The Article 29 Working Party
JUST-ARTICLE29WP-SEC@ec.europa.eu
presidenceg29@cnil.fr
cc. The Dutch Data Protection Authority

Re: Comments on the Guidelines on Data Protection Officers (WP 243)

The Hague, January 31, 2017.

Dear Madams, Sirs,

The Dutch Data Protection Officers Association (NGFG) welcomes the opportunity to provide feedback on the Guidelines on Data Protection Officers of December 13, 2016 (WP 243). The guidelines form an important means for interpretation of articles 37, 38 and 39 of the GDPR. The NGFG is satisfied with the purpose and general content of the Guidelines and welcomes their swift adoption and consistent roll-out across the EU.

However, the NGFG would like to provide you with some suggestions for additions and changes, which may improve the clarity of the Guidelines, the acceptance of the DPO role and the proper functioning of the individuals that will be taking up that role.

We believe that the DPO plays a key role in ensuring compliance with the GDPR and other privacy and data protection legislation. Research by order of the Dutch government on compliance with current data protection law in practice has shown that organizations that do have a DPO are considerably more likely to be compliant than organizations that don't have a DPO. Therefore, the NGFG believes that it is of the utmost importance that the Guidelines not only provide the legal interpretation of the DPO-related parts of the GDPR, but also promotes the benefits of having a DPO.

We welcome the fact that the purpose of the guidelines is not only to of clarify the relevant provisions in the GDPR, but also to assist the DPO's in their role. We would like to add to the initiative of the guidelines and aid its purposes by submitting the following comments, corrections, and recommendations.

The Annex details our main points of concern and our recommendations.
They cover specifically:

I. the relationship between a DPO and a DPA.
II. the appointment of a DPO, and
III. a DPO's requirement for independence.

Kind regards,

mr. J. de Zeeuw
Chair NGFG

ANNEX

I. THE RELATIONSHIP BETWEEN A DPO AND DPA.

The Guidelines must clarify the relationship between the DPO and the DPA.

Key problems arise surrounding the difference in tasks, the enlisting of the DPO, and the need for consultation.

Clarifications needed:

1 Clarify the DPO's and DPA's respective tasks of monitoring compliance and application of the GDPR vis-à-vis the controller/processor;
2 Clarify when consultation between the DPO and the DPA is "appropriate" (Art. 39(1)(e));
3 Clarify what is expected after the controller/processor notifies the DPA of the enlistment of a DPO.

1. **Clarify the DPO's and DPA's respective tasks of monitoring compliance and application of the GDPR vis-à-vis the controller/processor.**
   The GDPR tasks the DPO with the "monitoring of compliance" with the GDPR (art. 39(1)(b)); the Supervisory Authorities are tasked with the "monitoring of application" of the GDPR (art. 51(1)). The Guidelines should clarify the difference between these terms and the respective roles of the DPO and the DPA vis-à-vis the controller/processor. E.g., the Dutch Data Protection Authority recognizes the "smooth cooperation" between a DPO and a Supervisory Authority, thus suggesting that the DPA will show restraint in investigating, monitoring and auditing an organization which has appointed a DPO and recognizing the DPO as the primary supervisor of a controller/processor.

   Furthermore, the Guidelines should address the course of action in case of a dispute between the DPO and the DPA. E.g., whose opinion should be leading? Should a DPO and DPA notify each other in case of non-compliance and irregularities? Also, both the DPO and the DPA have been tasked by the GDPR to deal with complaints. Is the DPA required to forward a complaint to the DPO or vice versa? Or should they deal with a complaint themselves? The Guidelines should make clear how the DPO and the DPA cooperate with each other.

2. **Clarify when consultation between the DPO and the DPA is deemed "appropriate" (Art. 39(1)(e)).**
   In what situations is consultation between the DPO and the DPA appropriate? The NGFG would expect the Guidelines to provide examples clarifying this question. Also, does the DPA have an obligation to help DPOs seeking guidance? Generally, what obligations do DPA's have towards DPOs's? The NGFG believes the guidelines should address these uncertainties.

