DPO Meeting
EIF
Luxembourg, 8 May 2015

1. Introduction and presentation of the new EDPS Team and the EDPS Strategy 2015-2019

GB and WW presented the new EDPS Team and briefly outlined the division of work between themselves. GB then went on to present the Strategy and the three objectives - 1) Data protection goes digital: promote technologies to enhance privacy and data protection, identify cross-disciplinary policy solutions, increase transparency, user control and accountability; 2) Forging global partnerships: develop an ethical dimension to data protection, mainstream data protection into international agreements and speak with a single voice in the international arena; and 3) Opening a new chapter for EU data protection. The way people use technology has changed dramatically over the past years and data protection therefore also needs to change. Big data needs accountability and GB discussed the challenges, such as lack of transparency and potential unfair discrimination in access to data or lack of efficient control, and responses in relation to this. He also went into the EDPS' role as a diplomat for data protection world-wide, for non-EU countries and international companies. To achieve the objectives the EDPS must adopt and implement up-to-data protection rules, increase the accountability of EU bodies processing personal information and engage in a productive cooperation. Finally, the DPOs were informed of the new EDPS logo.

2. State of play and priorities

SLx gave a short presentation explaining who the EDPS wants to be and what the priorities should be in the light of the Strategy: 1) an active partner for EU institutions, providing practical and dynamic solutions; 2) selective in each activity using a risk-based approach; 3) accountable and promoting accountability. She advised that there will be a new inspection methodology and a new format of prior check opinions, which will be less legalistic. Furthermore, the DPO meetings shall henceforth be more interactive and dynamic, using the workshop format. More visits are planned, also on a staff level for consulting and giving guidance. The reform of Regulation (EC) 45/2001, the data protection impact assessment and the data breach notification, shall be anticipated. Furthermore, training of the Court of Justice on data protection is planned and a data protection toolkit, providing easy access to data protection guidance, is being developed.

3. Recent case law

CD gave a presentation of recent data protection case law:
- **C-212/13, Ryneš v UPOOU**: the ECJ held that video surveillance of persons in public areas is not purely personal but falls under EU data protection law. Apart from consent, there can be other grounds for processing, such as legitimate interest.
- **C-141/12 and C-373/12, YS v Minister voor Immigratie**: the ECJ held that the legal analysis of the application for residence of a third country national is not personal data, but simply information about the legal assessment of a person's situation, and that therefore, providing a full summary of the relevant documents is sufficient.
- **Google v Vidal-Hall et al.**: a person claimed moral damages for Google's collection of browser generated information about his internet use. The Court held that such information can be considered personal data under the directive and since the damage was sustained in the UK, the company could also be sued in the UK.
- **C-615/13, Client Earth v EFSA**: an NGO requested access to documents containing names of experts and comments made. Access was given, but the documents did not allow a connection between the experts and the comments. The General Court dismissed the application. The Advocate-General agreed with the General Court and the EDPS that the 'intersection' of information is personal data, but applied a lower level of necessity under Article 8 of Regulation (EC) 45/2001 where the data are professional and do not fall within the scope of privacy in the strict sense.
- **C-362/24, Schrems v DPC Irl**: the latter refused Mr Schrems' request to suspend transfers under the Safe Harbour Decision, to stop Facebook transmitting personal data to the US. The case challenges the lawfulness of the Safe Harbour Decision and questions whether it limits the powers of the DPAs.

4. Contribution of the DPOs to the data protection reform, including feedback from the DPO Quartet

Emese Savoia-Keleti, assistant DPO of EEAS, presented an overview of the input of the DPOs with regard to the reform of Regulation (EC) 45/2001. A coordinated work has been carried out in different working groups in three stages.
1. April – June 2014: five working groups the following themes:
- Role of the DPO, EDPS and other questions related to formal aspects
- Substantive aspects
- ICT aspects
- Transfers
- Transitory period

The working groups provided input that were summarised at the DPO meeting in June in Brussels.

