DPO Implementing Rules

Regulatory framework

- Legal obligation: Art.45(3) DPR requires "further implementing rules concerning the Data Protection Officer (…) in particular concern the tasks, duties and powers of the Data Protection Officer".
- The EDPS has its own DPO implementing rules from December 2018 (following DPR) – inspiration (?)
- FX Regulation: obligation to have DP implementing rules, also for the DPO
- Guidelines:
  - EDPB: Guidelines on Data Protection Officers ('DPOs') (2017)
  - EDPS: Position paper on the role of Data Protection Officers (Dec'18)

Aspects to consider: Appointment, term and modalities

- A DPO can be external, internal or shared.
- Shared for small agencies, on same location, aware of conflict of interests (e.g.: Transfers between agencies)
- Outsourcing for admin data (?) (considering scarcity of resources and sensitivity of the data)
- For JHA Agencies, recommendation would to be internal staff member.
- Term: 3-5y minimum, renewable. No limit mention for renewal – Recommendation: the longer the appointment is, the more independence is ensured.

- SKILLS:
  - Knowledge and expertise on DP (essential) depending on agency size and topic
  - Knowledge on the agency, functioning and structure (desirable)
  - IT knowledge
  - Communication and organizational skills
  - Integrity and high professional ethics

Aspects to consider: Position and Independence

- DPO, Assistant DPO and DPO staff are equals in term of independence. (term of appointment?)
- Involved properly and in a timely matter in all topics affecting DP (consulted and informed since the offset of an operation). Requires a **standard procedure** for involvement in all topics.
- Needs to be invited to management meetings (internal and MB – middle, higher management)
- Resources:
  - staff, financial resources, infrastructure + support from other Units
  - Access to all PD, premises, processing operations
  - Continuous training

Aspects to consider: Independence

- Reporting line: highest management level – devise a two tier system – ED & MB
- Independence covers the function- not total coverage from disciplinary sanctions for legitimate reasons
- Conflicts of interests: not taking any other role/position that may convert him/her into a controller. Incompatibility with high-level positions. No representation of the Agency in the Courts
- Cannot be dismissed or penalized by a controller/processor (requires shield from management)
- Conditions for dismissal, cumulative: no longer fulfil conditions + EDPS consent
- Possibility that the EDPS does part of the appraisal of the DPO (independence + conflict of interest?)

Aspects to consider: Tasks of the DPO

- Golden principle: responsibility lies on the controller
- Tasks are Role dependent:
  - Information and awareness (trainings, meetings, conferences, webpage, papers, etc.)
  - Advisor: for data breaches, for DPIAs for prior consultation, on application of DP provisions
  - Provide for a safe channel of communication for confidential reporting to the DPO (=Whistleblowing?)
  - Organizational: central record keeping (centralized or per Controller)
  - Cooperative function: vis-à-vis EDPS (note: informing EDPS on developments impacting DP – obligation or nice to have?)
  - Monitoring compliance – audits? (overlapping with internal audit service?) +
  - Handling queries or complaints: investigative powers – procedure to initiate and report on those would be needed + obligation to cooperate by all units with the DPO
  - Enforcement: bringing it to the attention of the appointment authority about the possibility to sanction servants (intentionally or by negligence) for disciplinary or other actions by Staff Regulations

Aspects to consider: dependencies

- Is escalation to EDPS a must?
- Measuring DPO effectiveness: develop own criteria for good supervision (professional standards, specific plans for the agency, annual work plan) with a double objective:
  - Enable EDPS to evaluate the work of the DPO (if invited)
  - Measure degree of implementation of the DPR

- QUESTIONS?

Thank you!