EDPS EUROPEAN DATA PROTECTION SUPERVISOR

EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

WORKSHOP FOR NEWLY APPOINTED DPOs

Petra CANDELLIER
Xanthi KAPSOSIDERI

27 October 2016

The EDPS Strategy

2015-2019

Leading by example

The EDPS

Established in 2004

- appointed by a joint decision of the EP and the Council for a 5 year mandate
- current mandate 2014-2019

Giovanni Buttarelli
Supervisor

Wojciech Wiewiórowski
Assistant Supervisor

Legal framework

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 and bodies…***"

The EDPS

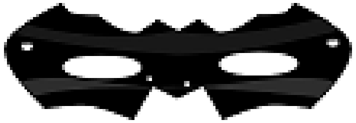
1. **Supervise** data processing done by EU institutions and bodies;
2. **Advise** the EU legislator and appear before the EU courts;
3. **Cooperate** with other supervisory data protection authorities;
4. **Monitor** new technologies with an impact on privacy.

EDPS compliance monitoring tools

- Prior checks
- Consultations
- Complaints handling
- General monitoring and reporting exercises
- Awareness raising
- Inspections
- Compliance and Accountability visits to agencies/institutions
- Secondments

Powers of the EDPS

- **Advise** data subjects in the exercise of their rights
- **Order** controller to grant access rights to data subject
- **Warn or admonish** the controller
- **Impose** a temporary or definitive **ban** on processing
- **Refer** the matter to the EP, Council, Commission or ECJ
- **Intervene** in actions brought before the EU Courts
- **Obtain** from the controller **access** to personal data necessary for his enquiries
- **Obtain access** to any premises in which an EU institution carries out an data processing

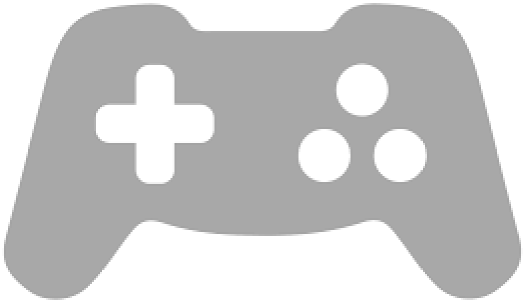


DPO’s role

- **Ensure in an independent manner** the application of the Regulation
- **Inform** controllers and data subjects of their rights and obligations
- **Cooperate** with the EDPS
- **Keep a register** of all processing operations (risky and non-risky)
- **Notify** the EDPS of sensitive processing operations

DPO's role

- Make **recommendations** for the practical improvement of data protection within the EU institution/body
- **Advise** the EU institution/body on data protection matters
- **Investigate** data protection matters on his/her own initiative or at the request of his/her institution/body, the staff Committee or any individual.
- Can be **consulted** by anyone without going through official channels



Controller

EU institution/body, DG, unit which alone or jointly **determines the purposes and means of the processing of personal data** (Art. 2(d))

It shall be for the controller to **ensure** that the **data quality requirements** are complied with (Art. 4.2)

Data quality

Certain principles must be complied with (Art. 4);

i.e. personal data should be:

- Processed **fairly and lawfully**
- Collected for **specified, explicit and legitimate purposes**
- **Adequate, relevant and not excessive** (proportionate to the purpose for which they are collected/further processed)

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

2/ A **processor** carries out processing operations on behalf of the controller (Art. 23);

- Contract or legal act binding both controller and processor;
- The controller remains responsible and the processor shall act only on instructions from them;
- Confidentiality and security obligations apply also to processor.

Ex.
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**”.

Rights and obligations of the processor

Separation of two paragraphs in the contract:

- **Obligations of your institution** vis-à-vis the personal data of the processor and the processor’s rights

- **Obligations of the processor** bound by the contract with your institution under Article 23 of the Reg.