2. June – November 2014: consolidation work (initiated and coordinated by Laraine Laudati DPO of OLAF, and Emese Savoia-Keleti in consultation with the DPO Quartet), incorporating the DPOs comments and proposals. An initial proposal document was elaborated article by article with an outlook on:

- the EC proposal of the GDPR
- Regulation (EC) 45/2001
- the DPO network's comments and proposals

The initial proposal document of the DPO network on the reform of Regulation (EC) 45/2001 was presented at the DPO meeting in November 2014.

3. November 2014 – May 2015: The initial proposal document was uploaded on CIRCA for comments. The document has been updated with the comments and proposals from DPOs, sent to the DPO Quartet and presented at the March EC workshop. Additional comments and the updated document were sent to DG Justice.

The DPO input referred to:

- Notion of Controller
- Right to data portability
- Historical purpose
- Confidentiality
- DPCs, DPO, EDPS
- Prior checking, PIA, PS
- Transfer

5. Workshops

- ***Introduction for newly appointed DPOs***

The aim of this workshop was to give newly appointed DPOs an overview of their tasks and responsibilities as well as the interaction and cooperation between DPOs and the EDPS; and provide some practical guidance. Firstly, the respective missions and powers of the EDPS and the DPOs were presented. Emphasis was put on the importance of the independence of the DPO and the difficulties that part-time DPOs, junior DPOs and DPOs with temporary/contractual agent status may have in this respect. Secondly, a large part of the workshop was dedicated to prior checking (what processing operations require prior checking, how to proceed, how to complete the notification form, the scope and requirements of Article 27, etc.), with practical examples and a Q&A session. Questions notably concerned the definition of controller, the purpose of the processing operation, and information to data subjects. The participants particularly appreciated the good atmosphere, the practical examples and the opportunity to receive detailed answers to their questions.

- ***Mobile Device Guidelines***

The EDPS presented their draft guidelines on the protection of personal data in mobile devices used by European institutions and bodies. The guidelines aim to provide practical advice and instructions to the EU institutions as data controllers on the application of Regulation (EC) 45/2001 to the processing of personal data via mobile devices. They are specifically aimed at DPOs, as well as IT and IT security staff. This document was sent for consultation before the meeting and comments are expected by 19 June 2015. The EDPS presented the main guiding principles for any organisation when adopting rules and procedures on the use of mobile devices, which should be accountability, necessity, proportionality and security. Organisations should be accountable for their actions and their procedures should be clearly determined; interference with fundamental rights, in particular privacy and data protection should be limited to what is necessary and proportionate. As the security of personal data processed is fundamental for guaranteeing data protection, one of the main pillars of the guidelines and the presentation was the presentation of a toolbox for implementing a risk management process, assessing security risks of the use of mobile devices for processing personal data and – on the basis of the outcome of such assessment - implement measures to mitigate or eliminate the identified risks.

The attendees pointed to the difficulty of separating professional and personal use of mobile devices and its implications regarding data protection and privacy. It was also put forward that the security measures implemented usually focus on controlling the user but a more balanced approach should be pursued as the organisations also has responsibilities towards the user.

- ***Complaints and the role of the DPO (new policy and practical examples)***

The workshop had three phases:

1- Presentation by MVPA on the life of a complaint and the moments where contribution/cooperation and/or advise might be expected or required from the DPO.
2- Presentation by Laraine Laudati (DPO of OLAF) of her experience in complaints handling.
3- Case studies: Division of the participants in three groups to discuss three case studies (examples of hypothetical complaints submitted to a DPO. Questions were asked on the basis of the facts of the case).

The structure of the workshop was very well received by the participants. However, due to a reduction of the time allocated to the workshop, there was no time to have a general discussion about the answers provided by the groups. Participants expressed enthusiasm to have more of the "case-study" workshops in the future.

- ***The role of the DPO and accountability***

The aim of this workshop was to launch a discussion among the DPOs on how they could help their institution to be accountable in data protection. The intention was to foster dialogue, promote active participation, boost the DPOs common reflection and minimise the "*ex cathedra*" intervention of the EDPS.