3. **Clarify what is expected after the controller/processor notifies the DPA of the enlistment of a DPO.**
   After the DPA has been notified of the installation of the DPO, should the data of that DPO be kept in a (public) register by the DPA? Should organisations notify the DPA when a DPO is no longer in office? What criteria should the DPA use to determine whether the details supplied are those of a DPO as meant in the GDPR? This question is especially important in case a DPA keeps a register of all DPOs.

II. THE APPOINTMENT OF A DPO

The criteria and context of appointment are insufficiently made clear.

Key problems arise surrounding the voluntary appointment of a DPO, requirements for appointment, the span of control, and the external DPO.

Clarifications needed:

1 Provide more guidance on 'large scale'
2 Encourage the appointment of voluntary DPO's;
3 Explain when a voluntary DPO can use the designation 'DPO';
4 Explain how a controller/processor could ensure the appropriateness of a DPO as a data protection measure for the organisation;
5 Clarify the rules regarding the appointment of an external DPO.

1. **Provide more guidance on 'large scale'**
   Since the Guidelines have been published, the one thing that has been heavily criticized by experts in the field is the lack of clarity about what 'large scale' actually means. Given the fact that violation of article 37 GDPR carries a potential fine of 10 million euro or 2% of annual turnover, it is unacceptable to leave this issue undetermined. Although the NGFG understands that hard criteria are undesirable for various reasons, the Guidelines should provide a plethora of examples of what constitutes large scale and what doesn't.

2. **Encouraging the appointment of voluntary DPO's.**
   The Guidelines encourage the voluntary appointment of a DPO, but fail to provide pointers to the DPA's as to how to do this. The Guidelines should provide examples of situations in which the appointment of a DPO is recommended. The Guidelines also should explain the benefits of having a voluntary DPO, such as a likely higher degree of compliance with the GDPR and having an expert advisor at hand. The NGFG asks you to consider to recommend DPA's to take an attitude of restraint when it comes to supervising controller/processors, which have appointed a DPO, thus promoting the appointment of DPO's even in situations where none is required.

3. **Explain when a voluntary appointed DPO can use the designation 'DPO'.**
   There are many experts in the field who carry various job titles, such as privacy officer, privacy manager or privacy lead. Such job titles may be found in organizations which do not need to appoint a DPO. Nevertheless, they play an important role in the protection of personal data. It should therefore be clear under what circumstances the people carrying such job titles should be considered a DPO, including all the tasks, powers and protection that a DPO carries. Although the NGFG believes that the title DPO should be used where possible, the NGFG does not believe that anybody who does not carry that title, but who carries out the tasks stated in article 39 GDPR should not be considered a DPO under art. 37 GDPR.

   The Guidelines should make crystal clear what constitutes a DPO and what doesn't, considering the fact that the designation of a DPO has legal effects, such as protection against unfair dismissal. For instance, if a person fulfils all the criteria in article 37 to 39, should that person be considered a DPO even when that person does not carry the title? Or if such person is meant to be the DPO, but the controller/processor has failed to register him/her with the DPA? Also, when someone's contact details have been mentioned in the privacy notice as point of contact for privacy questions, should that person be considered the DPO even when that person does not carry the title DPO? In any case, the controller/processor should not be able to change their mind at the detriment of the (perceived) DPO.

   And last but not least, do articles 37 to 39 GDPR cease to apply when the controller/processor decides to terminate the voluntary appointment the DPO? Is that even possible? What does that mean for the DPO's employment protection?

4. **Explain how a controller/processor could ensure the appropriateness of a DPO as a data protection measure for the organisation.**
   Data protection measures should be appropriate, taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons (art. 24 (1) GDPR). Therefore, it is insufficient to make the function of a DPO dependent on the scale and structure of the organisation. A realistic and thorough analysis of the circumstances and risks is required. Regardless of size and structure, an organization which appoints a DPO must allocate sufficient resources to the DPO based on those risks. This is important to facilitate the tasks of the DPO and to recognize his/her job. The Guidelines should include some criteria to determine when such resources are sufficient considering the tasks of the DPO, including monitoring. This would also help DPO's in procuring the necessary resources from the controller/processor.