- **Tailor-made data protection clauses** in processing operations which are sensitive or include complex technology

Name and Purpose

3/ Please provide the **full title** of the **processing**, **not** the **name of the database.**

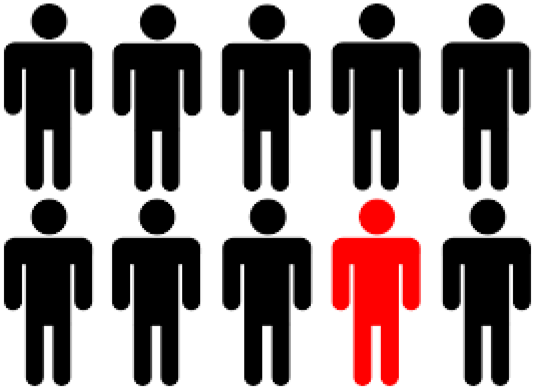
4/ Be **explicit** with the **purpose**: it **helps** assess the:

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

Data subject

5/ Please indicate **all categories of data subjects, i.e. identified or identifiable persons**:

who can be identified, **directly or indirectly**, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.



Categories of data

6/ Any information relating to an identified or **identifiable** natural person (*data subject*)

Categories of data

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

Does your institution use any **templates**, questionnaires, other **forms** to collect personal data?

Please **attach them** to the notification!

Information to data subjects

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.

Information to data subjects

The controller shall provide the data subjects with certain information (Art. 11-12), e.g.:

- Identity of controller
- Purpose of processing
- Recipient of the data
- Existence of right of access and right to rectify data and how to exercise these
- Legal basis
- Retention period
- Right to have recourse to the EDPS

Such information can be provided in a Data Protection Notice

Data subjects' rights

8/ Right of access, rectification, blocking and erasure

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)

Right of access

- **Confirmation** as to whether data related to him/her are processed
- **Information** on purpose, categories of data, recipients
- **Communication** in an intelligible form of the data processed
- **Logic** behind any automated decision process concerning him/her

Right of access

Selection procedures, appraisal, promotion exercises:

• Applicants should in principle be given access to their evaluation results regarding **all stages of the procedure**.

• Limitations: No comparative results of other candidates, no individual opinions of the members of the Selection Committee

• Staff members are provided with a copy of their report, are invited to make comments on it and may have access to all documents in their personal file even after leaving the institution

Rectification, blocking and erasure

Rectification

Rectification without delay of inaccurate or incomplete data

Blocking and Erasure

In certain specified situations (for ex where data subject contests accuracy (blocking) or where processing is unlawful (erasure).

Right to rectify

Staff members may exercise their right of rectification,

Appraisal/Promotion exercises: by introducing appeal procedures and adding the revised reports to their personal file.

Medical files: adding existing medical opinions with a second opinion or counter expertise.

AI & DP file: adding their **comments,** including **testimonies** and other documents related to a **legal recourse/appeal procedure. Final decision** to be replaced or removed from their **personal file**.

Exceptions to data subjects' rights

Article 20(1) of the Regulation

"…*necessary measure to safeguard:*

(a) the prevention, investigation, detection and prosecution of criminal offences;

(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;

(c) the protection of the data subject or of the rights and freedoms of others;

…"

Limitations to right of access

*Staff members should have **full access to their medical file**, but certain conditions may apply (Heads of Administration Conclusion 221/04 of 19 Feb 2004):*

- *Consultation of the medical file in the presence of a doctor of the institution's medical service/external provider*
- ***Indirect access to* psychological or psychiatric data through a private doctor (Art.20(1)(c))**
- No access to the doctors' personal notes (Art.20(1)(c)).

Limitations to right of access

- If A is a **victim** or **witness** of an alleged harassment, the controller will in principle **restrict access of A's identity** to an **alleged harasser** in order to protect A.

- If B is a **witness** and **requests access to the final Decision** of the inquiry, this should be strictly assessed by the controller on a **need-to-know basis** ; the final Decision in the end might not include B's personal data.

- If C is accused of **serious wrongdoings** and C asks for all information on him in relation to the accusations. **Even if the whistleblower's identity is deleted**, the latter's identity would be obvious through reference to events, situations and contexts described.

