
# The supervision of personal data processing by EU institutions and bodies

Ute Kallenberger
Head of Inspections
Supervision & Enforcement Unit
European Data Protection Supervisor
EUSA Luxembourg (course no. 500877), 16 June 2016

# What is “personal data”?

- any information relating to an identified or **identifiable** natural person (*data subject*);
- **an identifiable person** is one 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.

# Two fundamental rights

## Privacy

"Right to be left alone"

Art. 8 ECHR (1950):

"Everyone has the right to respect for his or her private and family life, home and correspondence "

Article 7 EU-Charter (2000): "and communications..."

## Data protection

Article 8 EU-Charter

Article 16 TFEU

"Everyone has the right to the protection of personal data concerning him or her."

"self-determination"

# 2009: Treaty of Lisbon

- Everyone has the right to the protection of personal data concerning them

**Data protection principles**

**Art. 16 TFEU**

- EP + Council shall lay down the rules on processing of personal data by EU administration + Member States for activities under Union law, and the rules relating to the free movement of such data.

- Compliance with these rules shall be subject to the control of independent authorities.

# Some basic rules…

1. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
2. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority

# Supervision: who controls the controllers?

- Art. 28 Directive 95/46: MS must provide for independent Data Protection Authorities (DPAs) to monitor and enforce application of national law implementing Directive 95/46;
- Every data subject can lodge complaints with the DPAs, DPAs can go to court;
- **EDPS** monitors and ensures compliance with Regulation 45/2001 by EU institutions and bodies.



Art. 41(2), 44, 46 Reg. 45/2001

EDPS

# The EDPS

**The EU's independent data protection authority**

# The EDPS

The **European Data Protection Supervisor**:

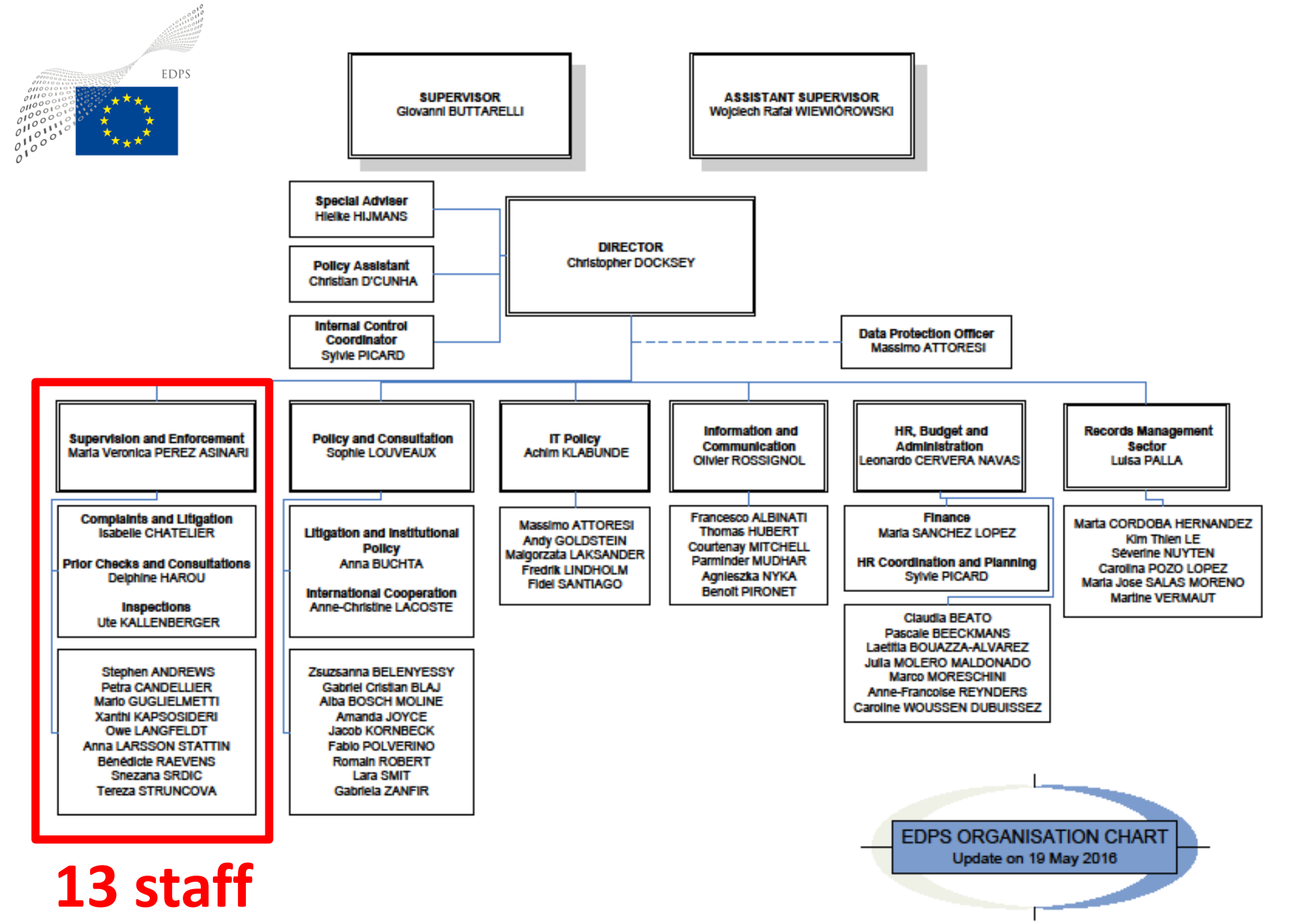
an independent institution responsible for ensuring the protection of personal data by the EU institutions and bodies

