EUROPEAN DATA PROTECTION SUPERVISOR

INTRODUCTION TO NEWLY APPOINTED DPOs

Xanthi Kapsosideri &
Petra Candellier

DPO MEETING, EIF
Luxembourg, 8 MAY 2015

EDPS MISSION (1)

Art. 41(2) Reg. 45/2001:

“With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies…”

EUROPEAN DATA
PROTECTION SUPERVISOR

EDPS MISSION (2)

EDPS responsible for:

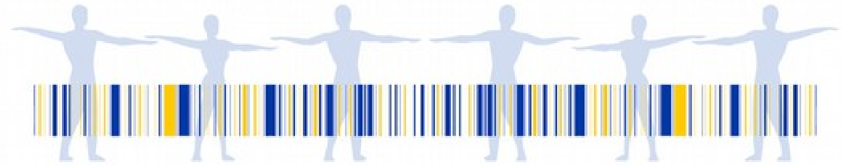
-Monitoring and ensuring the application of Reg. 45/2001

-Advising EU institutions/bodies on all matters concerning processing of personal data

-Examining complaints lodged by individuals whose personal data have been allegedly processed by EU institutions/bodies

Compliance monitoring tools

- “Prior checks”;
- Consultations on administrative procedures;
- Complaints handling;
- General or targeted monitoring and reporting exercises;
- Awareness raising (e.g. guidance papers, training, network of Data Protection Officers);
- Inspections (general, thematic, targeted);
- Compliance visits to agencies/institutions.



DPO’s MISSION

Art. 24:

-Informing controllers and data subjects of their rights and obligations

-Cooperating with the EDPS

-Ensuring in an independent manner the internal application of Reg. 45/2001

-Keeping a register of all processing operations (risky and non-risky)

-Notifying the EDPS of sensitive processing operations

DPO’s MISSION

Annex:

-Make recommendations for the practical improvement of data protection within your institution/body

-Advise controllers on data protection matters

-Investigate data protection matters on your own initiative or at the request of your institution/body, a controller, the staff Committee or any individual

PRIOR-CHECKABILITY

Start off with the **questions**:

-What is the **purpose of the processing?**

and

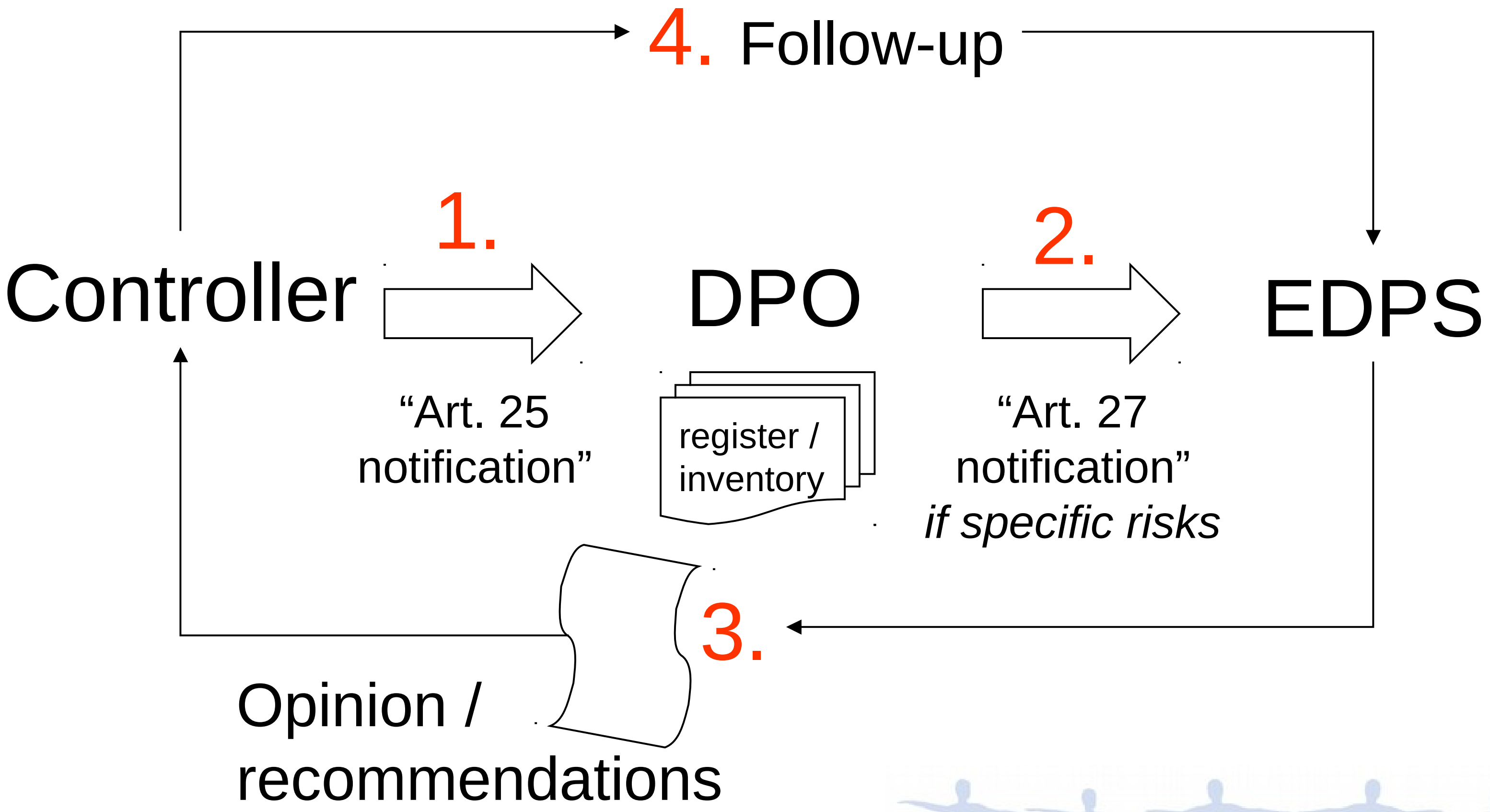
- Which **specific risks** in light of **Article 27(2), may justify prior-checking**? *Article 27 lists (non) exhaustively risky processing operations*

