EDPS

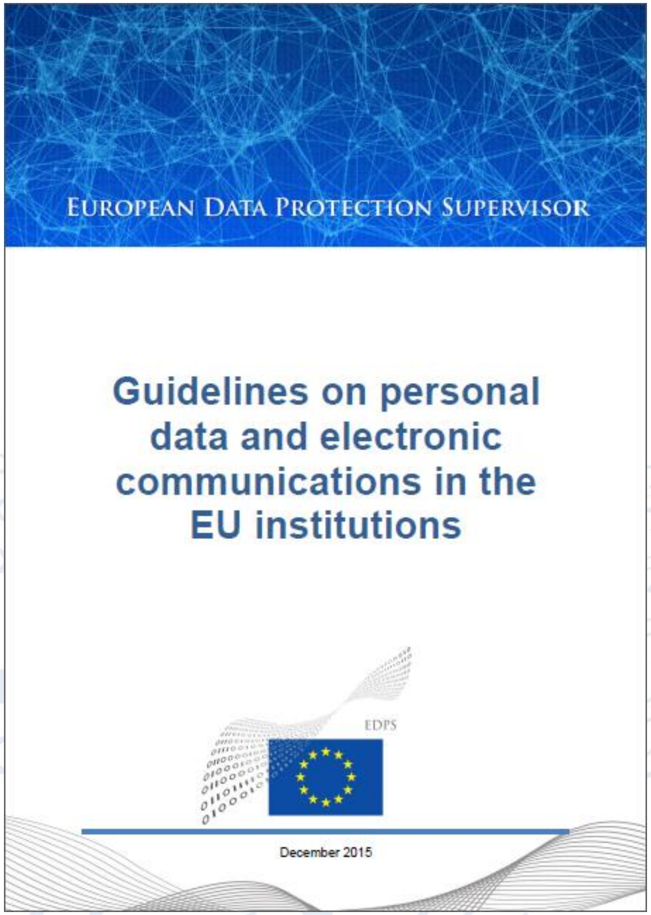
EUROPEAN DATA PROTECTION SUPERVISOR

Workshop eCommunication Guidelines

DPO-EDPS meeting
28/04/16

@EU_EDPS
#DPO

Agenda



EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on personal data and electronic communications in the EU institutions

EDPS

December 2015

- Introduction
  - Process
  - Quick overview of content
- Three case studies
  - Access to mailbox of former staff member
  - Web monitoring
  - Recording of telephone lines
- Conclusion & Discussion

Introduction

- Why eComms GL? Similar problems in all institutions, same rules in Regulation 45/2001
- EDPS had quite a number of complaints and consultations relating to eComms
- Not necessarily prior-checkable

⇒ Guidelines offer opportunity to have common standards.

⇒ Avoiding common problems

⇒ No need to re-invent the wheel each time

Introduction

- Process
  - Based on past cases (prior checks, consultations, complaints) & Article 29 WP Opinions
  - Consultation of all DPOs late 2014 to early 2015
  - During 2015: redrafting for “new style”
  - Early December 2015: sneak preview for DPO quartet
  - Adoption 16/12/15
- Approach:
  - “Hands-on”: less jargon, more examples, concrete guidance => audience-oriented
  - Specific part: “When doing X, do Y”
  - General Part: “When processing personal data, think of Z”

Introduction

- In scope:
  - Security and traffic management
  - Billing and budget management
  - Authorised use
  - Recording dedicated phone lines
  - Access to e-mail in absence of employee
  - Use of eComms data in administrative inquiries and disciplinary proceedings
- Out of scope:
  - Identity and access management
  - User activity monitoring (e.g. productivity monitoring)
  - Remote sessions
  - User-user and user-server communication in internal networks (instant messaging, internal websites)
  - Public websites

Introduction

- 24 recommendations in total
  - 12 on specific processing operations
  - 12 on general approach
- Main lines
  - Think about what you need to fulfil your business needs and limit yourself to that
  - Define what you do, document it
  - Tell people about it

Three Case Studies

- Presentation of the case
- Discuss 15 minutes with your neighbour(s)
- Some answers
- Q&A

Case Study 1: access to email

- A Staff member left recently
- Important information missing from his case files
- Information very likely in his mailbox
- Staff member is hard to reach
- HoU wants to recover information from mailbox
- HoU asks for advice on policy to ensure business continuity in such cases

Case Study 1: access to email

1. Are there different possibilities for reaching the stated goals? Which one is the least intrusive?
2. How should the approach taken be documented, both on a policy level and on the level of specific cases?
3. How to tell persons affected by the processing about it?
4. Is it a problem that Mr Baggins may be hard to reach?
5. Are there specific mailboxes that are "off-limits"?
6. What is the best basis for such a policy?
7. Variation: there is a policy stating that mailboxes of former staff are kept for two months after departure. Mr Baggins left three months ago. However, Mr Gamgee, the head of IT, tells you that this automatic deletion has in fact not been implemented and that the mailbox would still be available. Can it be accessed?

Case Study 1: some answers

1. Prevention is the best treatment: functional mailboxes, case management, handover notes, out-of-office notices (R9).
2. Internal decision, communicated to staff; specific cases to be documented (R10).
3. Let them know in advance by communicating the policy, possibly again just prior to departure; inform where possible when actually used (R10, R17).
4. Article 12(2) of the Regulation: no need to inform when “impossible or disproportionate effort” (prior information as safeguard); document it! (R17)

Case Study 1: some answers

5. Think of confidentiality expectations (DPO, staff committee, medical service)
6. This is one of the cases where consent in the employment context does not really work: what would you do if they say no? Better basis: business continuity as part of 5(a) + recital 29 (p. 15)
7. Legitimate expectations: don’t do it (or go Article 20 and document it)

Case Study 2: web monitoring

- Staff member suspected of excessive private use of internet access and dereliction of duty
- HoU has suspicion but no proof
- HoU asks HoIT orally to have logs
- Institution has an acceptable use policy allowing limited private use, AI&DP rules make reference to using logs

Case Study 2: web monitoring

1. Are there different possibilities for reaching the stated goals? Which one is the least intrusive?
2. How should the approach taken be documented, both on a policy level and on the level of specific cases?
3. How do you tell persons affected by the processing about it?
4. Are there specific requirements for the format of Ms Kilmister's request?
5. What would be an appropriate approach for detecting and/or stopping excessive private use?

Case Study 2: some answers

1. Blacklisting certain sites may be less intrusive than monitoring use (R6)
2. Internal decision, tell staff (R11, R17)
3. In general: acceptable use rules // specifically: individual notification; use of Article 20 may be possible (R17, R19)
4. Follow procedure in internal decision (R11, R21)
5. Gradual increase of how close you look (R6)

Case Study 3: call recording

- Plans to record incoming calls to
  - Internal emergency line
  - IT helpdesk
  - General inquiry line
- Purposes not clearly defined

Case Study 3: call recording

1. Are there different possibilities for reaching the stated goals? Which one is the least intrusive?
2. How should the approach taken be documented, both on a policy level and on the level of specific cases?
3. How do you tell persons affected by the processing about it?
4. For which purposes may the calls be recorded?
5. Who should be consulted on (and when) these new policies?

Case Study 3: some answers

1. Is it really necessary? Define purposes and stick to them (R7, R16)
2. Have internal rules and communicate them (R7)
3. Inform both callers (e.g. website, announcement) & staff (e.g. notice) (R8).
4. Depends on purpose of the line, e.g. emergency line replay for better understanding (R16)
5. You of course, concerned staff etc. – at a stage where changes can still easily be made.

Conclusion & Discussion

- The very short version: make sure controllers know what they're doing, why they're doing it and that they tell people about it
- Guidelines are a living document – let us know what we missed!
- Q? A!

Thank you for your attention!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS

#DPO

Backup slide: explanation of recommendations

Security and traffic management

- R1: Define the content of security logs and their conservation periods according to the security needs of your institution
  - Think of what you need, for how long and how you can avoid collection in the first place.
- R2: Data collected for security monitoring purposes must only be used for those purposes
  - Specific purpose limitation for security logs!
- R3: Ensure that statistics generated are anonymous.

Billing and budget management

- R4: Instruct external providers to minimise the amount of personal data provided to the institutions for billing purposes wherever possible
  - E.g. asking to remove last digits of numbers dialled.
- R5: Define conservation periods based on the periods for contesting invoices
  - Methods for re-invoicing private use: declaration ex-post, request to switchboard, PIN code => up to you!
  - If longer conservation is needed for other purposes (financial, auditing), then restrict access accordingly.

Authorised use

- R6: Adopt a progressive approach towards monitoring the authorised use of eCommunications Services.
  - Be transparent about what you do (documentation).
  - Blacklists for websites instead of constant use monitoring.
  - Analysis of logs should first be on no-name basis, progressively going closer where necessary (e.g. reminder to all staff / warning to department / …).
  - Individual monitoring only within defined procedures & with documentation.
  - Phones: targeted verification – e.g. invoices exceeding a pre-defined limit.

Recording dedicated phone lines

- R7: Adopt an administrative measure detailing how and why phone calls need to be recorded
  - Documentation!
- R8: Inform both callers and staff about the (possible) recording of phone calls before it happens.
  - Communicate policies to staff.
  - For callers, have e.g. pre-recorded message while waiting for operator to pick up, info next to phone number on website…

Access to e-mail in absence of employee

- R9: Take precautionary measures to reduce the need for accessing personal mailboxes for business continuity purposes
  - Instruct staff to save relevant mails in case management system / have service mailboxes / ensure proper handover.
- R10: Adopt a policy on accessing staff mailboxes in the absence of staff members.
  - Documentation! Information to staff (both general and specific).
  - This is not about consent.

Administrative inquiries and disciplinary proceedings

- R11: Make sure that access to eCommunications data is covered under the rules for administrative inquiries and disciplinary proceedings
  - No blanket access => individual suspicion
  - Investigating authority to assess necessity.
- R12: Provide adequate safeguards when planning covert surveillance
  - This is subject to prior-checking!
  - Proper legal basis, targeted authorisation, register, no less intrusive means available.

General Recommendations

- Basic DP principles (R13 to R16)
  - Purpose specification, data minimisation, conservation periods, (in)compatible further use.
- Information and data subject rights (R17 and R18)
  - Tell them!
  - Make exercising data subject rights easy.

General Recommendations

- Notifications and documentation (R19 to 22)
  - Risk management process, defined policies, notifications – everything up-to-date and reviewed as necessary!
- Outsourcing (R23 and R24)
  - Make sure contractors know what (not) to do (=> contract clauses and instructions) and verify that they stick to what they signed (=>audits, reporting…).