Giovanni Buttarelli
EDPS

Wojciech Wiewiórowski
Assistant EDPS

# The EDPS


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


EDPS
SUPERVISOR
Giovanni BUTTARELLI
ASSISTANT SUPERVISOR
Wojciech Rafał WIEWIÓROWSKI
Special Adviser
Hielke HIJMANS
Policy Assistant
Christian D'CUNHA
Internal Control Coordinator
Sylvie PICARD
DIRECTOR
Christopher DOCKSEY
Data Protection Officer
Massimo ATTORESI
Supervision and Enforcement
Maria Veronica PEREZ ASINARI
Complaints and Litigation
Isabelle CHATELIER
Prior Checks and Consultations
Delphine HAROU
Inspections
Ute KALLENBERGER
Stephen ANDREWS
Petra CANDELLIER
Mario GUGLIELMETTI
Xanthi KAPSOSIDERI
Owe LANGFELDT
Anna LARSSON STATTIN
Bénédicte RAEVENS
Snezana SRDIC
Tereza STRUNCOVA
Policy and Consultation
Sophie LOUVEAUX
Litigation and Institutional Policy
Anna BUCHTA
International Cooperation
Anne-Christine LACOSTE
Zsuzsanna BELENYESSY
Gabriel Cristian BLAJ
Alba BOSCH MOLINE
Amanda JOYCE
Jacob KORNBECK
Fabio POLVERINO
Romain ROBERT
Lara SMIT
Gabriela ZANFIR
IT Policy
Achim KLABUNDE
Massimo ATTORESI
Andy GOLDSTEIN
Malgorzata LAKSANDER
Fredrik LINDHOLM
Fidel SANTIAGO
Information and Communication
Olivier ROSSIGNOL
Francesco ALBINATI
Thomas HUBERT
Courtenay MITCHELL
Parminder MUDHAR
Agnieszka NYKA
Benoît PIRONET
HR, Budget and Administration
Leonardo CERVERA NAVAS
Finance
Maria SANCHEZ LOPEZ
HR Coordination and Planning
Sylvie PICARD
Claudia BEATO
Pascale BEECKMANS
Laetitia BOUAZZA-ALVAREZ
Julia MOLERO MALDONADO
Marco MORESCHINI
Anne-Françoise REYNDERS
Caroline WOUSSEN DUBUISSEZ
Records Management Sector
Luisa PALLA
Marta CORDOBA HERNANDEZ
Kim Thien LE
Séverine NUYTEN
Carolina POZO LOPEZ
Maria Jose SALAS MORENO
Martine VERMAUT
EDPS ORGANISATION CHART
Update on 19 May 2016

**13 staff**

# Supervision & Enforcement

## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Obligations of Controllers

Data must be…

- Processed fairly and lawfully;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Kept in an identifiable form only for as long as necessary for the purpose
- Data security

Arts. 4+22 Reg. 45/2001


WAIT! HAS ANYONE DONE A PRIVACY IMPACT ASSESSMENT?