Prior checking

- Risky processing under Article 27?

- Prior ?
  - *Before the processing operation starts*
  - *Before the decision/procedure is adopted*
  - *The development of the procedure is sufficiently advanced*
- Checking ?
  - *Control*
  - *Consultation*
  - *Authorisation*

Workflow prior checking



4. Follow-up

Controller

1.

“Art. 25 notification”

DPO

register / inventory

2.

“Art. 27 notification” *if specific risks*

EDPS

3.

Opinion / recommendations

LIST OF Art.27(2)

- Art.27(2)(**a**): processing of data relating to **health**, **offences**, **criminal convictions**, **security measures**
  - Management of sick leave, management of pre-recruitment medical visit (health data must be processed structurally to present a risk, i.e. the aim of the processing is to process data relating to health)

- Art.27(2)(**b**): processing intended to evaluate personal aspects relating to the data subject, including his or her **ability**, **efficiency** and **conduct.**

  Selection and recruitment of staff, evaluation and promotion of staff, administrative inquiries and disciplinary measures, procedures to fight against harassment (the evaluation of employees abilities or conduct represents the vast majority of opinions published)

LIST OF Art.27(2)

- Art.27(2)(**d**): processing for the purpose of **excluding** individuals from a **right**, **benefit** or **contract.**

  - Exclusion databases (Early Warning System), asset freezing processing activities, the principle here is the "blacklist"

To be prior-checked or not?

- Telework
- Establishment of rights after recruitment
- 360°evaluation
- Time management
- Access control
- Management of conflict of interest
- E-recruitment

➔ *GUIDED BY THE ACCOUNTABILITY PRINCIPLE*

CONTROLLER

1/ Name and address of the **institution**

From a legal perspective, the ultimate **responsibility** lies with the **institution.**

2/ The **specific DG**, **sector**, **unit** or **department** of the institution responsible for internally managing the processing should be indicated.

A **contact person**, easily accessible, should also be mentioned for both data subjects and further questions from the EDPS.

PROCESSOR

3/ Does your institution outsource the management of employees’ medical data or video-surveillance operations to an external service provider?

There should be a **contract** or **SLA** which you should send to the EDPS!

Before signing the contract, the institution should specify:

- That the **processor will act on behalf of the controller;**
- The **processor’s tasks;**
- Clauses on **data protection**, **confidentiality**, **security measures** (Article **23 requirements**).

Is any part of the processing **further subcontracted**?

