessarily involves, inter alia, the backing of the DPO’s function by senior management, an adequate support in terms of financial resources, infrastructure and staff—where appropriate—as well as continuous training to maintain its knowledge.

Resources to be given to the DPO shall be determined on the basis of the processing operations carried out by the organization, in order to ensure the effectiveness of the data protection function. In other words, the key point is that the more complex and sensitive the processing operations, the more resources must be given to the DPO.

**DPO’s Tasks**

The Guidelines clarify the tasks to be performed by DPOs with regard to three main areas of activity.

The first area concerns the DPO’s responsibilities in monitoring compliance with data protection laws; in this respect, the Regulation specifically entrusts the DPO with the duty to monitor compliance with GDPR provisions, and Recital 97 further specifies that the DPO “should assist the controller or the processor to monitor internal compliance with this Regulation”.

WP29 suggests that, as part of such a duty, DPOs may, in particular: collect information to identify processing activities; analyze and check the compliance of processing activities; and inform, advise and issue recommendations to the controller or the processor.

The GDPR also establishes the DPO’s role in carrying out data protection impact assessment (“DPIA”). Article 35 specifically requires that the controller “shall seek advice” of the DPO when carrying out a DPIA and WP29 expressly recommends the controller to do so with regard to the following issues: whether or not to carry out a DPIA and what methodology to follow; whether to carry it out in-house or to outsource it; what safeguards (including technical and organizational measures) to apply to soften the risks to the rights and interests of the data subjects; whether or not the DPIA has been correctly carried out and whether its conclusions are in compliance with the GDPR.
In case of disagreement between the controller and the DPO, the DPIA documentation should specifically justify in writing why the DPO’s advice has not been taken into consideration.

Lastly, DPOs also have a role in record-keeping activities, as a support for controllers or processors. While the controller or the processor 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,” Article 39 sets forth some duties that DPOs should carry out in terms of counseling, advising, and supervisory activities related to record-keeping. In this respect, nothing prevents controllers or processors from assigning such a task to the DPO under the responsibility of the controller. Indeed, the Guidelines recall how under many national laws, DPOs are already entitled to create inventories and hold registers of processing operations based on information provided by the various departments in their organizations.

In light of the above, the introduction of such a new subject will cause considerable compliance problems within the organizations.

For example, a practical consequence of appointing a DPO is the development of new communication flows and, thus, the need to properly regulate and coordinate the flows of information between DPOs, other privacy subjects and corporations’ bodies.

Conclusions
As mentioned above, the GDPR will be directly applicable within the EU from 25 May 2018.

It follows that national legislators, companies, professionals and market operators must get ready to comply with this new data protection instrument.

In such a framework, best practices and guidelines constitute a great support for market operators. Besides such Guidelines on DPOs, WP29 is working on further sets of guidelines on different topics of the GDPR.

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings Milan lawyers:

Francesca Petronio 39.02.30411.226 francescapetronio@paulhastings.com
Marilena Hyeraci 39.02.30414.222 marilenahyeraci@paulhastings.com

1 Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

2 The GDPR repeals the 20-year-old “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”.

3 Besides its Guidelines on DPO, WP29 also issued its “Guidelines on the right to data portability” and “Guidelines for identifying a controller or processor’s lead supervisory authority”.

4 Until 25 May 2018, Italian Legislative Decree n. 196/2003 (known as “Data Protection Code”) will still apply in Italy.

5 Article 37 GDPR.

6 In particular, requirements under Article 37, Article 38 and Article 39 GDPR will apply.
In WP29's view, large scale processing includes: processing of travel data concerning a city's public transport system (e.g., tracking via travel cards); processing of real time geo-location data of customers of international fast food chains for statistical purposes; processing of customer data in the regular course of business by an insurance company or a bank; processing of personal data for behavioral advertising by a search engine; processing of data (content, traffic, location) by telephone or internet service providers. On the contrary, two clear cases that do not fall in this category are 1) processing of patient data by an individual physician, or 2) processing of personal data relating to criminal convictions and offences by an individual lawyer.

Literally, WP29 interprets "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. Also, WP29 interprets "systematic" as meaning one or more of the following: occurring according to a system; pre-arranged, organized or methodical; taking place as part of a general plan for data collection; carried out as part of a strategy. Activities that are likely to require the appointment of a DPO are, among others: operating a telecommunications network or providing telecommunications services; email retargeting; 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); processing related to loyalty programs; behavioral advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; and connected devices (e.g., smart meters, smart cars, home automation).

Article 38(6) GDPR.

Article 38 GDPR.

Article 39(1)(b) GDPR.