# Some Useful Questions

- What exactly do we want to do and why?
- Why are we allowed to do it?
- What data we need to do it and for how long?
- Who needs to have access to the data?
- How do we make sure it's not used otherwise?
- How do we tell people about it and give them access to their data?
- How do we document all this?

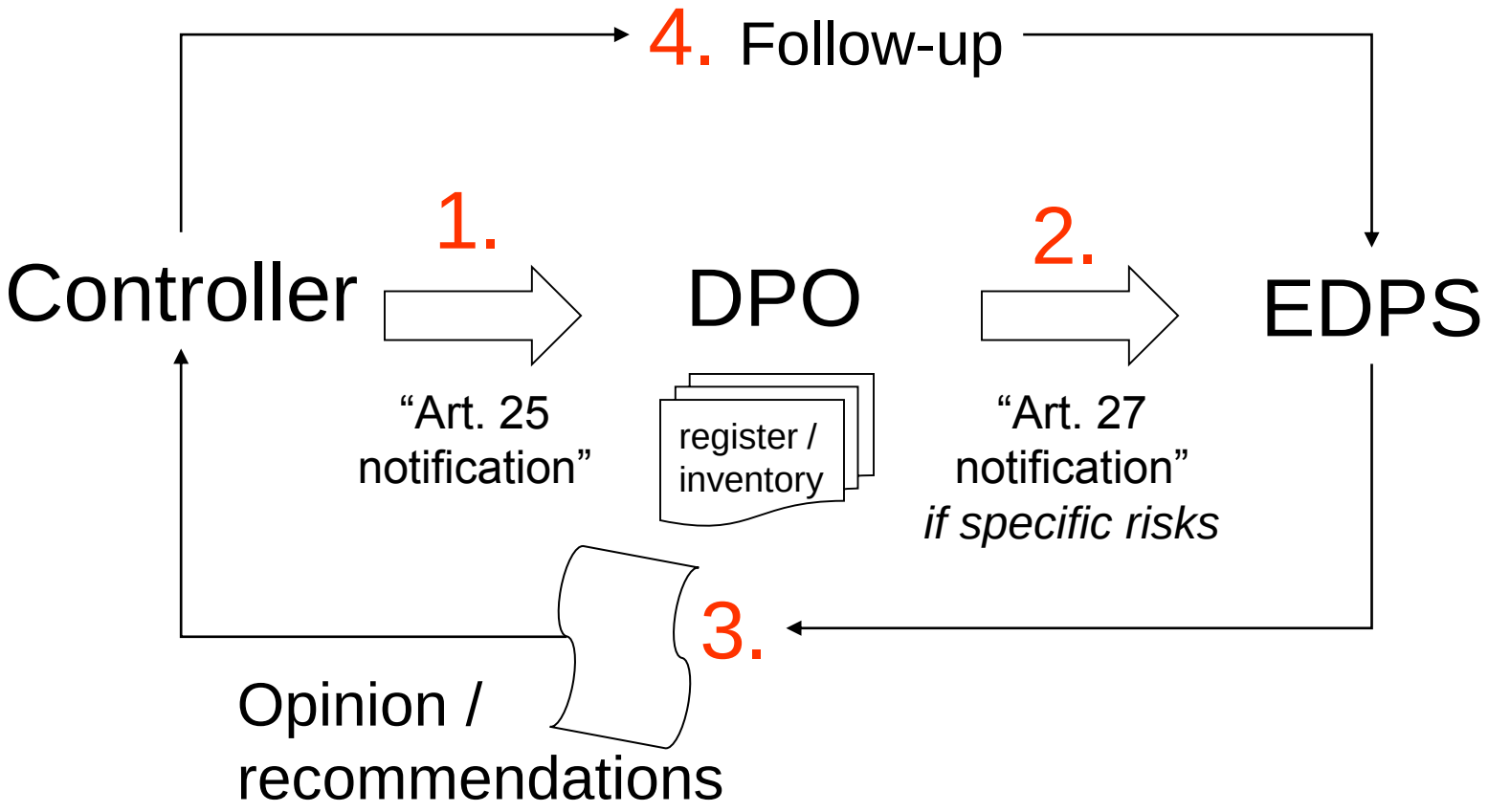
➢ Want to know more? Need guidance? Talk to your Data Protection Officer