   Furthermore, the Guidelines should recognize that when some organizations consist of multiple parts, which operate relatively autonomous from each other, or where multiple controllers/processors are appointing the same DPO, the span of control of the DPO should not be too large. The NGFG believes that a DPO with too large a span of control cannot carry out his/her tasks effectively. Especially in view of the supervisory task. Therefore, controllers/processors should not turn to the option mentioned in art. 37(2) GDPR too easily. A risk-based appointment of a DPO, or even multiple (assistant-)DPO's, in such organizations would prevent the span of control of the DPO from becoming too large. Our recommendation is to add this to paragraph 2.3.

5. **Clarify the rules regarding the appointment of an external DPO.**
The conditions discussed at point 4 of this paragraph also apply to external DPO's, and should be explicitly mentioned in paragraph 2.3 of the Guidelines. There is no difference in conditions between an external and internal DPO, and the Guidelines should leave no room for any such difference. Therefore, paragraph 2.4 should also apply to external DPO's, even where the DPO service is performed by an organization instead of an individual.

Clarifications are also necessary on the following questions:

- Can an external DPO be a legal entity of must it always be a natural person?
- Is the account manager of the external DPO service provider the only DPO supported by a team of non-DPO's, or should each of the team members also be considered a DPO (with all privileges and protections attached)?
- In case of a DPO-team: who's contact details must be published and communicated to the DPA?
- How should such DPO service provider avoid situations in which a conflict of interests may arise?
- Should the DPO function be separated by Chinese walls from the advisory part of the service provider, which carries out DPIA's or advises on the design of the data processing?

Finally, clarification is needed on how the privileges of DPO, like independence, presence at all affairs regarding data protection, resources, and ability to report to the highest management level, are guaranteed for external DPO's. And whether they are applicable on all the members of a DPO-team.

III. FUNCTION/ INDEPENDENCE OF A DPO

The guidelines fail to ensure the independent supervisory role of a DPO.

Key problems arise surrounding the distinction between the advisory and the monitoring role, the compatibility of other tasks and functions, and the proactive role of a DPO.

Clarifications needed:

1 Emphasise that the monitoring role of the DPO is the DPO's primary responsibility, and that it can only partially be reconciled with executing other tasks that the GDPR requires of a controller/processor;
2 Discuss how to prevent a conflict of the monitoring and the advisory role of the DPO;
3 Clarify which functions and tasks constitute a conflict of interest of the DPO.

1. **Emphasise that the monitoring role of the DPO is the DPO's primary responsibility, and that it can only partially be reconciled with executing other tasks that the GDPR requires of a controller/processor.**
   Many organizations see the DPO as somebody, who ensures that the organization complies with the GDPR. Consequently, they shift activities related to compliance to the DPO. However, the NGFG believes that the controller should not shift part of its duties under the GDPR to the DPO, as this would bring the DPO in a position where a conflict of interest may arise and limits the time available to the DPO to fulfil his/her tasks under article 39 GDPR. Therefore, the Guidelines should state that, to ensure the effective monitoring of compliance, the DPO cannot, or only marginally, be tasked with tasks that fall to the controller/processor under to the GDPR, such as the execution of DPIA's. No DPO should be tasked with operational responsibilities that requires his/her to supervise their own compliance with the GDPR. The NGFG believes that the only tasks of the controller/processor that may be shifted to the DPO is keeping the register of processing activities under art. 30 GDPR, since it directly contributes to the tasks of the DPO under the GDPR.