The workshop started with a brief presentation by the EDPS on:
- accountability in general and under GDPR;
- the DPO network's position on accountability;
- the tools at the DPOs' disposal to support accountability under Regulation (EC) 45/2001;
- advantages and potential adverse effects of accountability.

The participants were then divided into two groups that discussed the implementation of accountability in practice and the role of the DPOs respectively.

Accountability in practice
In order to effectively implement accountability the need for a "proactive approach" was highlighted, as well as a change of mind-set and a change of culture (from controlling to managing the risks). The measures that were suggested include: inserting data protection risks in an annual work plan to be signed by the top management; putting into force a risk register with the state of play for the ongoing year to be duly monitored through the following year; setting up a simplified register that would mix inventory/register/Article 25 notifications; streamlining data protection audit with existing audit practices; training DPOs on risk assessment and audit methodology, etc.

Role of the DPOs
Participants stressed that ex-ante notifications (Article 25) should be maintained, independently from the intervention of the EDPS, as it is a unique opportunity for controllers to reflect on data protection at an early stage. The workload and resources of an enhanced role of the DPO was raised. Pros and cons of providing DPOs with enforcement powers were discussed. Some participants noted that institutions will invest in compliance only if the DPO has effective enforcement powers. The latter would increase the DPOs' independence and enable them to be more effective in urgent situations. The audience was, however, divided on the possibility of giving more enforcement powers to the DPOs, because of the increased responsibility that it could involve.

The participants were actively engaged in the discussion. They generally welcomed a deeper collaboration between the DPOs and the EDPS on how to implement accountability in practice. It was suggested to develop a tool to share views and

exchange best practice ideas on how to implement accountability in practice. The topic should be further discussed at the next DPO meeting.

- ***Security of processing***

The first half of the workshop on Security of processing concerned Article 22 of Regulation (EC) 45/2001 and its relation to best practices in Information Security Risk Management ("ISRM") with the aim to help controllers applying accountability regarding information security. Firstly, the basics of ISRM were introduced and linked to Article 22. It was shown how the need for measures has to be analysed in the light of the risks of the processing of personal data by the EU institution, the nature of the personal data processed and the type of processing operations. Secondly, different implications for the EU institutions were discussed, among them the accountability aspect and the responsibilities of the EU institutions as data controllers, and more particularly, their management, with regards to the security of processing and the ISRM process.

The main outcome of the subsequent discussion was the need for the DPOs to work more closely with the security function of EU institutions. Also, more practical guidance and examples were suggested by some participants.

6. Follow-up

The feedback from the meeting has been very positive and the DPOs were particularly satisfied with the new meeting format. The participants appreciated the workshop themes and the opportunity to discuss in smaller groups. The comments made in the assessment forms were mostly positive, although there was a general feeling that not enough time was allocated to the workshops. All of them suffered from time constraints, and in some workshops there was unfortunately no time for questions and exchange of views. For the next meeting, it is therefore suggested to allocate more time to the workshops on the agenda and more time for interactive discussions in the respective workshops. Some participants also regretted that they had to make a choice between several themes that they found interesting. It seems difficult, however, to avoid parallel workshops since it is important to have smaller groups, which facilitates discussion.

<u>Practical suggestions for next DPO meeting:</u>
- Lunch break could be shorter and preferably standing in order to facilitate interaction with DPOs
- If one or several DPOs participate in the organisation of the workshops, it is useful idea to meet prior to the DPO meeting;
- The assessment forms will be updated so that the feedback can be given both on procedure and on substance;

- Add a short description of each workshop to the agenda or the invitation, in order to enable the DPOs to make their choice;
- Provide time to move from general meeting room to other meeting rooms in order not to shorten the workshops unnecessarily;
- Prepare a "speaker package" to the EDPS colleagues responsible for workshops, with a check list for the three phases: pre-event, during the event and post-event.