# Supervision & Enforcement

## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Workflow prior checking



# Data Protection Officers




Arts. 24-26 Reg. 45/2001

# Prior checking - example

A bitter pill to swallow:

**“Return to Work” Policy**

- **Purpose**: “…to provide the affected employee with the necessary support measures to facilitate his/her return to work after sick leave to encourage his/her mental and physical recovery.”

- **But how does that work in practice?**

# “Return to Work” Policy

HoU or HR

contacts

re-assesses

coordinates actions

offers referral



GP, health&safety,
union representatives…

# Prior checking - example

A bitter pill to swallow:

**“Return to Work” Policy**

Ticks many of our “problem boxes”…

- ✓ lawfulness (health data/consent), Art. 5
- ✓ special categories of data, Art. 10
- ✓ data quality, Art. 4
- ✓ transfers, Arts. 7+8
- ✓ information to data subject, Arts. 11+12

+ **temporary ban**, Art. 47(1f)

# Supervision & Enforcement

## Promote a ‘data protection culture’

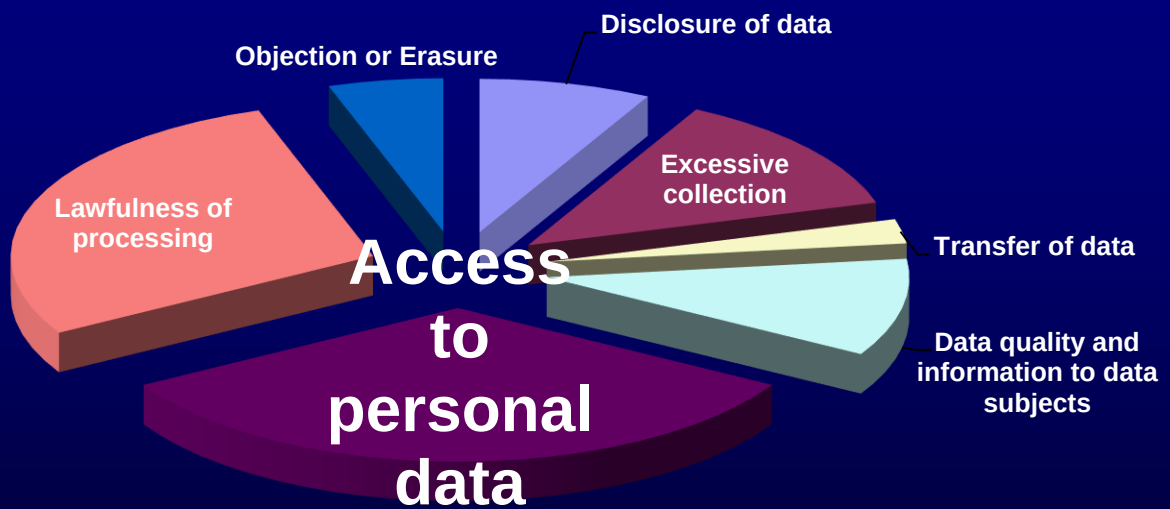
- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Data Subject Rights

- Information
- Access
- Rectification
- Blocking
- Erasure
- Objection
- No automated decisions



Arts. 11-19 Reg. 45/2001




**= 1/3 of our complaints!**

# Right to access


## Article 13

= access to *personal data*

## Reg.1049/2001

= access to *documents*



Art. 13 Reg. 45/2001

# Right to access

• Access to be granted **to the fullest extent**, as it helps data subjects to

- ➢ understand which of their data are processed;
- ➢ verify the quality of their own data;
- ➢ verify the lawfulness of the processing;
- ➢ exercise their other data protection rights.

• **Unless** an exemption under Article 20(1) applies:

- narrow interpretation, on a case-by-case basis;
- must not be restricted more broadly than necessary.



