Appendix B - Position of the DPO

Article 38 sets the framework within which DPOs are expected to operate, including the obligations on controllers and processors to ensure that they have the resources to operate effectively and the degree of autonomy and independence the DPO is expected to have in performing their tasks.

Specifically, these requirements are that the DPO must:

- Be involved, properly and in a timely manner, in all issues which relate to the protection of personal data
- Be allocated adequate resources to perform their tasks
- Have access to personal data and processing operations
- Be able and supported in maintaining his or her expert knowledge
- Not be given instructions regarding the exercise of those tasks
- Not be dismissed or penalised for performing the tasks of the DPO
- Report to the highest management level
- Be contactable by data subjects on all issues related to processing of their personal data and to the exercise of their rights
- Be bound by secrecy or confidentiality concerning the performance of his or her tasks (but able to seek advice from/engage with ICO)
- If member of staff, be assigned other tasks and duties only if these do not give rise to a conflict of interests

The Guidance issued by the Article 29 WP seeks to provide more detail about these requirements and their parameters and to provide advice on practical implementation:

Instructions and 'performing duties and tasks in an independent manner'

- DPO not to be instructed on how to deal with a matter (for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority)
- the autonomy and decision-making powers of DPOs do not extend beyond tasks pursuant to Article 39
- DPO should be able to report and share advice and recommendations or dissenting opinion with "highest management level and to those making the decisions" if these are incompatible with the GDPR and the DPO's advice
- in terms of direct reporting at Board level, an example given is for the DPO to present an Annual Report on their activities

'Resources', 'Support' for DPO function and involvement in 'timely manner'

- active support of the DPO's function by senior management (e.g. at Board level)
- regular participation by the DPO in senior/middle management meetings and at meetings where decisions with data protection implications are to be made

- early communication to ensure DPO is able to provide advice on timely basis
- ensuring appropriate weight given to opinion of the DPO and where not followed, reasons to be documented
- prompt consultation with the DPO:
  - once a data breach or another incident has occurred
  - new or changed processes or systems are conceived so the DPO can advise on and decide if a DPIA is necessary

- sufficient time for DPOs to fulfil their tasks (especially where other tasks may be assigned creating competing priorities that might result in DPO's duties being neglected)
- 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 (to ensure role is known and understood)
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services (e.g. HR, IT, legal, security etc.)
- continuous training and networking to ensure data protection knowledge remains up to date

No 'dismissal or penalty' for performing DPO tasks and 'conflict of interest'

- protection from dismissal or penalty (intended to strengthen autonomy and independence of DPOs in performing their data protection tasks)
- penalties (direct or indirect) are only prohibited under the GDPR if imposed as a result of the DPO carrying out his or her duties as a DPO
- as would be the case for any employee or contractor, a DPO may still be dismissed legitimately for reasons other than for performing DPO tasks (for instance in case of theft, physical, psychological or sexual harassment or similar gross misconduct)
- DPOs may 'fulfil other tasks and duties' only if these do not give rise to conflicts of interests (e.g. DPO must not determine the purposes and the means of the processing of personal data)

- example of internal DPO conflict:
  - also holding senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) or roles lower in the organisational structure if such positions or roles lead to the determination of purposes and means of processing (guidance gives good practice advice on how to raise awareness of issue)
- example of external DPO conflict:
  - representation before Court in cases involving data protection issues

Specified Tasks of the DPO

The minimum tasks of the DPO specified in Article 39 are:

- informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws
- monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities
- training staff
- conducting internal audits
- advising with regard to data protection impact assessments when required under Article 35 (e.g. evaluating whether residual risk is acceptable or meets the threshold for 'prior consultation' with the ICO)
- acting as contact point for the supervisory authority on issues relating to processing, including prior consultation, and to consult, where appropriate, with regard to any other matter (Article 39(1)(e))
- handling inquiries from data subjects on issues relating to data protection practices, subject access, withdrawal of consent, objections to and restrictions on processing and related rights.

The Article 29 WP guidance sets out when advice must be sought from the DPO in relation to undertaking DPIAs, the need to adopt a risk-based approach to prioritising data protection activities and, the types of other tasks that may be assigned to the DPO (such as compiling records of processing operations for the organisation and monitoring ongoing compliance). These are summarised below.

Data Protection Impact Assessments:

- 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 data protection impact assessment has been correctly carried out and the processing can go ahead and the identified safeguards in place or, if prior consultation with the ICO is required
- Risk-based approach to prioritisation:
- DPO to prioritise activities and focus of effort on issues that present higher data protection risks.

Record keeping & monitoring compliance:

- support record keeping obligation of the organisation by:
  - identifying, collecting and recording information about the organisation’s processing activities
  - creating inventories and holding a register of processing operations supplied by service areas for evidential accountability purposes (and for use as tool in performance monitoring and reporting)
  - analysing and checking the compliance of processing activities, and

– informing, advising and issuing recommendations to the controller or the processor (with reasons recorded by the organisation if DPO advice is not pursued)