WRONG DATA PROTECTION CLAUSE

“Any personal data included in or relating to the Contract, including its execution shall be processed pursuant to Regulation 45/2001…It shall be processed solely for the purposes of the performance, management…**The Contractor shall have the right of access to his personal data and the right to rectify any such data that is inaccurate or incomplete.** Should the Contractor have any queries concerning the processing of his personal data, he shall address them to the institution/agency. **The Contractor shall have the right of recourse at any time to the EDPS**”.

DATA PROTECTION CLAUSE

Reference to the **contractor’s personal data and right of access** to them is **irrelevant!**

- **Data subjects** are the persons **concerned**.

- The **clause should focus** on the **personal data of data subjects** whose data are processed by the Contractor.

Name, Purpose, Data subjects,

3/ Please provide the **FULL TITLE** of the **processing**, **NOT** the **name of the database.**

4/ Be **explicit** with the **purpose**: it **helps** assess the:

- **legitimacy** of the processing
- **data quality** requirements
- whether the **processing is prior-checkable**

5/ Please indicate **all categories of data subjects**

CATEGORIES OF DATA

6/ Specify all categories of data (identification, **administrative**, financial, health, criminal records, other **special categories of data** (Article 10).

Are any **templates**, questionnaires, other **forms** used to collect personal data?

Please **attach them** to the notification!

INFORMATION TO THE DATA SUBJECT

7/ *Form:* Via a privacy notice **BEFORE THE PROCESSING** which should be **easily accessible**, please indicate **where it is displayed** (intranet, forms, leaflets …).

Content: It should provide **simple, clear** and **relevant** information on the elements listed in Articles 11(where data were collected from the data subject) and 12 (where data were collected from other sources).

Aim: to guarantee **fair** processing **(art.4(1)(a))** and transparency.

RIGHTS OF DATA SUBJECTS

8/ Right of access and rectification

Do not simply mention their **possibility to exercise them**, but

explain **how data subjects** may exercise them and

specify their possible **limitations.** (i.e Article 20)

Automated/Manual, Storage, Legal basis

9/ Explain **briefly main steps**: collection, use, transfer, storage of data and if **processing** is **manual** or **automatic**.

10/ Specify where personal data are **stored**: in a filing cupboard, CD?

11/ Indicate the **exact provision** of the Treaty, Staff Regulation, contract, decision. Please attach a copy of an internal Decision, contract, other document.

EUROPEAN DATA
PROTECTION SUPERVISOR

RECIPIENTS

12/ Indicate **each recipient** (any natural/legal person, public authority, other body), if it is

- an EU institution/body,
- Subject to national law implementing Directive 95/46 (i.e external doctor, national Court)
- Not subject to the Directive (i.e third country)

Which type of personal data are transferred (need-to-know basis principle)

and the **purpose of the transfer.**

EUROPEAN DATA
PROTECTION SUPERVISOR

RETENTION POLICY, BLOCKING, ERASURE

13/ Provide a **specific max retention** period for **each category of personal data** and

justify with concrete examples/experiences the **period** indicated.

13A/ Specify a **specific time-limit** for doing so i.e 15 days after receiving a request.

STATISTICAL PURPOSES, Art.9

14/ Are personal data kept for historical, statistical or scientific purposes?

If so, are they **anonymised** or is the identity of the persons is **encrypted**? **How**?

If data are not anonymised, explain why and specify **safeguards** in place to ensure that they are not processed **for other purposes**

15/ Explain the **legal grounds** for a transfer under **Art.9.**

SECURITY MEASURES

16/ Detailed description in the notification and **attach** your internal **security policy** about the **organisational and technical measures** your institution has adopted regarding the **specific processing.**

Article 22 guides you about the aims of such measures!

Confidentiality declarations: (organisational measure preventing unauthorised disclosure)

EUROPEAN DATA PROTECTION SUPERVISOR

Accountability

EDPS objective:

-train EU institutions/bodies on how to best respect in practice data protection rules;

-support EU institutions in moving to an **accountability-based approach**;

❖DPO’s role stronger

❖EU institutions/bodies must be able to **demonstrate compliance *in concreto*** with principles and obligations of Reg. 45/2001.

CONCLUSION

For specific examples, Guidelines, questions, doubts, you may consult www.edps.europa.eu

✓Prior-checking Opinions
✓Consultations
✓Thematic Guidelines
✓DPO Corner
✓Call us on Thursdays from 14-16h

Thank you for your attention!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS