EUROPEAN DATA PROTECTION SUPERVISOR

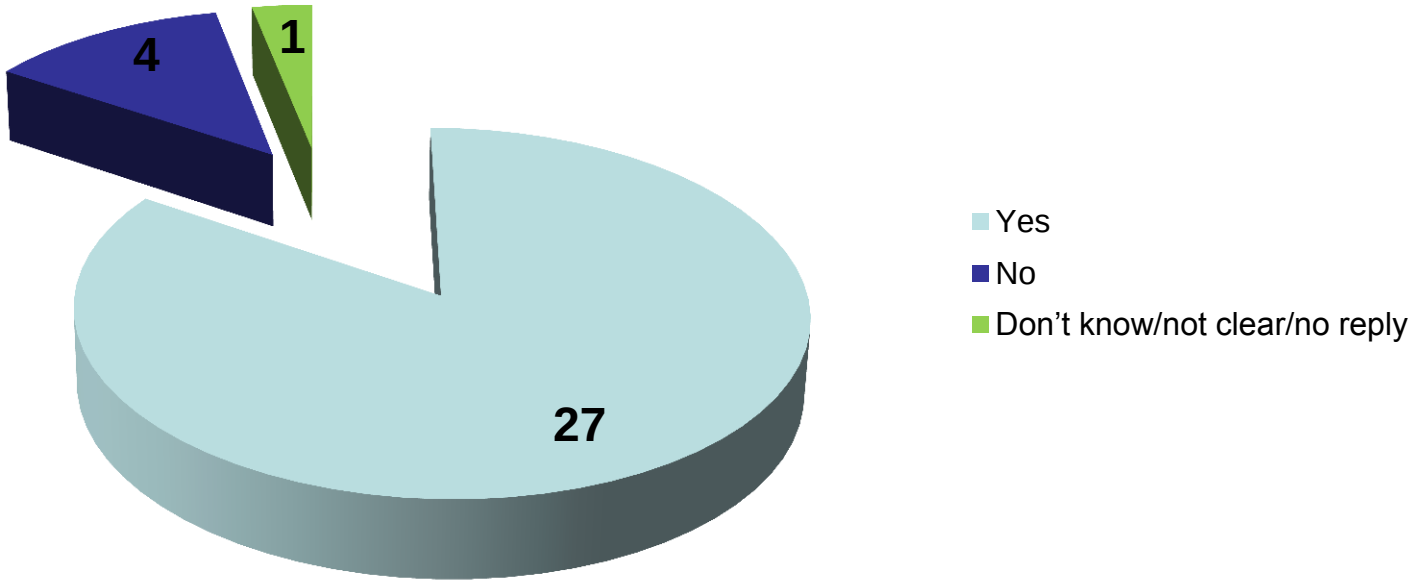
EU institutions websites workshop

19/09/2013

9.15 – 9.30

Survey results – EU public websites

Do you process personal data through websites?



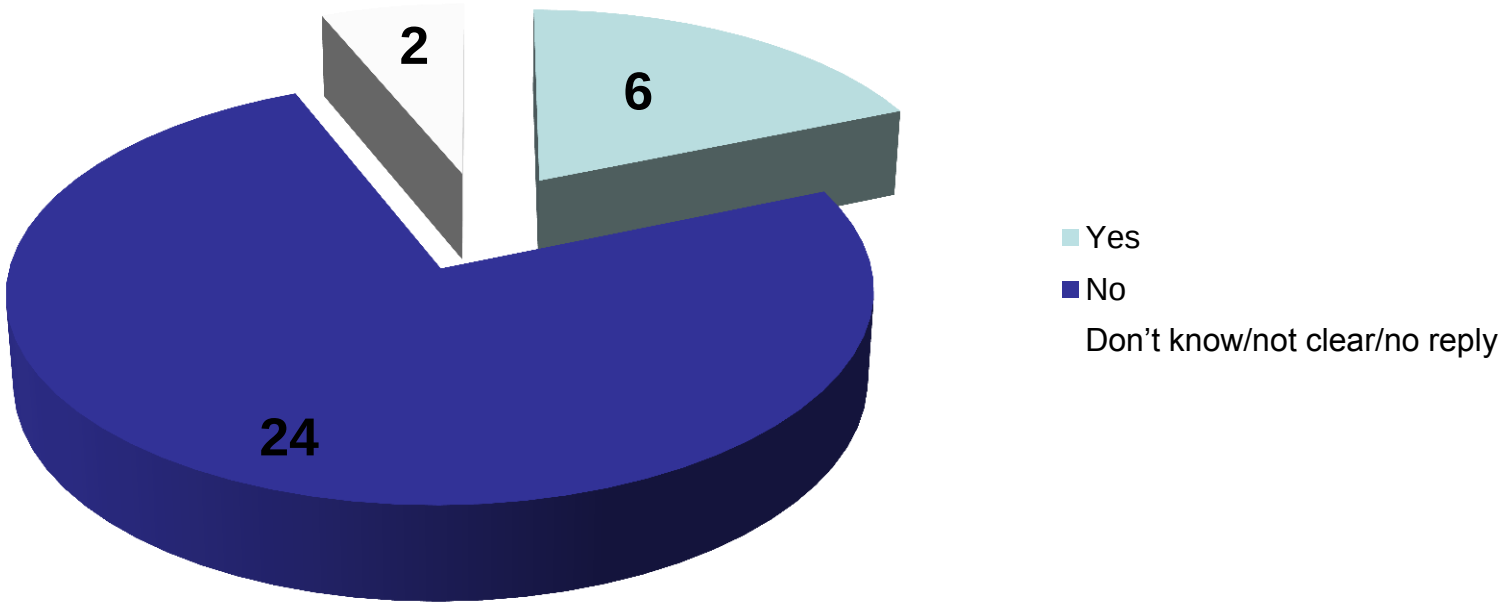
EUROPEAN DATA PROTECTION SUPERVISOR

Tools used to process personal data

- Web forms to collect personal information
- Data are stored in databases
- SSL to protect data in transit
- Logs and cookies (in a small number of cases)

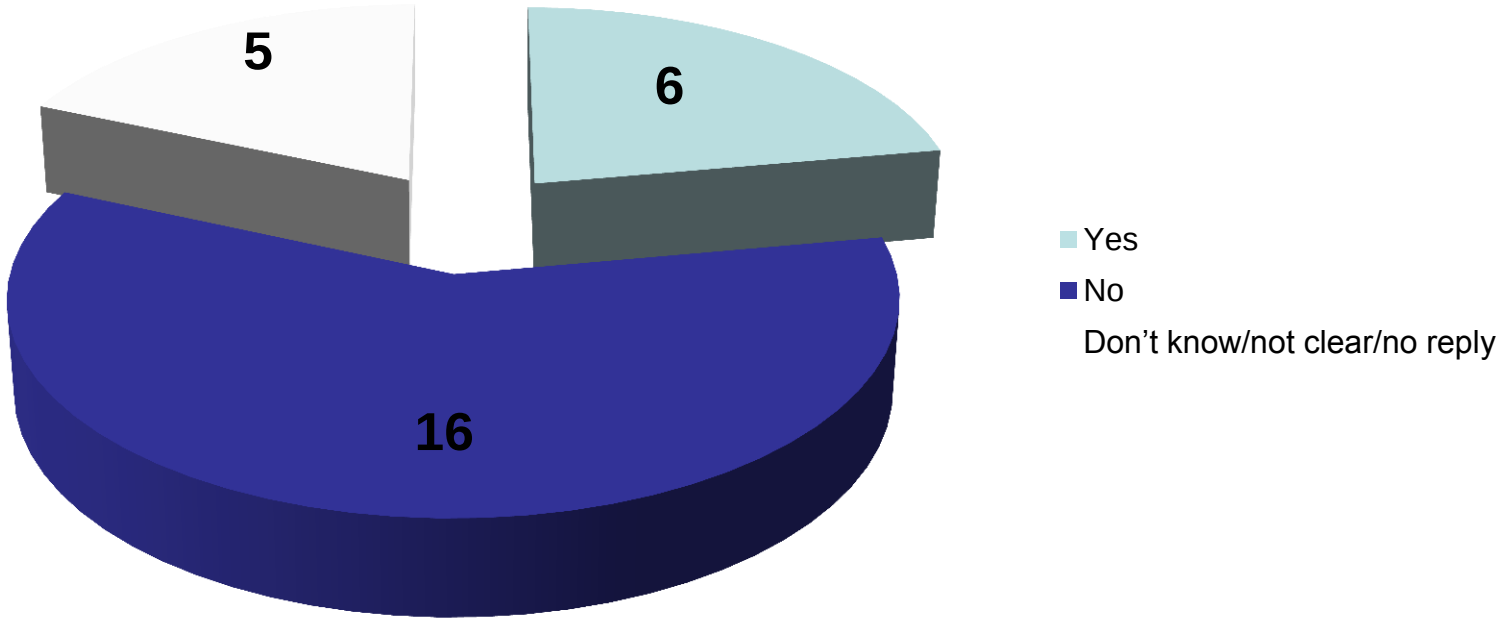
Mobile apps to access public websites

Do you provide mobile "apps" to access your websites?



Management of risks to personal data

Have you carried out a risk assessment?



EUROPEAN DATA PROTECTION SUPERVISOR

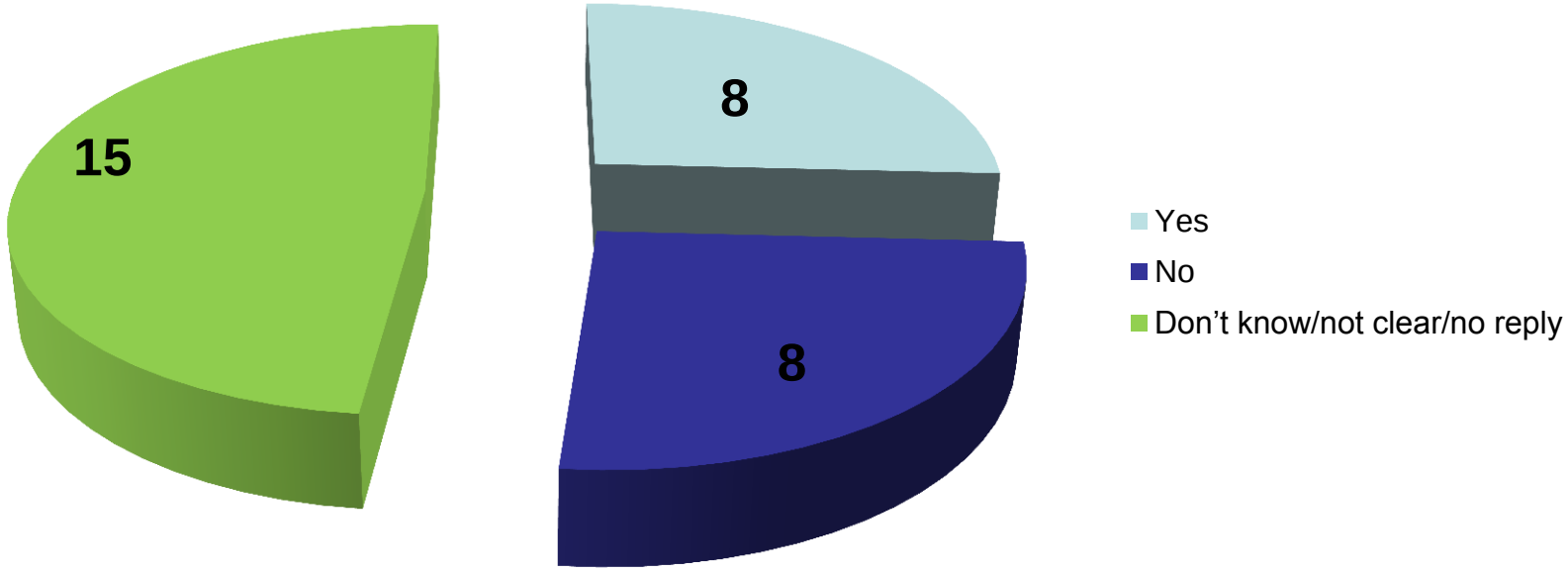
Risk treatment & countermeasures

These include…

- Access control
- Data/ password encryption, SSL for data in transit
- Secure development
- Network IDS, penetration testing
- Firewall
- Separation of environments
- Logs
- Liaison with EU-CERT
- Awareness of most common security threats
- Contractual clauses with external contractors
- Data minimisation, privacy notices, audits etc…

Security

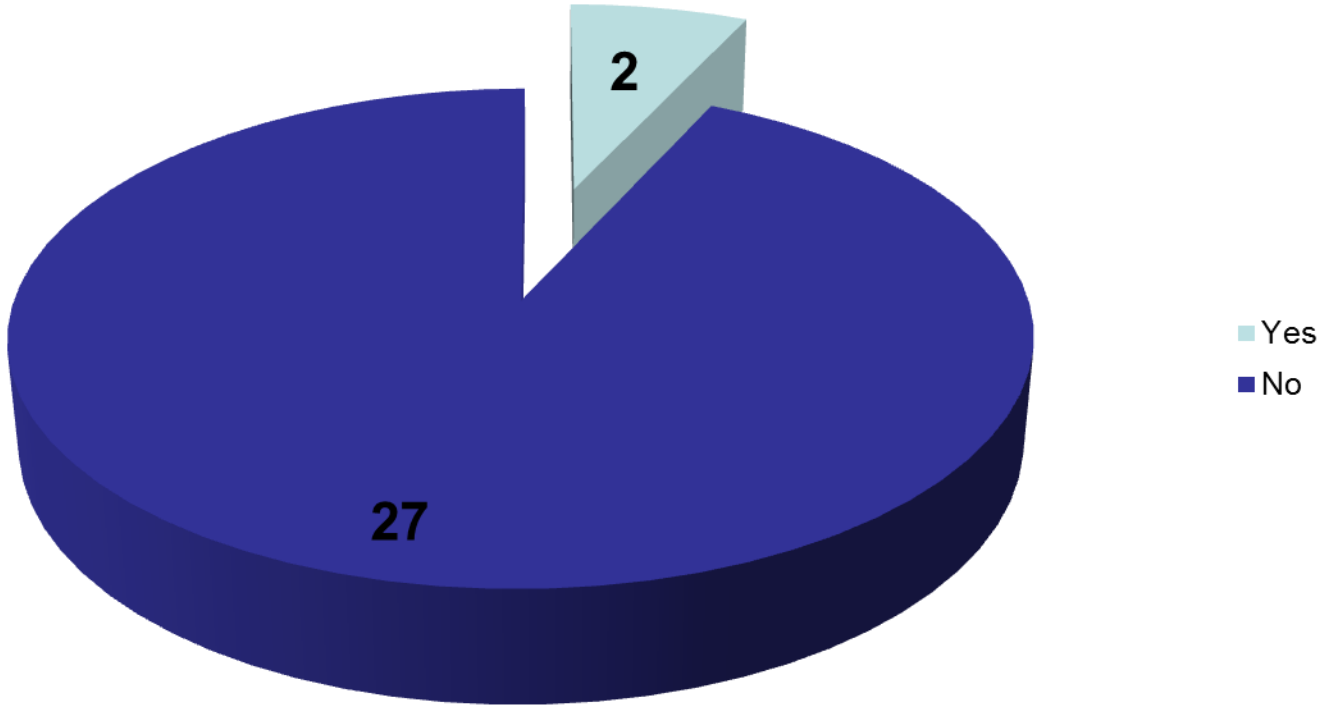
Do you have any security policies for web site development, operation and maintenance?



EUROPEAN DATA PROTECTION SUPERVISOR

Incident management

Has any security incident occurred to date?



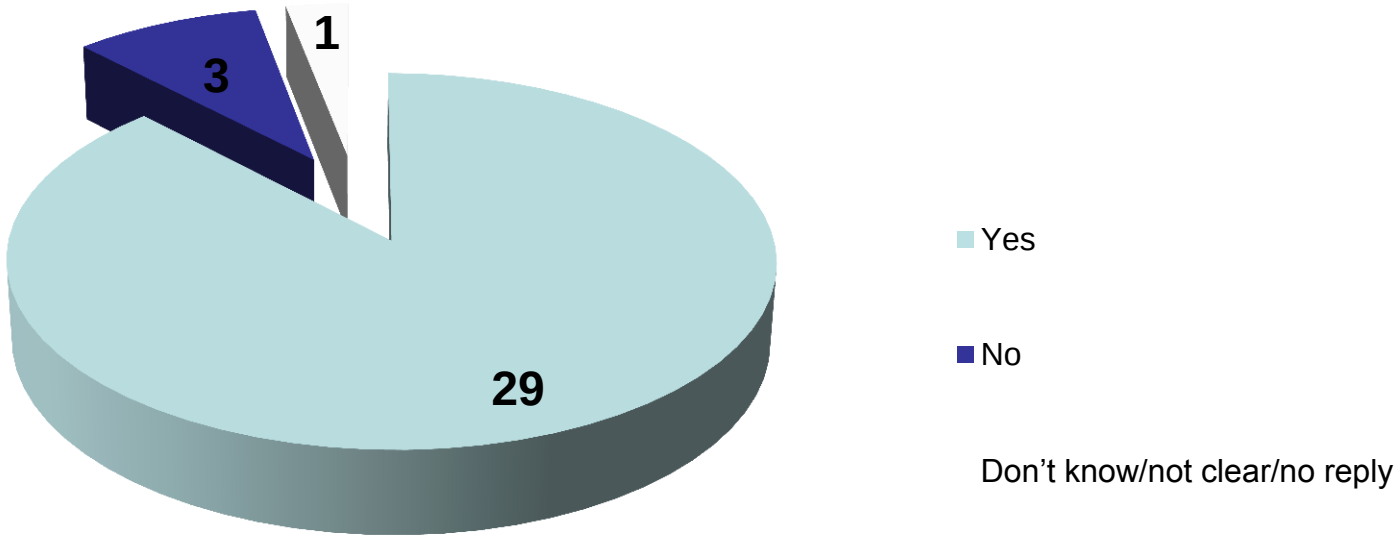
EUROPEAN DATA PROTECTION SUPERVISOR

Privacy by design & by default

- Less than half of institutions involve the DPO at website design phase
- Contractual clauses with external contractors
- Cookies disabled by default
- Data minimisation
- A few have NO privacy by design approach

Cookies and client side scripts

Do you use cookies or scripts ?



EUROPEAN DATA PROTECTION SUPERVISOR

Use of cookies

- Most for session management, user preferences and half for statistics (analytics)
- Most say they do not process personal data through cookies
- Some say they collect IP addresses
- Client scripts not used to read or write on client side

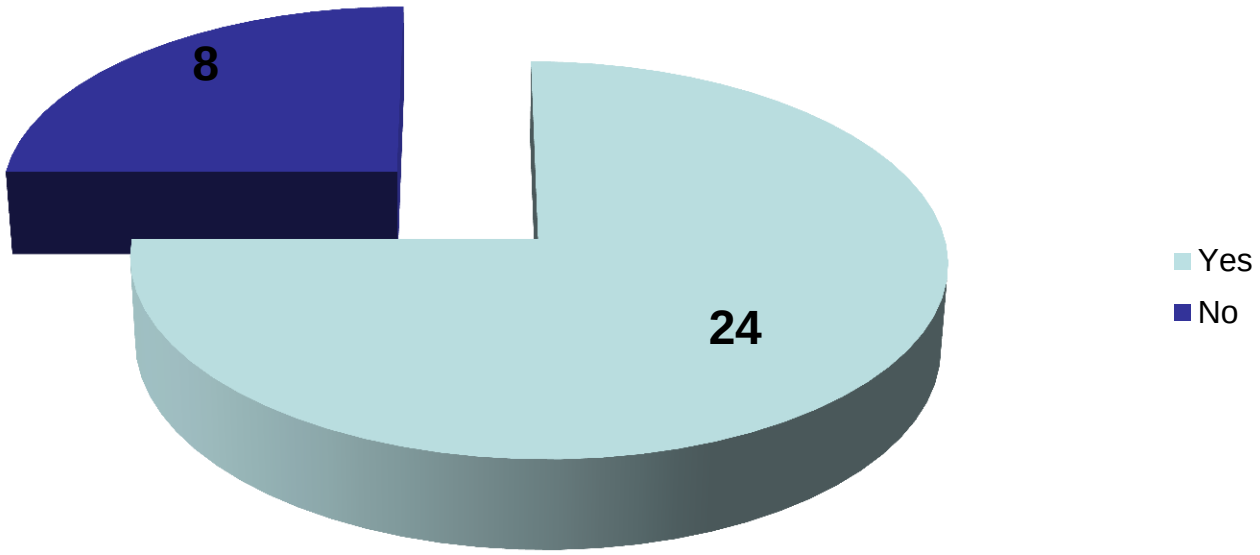
EUROPEAN DATA PROTECTION SUPERVISOR

Compliance with EU rules on cookies

- Described in legal notice
- Not always clear what the applicable rules are
- Some do not provide any explanation
- EC Guidelines issued on use of cookies for EC departments' websites

Tracking

Do you track your websites users?



EUROPEAN DATA PROTECTION SUPERVISOR

Processing by third parties

- 13 institutions declared use of Google Analytics
- Research into other software allowing processing on institutions' own servers
- Analytic software building statistics over logs
- External mailing/ newsletter service
- YouTube
- Embedded social websites software to share pages
- Use of external contractor pages or tools

EUROPEAN DATA PROTECTION SUPERVISOR

9.30 – 10.00

Accountability & data protection Management

- Data controller responsibility/ DPO roles
- Adoption of policies
- Website design, development, operation & maintenance - in light of data protection requirements
- Data protection risk assessment
- Privacy by design and by default

EUROPEAN DATA PROTECTION SUPERVISOR

10.00 – 10.30

Collection & further processing of personal data by EU websites

- Legal basis
- Adequate, relevant and not excessive
- Compatibility with purpose of collection
- Retention
- Website features to ensure data quality
- Information provided to data subjects
- Special categories of data & appropriate safeguards

EUROPEAN DATA PROTECTION SUPERVISOR

10.30 – 11.00

Cookie management, scripts & web tracking

- Tracking technologies & mechanisms
- Risks to privacy & other fundamental rights
- Legal rules
- Compliance with EU rules on cookies, including consent
- Information to data subjects
- IP addresses & other identifiers
- “Do not track” notifications
- Third party tracking

EUROPEAN DATA PROTECTION SUPERVISOR

11.15 – 11.45

Processing of personal data by third parties

- Data protection requirements in relation to procurement and data processors
- Third party analytics, behavioural advertising cookies, social networking, content management website components & cookies – **safeguards?**
- International transfers
- Information to data subjects about international transfers

EUROPEAN DATA PROTECTION SUPERVISOR

11.45 – 12.15

Website security, access monitoring/ logging and access restriction

- Security risk management process & policies
- Involvement of DPO in website security management
- Web protocol confidentiality & integrity, including backups
- Access restrictions
- Information to data subjects
- Privacy by design measures in terms of security
- Necessity & proportionality when following up incidents

EUROPEAN DATA PROTECTION SUPERVISOR

12.15 – 12.45

EU-made mobile apps

- Risks to privacy & other fundamental rights – **safeguards?**
- Legal rules, including consent & information to data subjects
- Purpose limitation, data minimisation, necessity
- Secure development policies and best practices of controllers & contractors. Contained in **contracts?**
- Processors & transfers
- Testing of app vulnerabilities, security countermeasures & patching
- Security of apps developed for children

EUROPEAN DATA PROTECTION SUPERVISOR

12.45 – 13.00

Summary, conclusions and next steps

EUROPEAN DATA PROTECTION SUPERVISOR

Process towards Guidelines (websites and mobile devices)

- Survey
  - Start collecting facts and understanding institutions reality
- Workshop
  - Orientation document for further insight and first perspectives
  - Other exchange opportunities as requested (IT managers, webmasters etc.)
- Draft guidelines (tentatively Oct 2013)
  - Your feedback on draft guidelines (tentatively Nov 2013)
  - Final consultation (?)
- Guidelines