Limitations to right to rectify

Selection procedures:

*Candidates may rectify their **identification data** at any time during the selection procedure;*

*Candidates may **not rectify their admissibility criteria after the closing date** of submitting applications*

Grant and procurement award procedures:

Applicants may not rectify after the closing date of submission of applications or tenders.

Aim: transparency and equal treatment.

Restriction of information

AI & DP / Harassment / Whistleblowing:

It might be **necessary not** to specifically **inform the person under investigation** so that the procedure is **not prejudiced** or to **defer provision of information** in order to **protect the victim.**

However, Article 20(3) obliges the controller to **inform** the data subject of the **principal reasons for deferring access, rectification, information** and the right to seek recourse to the EDPS.

Meaning of Article 20(3)

The controller should **inform** data subjects about the processing of their data at different stages, including **the opening of an inquiry** related to them. A d**ecision to restrict the right to inform, access, rectification etc** under Article 20(1) of the Regulation, should be taken **strictly on a case by case basis.**

Article 20(3) means: The controller should be able to provide **evidence demonstrating detailed reasons for taking such decision** (e.g. motivated decision). These reasons should prove that they **cause actual harm** to the investigation and they **should be documented** **before** **the decision** to apply any restriction under Article 20(1) of the Regulation is taken.

Automated/manual processing, storage media

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, USB stick?

Legal basis and lawfulness

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

- Necessary for the **performance of a task** carried out in the **public interes**t on the basis of the **Treaties or other EU legislation (legal basis**) *or* in the **legitimate exercise of official authority vested in the EU institution/body**

Recipients and transfers

12/

a) Identify **each recipient** (any natural/legal person, public authority, other body)*;

b) Specify the **purpose** of the transfer;

c) Limit data to what is **strictly necessary** for the purpose (need-to-know basis principle);

* NB: OLAF, IDOC, internal auditor, Ombudsman, ECJ, EDPS are not recipients in this context.

Transfers

Three types of transfers:

- **Transfer within or between EU institutions** (Art. 7):

- necessary for the performance of a task covered by the competence of recipient.

- **Transfer to recipients subject to Dir 95/46** (Art. 8):

- public interest or exercise of public authority

- necessity + no reason to assume that data subject’s legitimate interest might be prejudiced

- **Transfer to third countries or organisations** (Art. 9)

- adequate level of protection (15/)

Retention policy

13/ Do not keep data in a form which permits identification **for longer than necessary** for the purpose for which they were collected or further processed

- ✓ Provide a specific **maximum** retention period for each category of personal data;
- ✓ **Justify** with concrete examples/experiences

Time limit to block/erase, Historical, statistical, scientific purpose

13A/ Specify a specific **time limit** to react to requests for blocking and erasure, e.g. 15 days after receiving a request.

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

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

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

Security measures

18/ “Information security risk management” as required under Article 22:

Describe the **security measures** and attach the internal **security policy** on the **organisational and technical measures** your institution has adopted regarding the **specific processing.**

Please refer to **Article 22** and the **EDPS guidelines on Security measures**.

Prior checking by the EDPS

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

Prior-Checkability

16/ Start off with the **questions**:

- What is the specific **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*

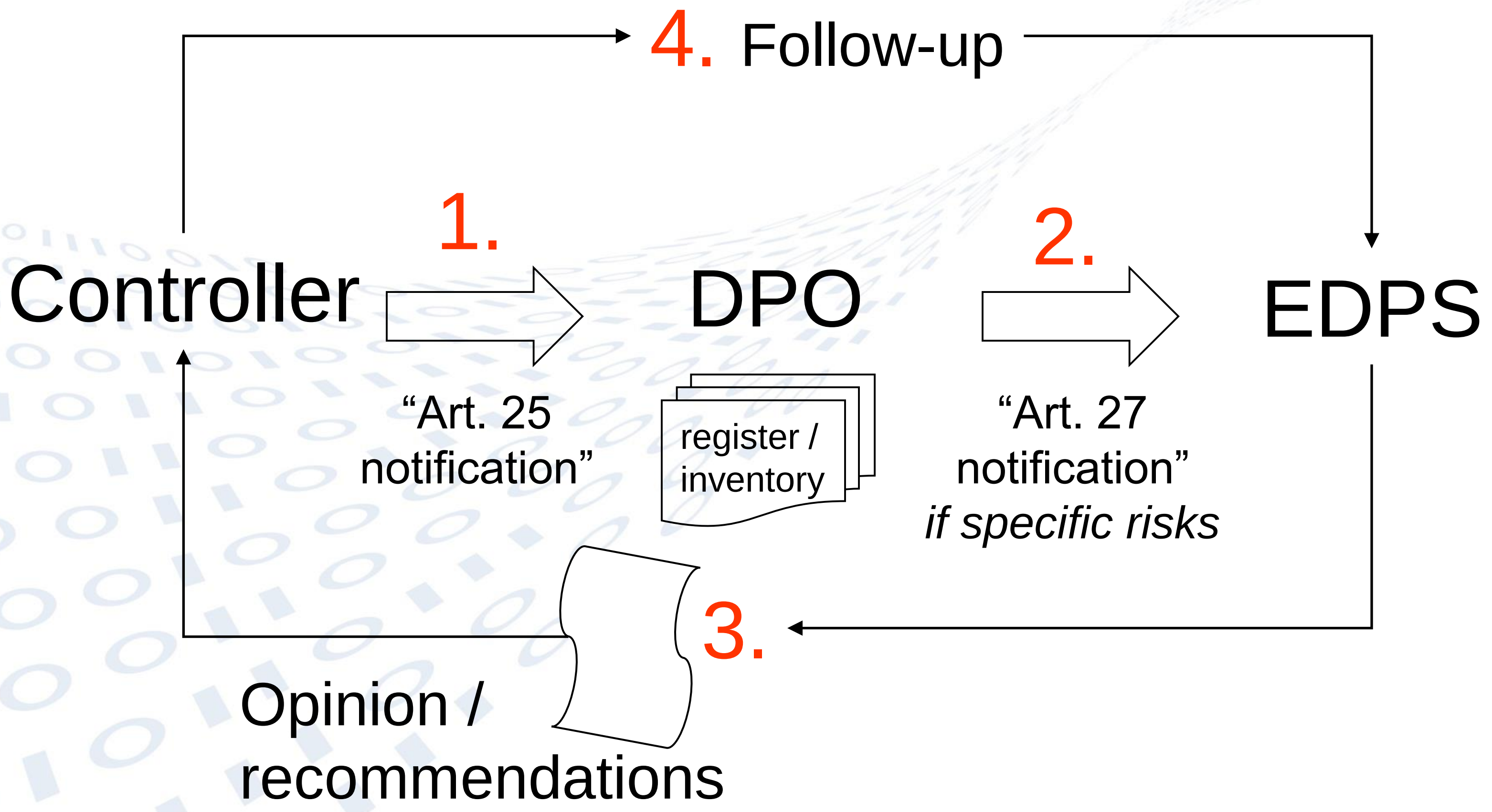
List of Art. 27(2)

- **Art. 27(2)(a)**: processing of data relating to **health**, **offences**, **criminal convictions**, **security measures**

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

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

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

Thematic Guidelines

Guidelines on specific themes:

- provide guidance for EU institutions and bodies in certain fields, such as recruitment, processing of disciplinary data and video surveillance.

- reference documents against which agencies can measure their current practices

Further information

For specific examples, guidelines, questions:

www.edps.europa.eu

- Prior-checking opinions
- Consultations
- Thematic guidelines
- Reference Library
- DPO Corner
- Call us on Thursdays between 14-16h

Accountability

EDPS objective:

✓ train EU institutions on how to best respect data protection rules in practice;

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

- Strengthen the **DPO's** role
- EU institutions must be able to **demonstrate compliance** *in concreto* with specific measures in conformity with the principles and obligations of the Regulation

Thank you for your attention!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS

#DPO-EDPS meeting
#DPO
#right of access
#restriction of rights