Arts. 13 + 20 Reg. 45/2001

# Exception Art. 20(1)(c)

***Selection procedures***

*(pre-selection tests, interviews and written examinations)*

• Principle (see above): **Access** to evaluation results at all stages of procedure

• Possible exception under **Article 20(1)(c)** to protect

- the independence of the jury;
- the confidentiality of the jury's deliberations;
- decision-making Selection Committee / individual members;
- safeguard the rights of other candidates.

But: Data subjects should nonetheless be provided with evaluation **criteria** and **aggregated results**.

# Complaints - example

- Access to personal data in recruitment procedure;
- Marks for each section made available, but…
- ***not*** the reasons for these marks.
- EU body: “made available orally”, “in writing would endanger secrecy of selection board proceedings”.
- EDPS: if orally does not compromise secrecy, no justification to deny comments in writing.

# Supervision & Enforcement

## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Supervision & Enforcement

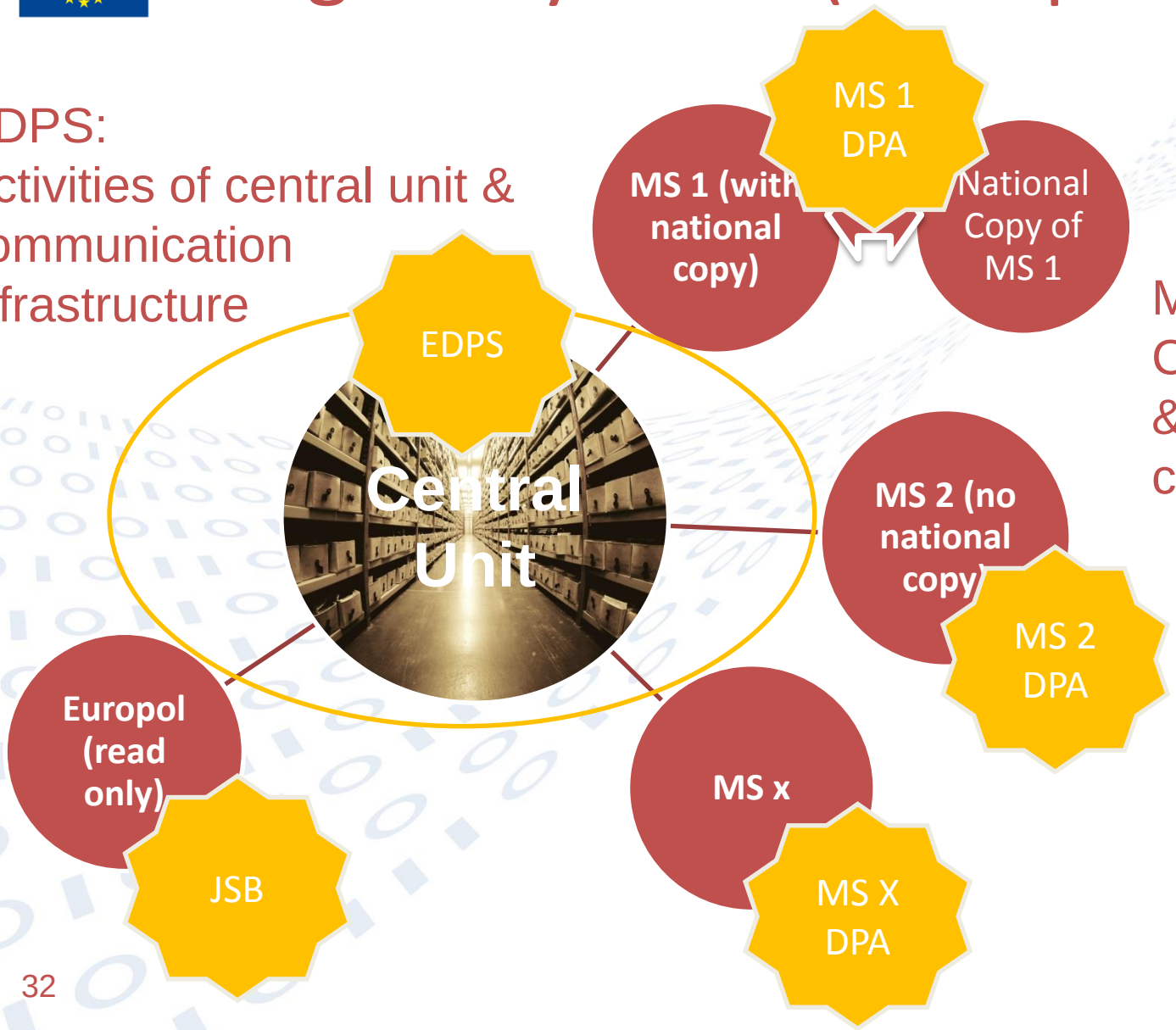
## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases


ESTE EDIFICIO
ESTA VIGILADO
POR CIRCUITO CERRADO
DE VIDEOCAMARAS
FOR MORE INFORMATION CONTACT THE SECURITY SECTOR OF THE OAMI

# Large IT systems (example: SIS)

EDPS:
Activities of central unit & communication infrastructure




MS DPAs:
Content entered & use of content by MS

# Supervision & Enforcement

## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Supervision & Enforcement

## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Example: Video-surveillance

- 2009 stakeholder consultation
- Providing guidance: 2010 Video-surveillance Guidelines (GL) (see www.edps.europa.eu)
- Promoting accountability: obligation to *comply and demonstrate compliance* with the GL
  - Discretion EU administration on how to design each system;
  - GL recommend organisational practices such as safeguards, a video-surveillance policy and periodic audits;
  - If particularly high risks for fundamental rights (e.g. covert surveillance): privacy and data protection impact assessment + prior checking by EDPS.

# Example: Video-surveillance

- Awareness raising: 2012 Follow-up Report
  - Systematic and comparative analysis of the status reports received from over forty EU institutions and bodies;
  - Highlights best practices and shortcomings on compliance.
- Monitoring of compliance on-the-spot:
  - Inspections conducted between 15 June and 18 July 2012 on the premises of 13 Brussels-based EU institutions and bodies;
  - Limited scope (see press release: www.edps.europa.eu):
    (1) Existence, location & content of on-the-spot notice,
    (2) Availability and content of a data protection notice and
    (3) Online CCTV policy.
  - Repeat exercise July 2013: four Luxembourg-based entities.

# Example: Video-surveillance

**Appendix 2 of the Guidelines contains a sample on-the-spot data protection notice**:

[Insert your video-surveillance pictogram: you may consider, for example, the ISO pictogram or the pictogram customarily used where you are located.]

For your safety and security, this building and its immediate vicinity is under video-surveillance. No images are recorded.
[Alternative: The recordings are retained for 48 hours.]

For further information, please consult www.*domainnameofyourinstitution*/cctv or contact the Agency's security unit at [telephone number and email address].

[Include multiple language versions when applicable.]


## On-the-spot notices video-surveillance



Arts. 11 + 12 Reg. 45/2001

# Supervision & Enforcement

## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Supervision & Enforcement

## Promote a ‘data protection culture’

- **Prior-checking opinions:** specific risks
- **Complaints:** processing by EU bodies
- **Consultations** on administrative measures
- **Inspections / visits**
- **Monitoring exercises** - visit www.edps.europa.eu
- **Thematic guidelines** on e.g. recruitment, CCTV
- **Awareness raising**
- **Court proceedings**: interventions in staff cases

# Powers of the EDPS



Art. 47 Reg. 45/2001

# The EDPS


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

# Monitoring technology

Assess technological developments that challenge privacy and data protection by

- Advising on policy opinions (cloud, drones, anonymisation, tracking, Internet of Things, biometrics, smart borders…);
- Technology monitoring, e.g. IPEN – Internet Privacy Engineering Network, Guidelines (websites, mobile devices, cloud computing)…

Art. 46(e) Reg. 45/2001

# The EDPS

Vision: Help the EU lead by example in global dialogue on data protection and privacy in the digital age.

The EDPS Strategy

2015-2019

# Three takeaways:

Use startpage.com or similar;

Ask yourself: why do we process this information?

Talk to your DPO!

EDPS

# thank you!

# Q? A!

@EU_EDPS

**For more information:**

www.edps.europa.eu

edps@edps.europa.eu