2. **Discuss how to prevent a conflict of the monitoring and the advisory role of the DPO.**
   Research among the members of the NGFG has shown that most DPO's spend the largest part of their time in advising the controller/processor about the interpretation of the law (21%). Various monitoring tasks, such as compliance checks, investigation of data breaches and dealing with complaints take up 8% of a DPO's time each. The rest of the time is spent on tasks such as training and awareness (22%), processor agreements (9%), drafting privacy policies (6%) and executing DPIA's (4%).[1]

   Reconciliation of an advisory role with the monitoring tasks of a DPO is difficult. How does a DPO prevent a conflict of interest in these two roles. In this context, we would like to point to the text of the current Dutch Personal Data Protection Act, which requires that the Dutch Data Protection Authority puts into place safeguards, which prevent the entanglement of its supervisory, advisory and enforcement tasks (art 56 par. 3 PDPA). Obviously, a DPO cannot put in place similar safeguards, except when he/she would head a department which consists of an advisory part and a monitoring part. The Guidelines should discuss strategies a DPO could use to avoid a conflict of interest between the two roles.

3. **Clarify which functions and tasks constitute a conflict of interest of the DPO.**
   It's a reality that most DPO's perform other roles in the organisation. Research among the NGFG membership has shown that 65% of the DPO's have other duties which require more than 50% of their available time. Moreover, 90% of all DPO's in small organizations perform the tasks of DPO as a secondary function. Not only may such combination of duties interfere with the adequate functioning of the DPO, it may also lead to a conflict of interests.

   Given that most DPO's perform tasks of a legal nature (e.g., as in-house legal counsel) and many DPO's perform tasks related to IT (e.g., information security), it is essential to clarify further which functions in the organization are irreconcilable with the function of the DPO. For instance, is it possible that an in-house legal counsel drafts data processor agreements *and* is the DPO? Is it possible that an information security manager takes decisions relating to information security *and* is the DPO?

[1] J. Terstegge, *Insight in the DPO*, Privacy & Compliance 2013, nr. 4/5 (available in Dutch only).

It is essential that the Guidelines provide more guidance on the irreconcilability of various functions in the organization, especially the ones mentioned above. The NGFG believes this subject is too important to be dealt with in a mere footnote. The Guidelines should clearly specify that as soon as a DPO (co-)determines purposes and means of a data processing, or is otherwise tasked with responsibilities that fall to the controller/processor, he/she will be unable to effectively perform the duties of a DPO.

IV. OTHER POINTS OF CONCERN

a) Personal availability of the DPO

The Guidelines specify the requirement that the DPO should be directly and personally available to data subjects and the DPA. Is that an absolute requirement? What protects the DPO from unreasonable expectations to personally address each data subject in case of a substantial data breach, for example? Especially in organizations which process the personal data of many data subjects or who operate in multiple countries, this requirement would interfere with the effective performance of the tasks of the DPO.

The NGFG believes the DPO should be able to use the resources of the organisation, such a customer care center or a secretary, to deal with data subject complaints in the first instance, provided he/she carries the responsibility for the manner in which those resources handle those complaints. Also, the DPO should have the possibility to have support team, which performs DPO-tasks under his/her supervision.

b) Relationship between the DPO of a controller and the DPO of a processor

The guidelines do not sufficiently clarify what should be done in case of a dispute between the DPO of a controller and the DPO of a processor. How should they "cooperate" (Guidelines paragraph 2.2)? Whose judgement prevails in the end? Can the relationship between the two DPO's be determined in a processing agreement or is that a violation of the autonomy of the DPOs? And can the DPO of a controller trust part of the monitoring work to the DPO of the processor?

c) Reporting to the highest management level

A paragraph clarifying Article 38(3) GDPR is much needed. This paragraph would help organisations, especially in the public sector, to determine what is the highest management level. Does this include political leadership?

Moreover, what is meant by "directly report"? Does this require a direct management relationship or is it only meant to ensure a direct access to the highest management level (direct functional access)? And how does this requirement relate to the fact that many DPOs have another job in the organisation? Would they then have two managers to report to?

Does the prohibition to receive instructions prohibit the manager of the DPO to perform evaluations of the performance of the DPO and setting targets? If yes, this would seriously hamper the employability of the DPO and their chances of promotion. If not, how would the DPO and their manager prevent that the performance review and targets do not interfere with the autonomy of the DPO?

d) Protection of employment

Clarification is needed on the conditions of protection of employment. Does this apply to all possible forms in which a DPO can be appointed (internal as well as external)? Does it also apply to all member of the DPO team? What about the assistant-DPO?