SERIES

"How to…" Data Protection: Printing of personal data

MAX PLANCK GESELLSCHAFT

WHAT NEEDS TO BE OBSERVED WHEN PRINTING/SCANNING PERSONAL DATA?

Personal data, whether in digital or analogue form, must be protected against destruction, loss, modification and disclosure. Especially printers/scanners (office printers/printers in the hallway, multifunctional devices) can constitute a potentially vulnerable spot, which is why various technical and organizational measures need to be taken. However, the use scenarios on site must also be taken into consideration in order to design such measures in an appropriate manner.

Demands and requirements

- Legal requirements pursuant to the GDPR:
  - Art. 25 ("Privacy by Design"; "Privacy by Default") and Art. 32 ("Security of Processing")
- MPG requirements:
  - General Works Agreement Security, Section 6, para. 1: Where personal data is processed in a client/server environment, all personal data must be encrypted during transmission on the network.
  - General Works Agreement Virtual Desktop, Annex 1, Section 3.2, Paragraph 1: The Institute's/facility's printing and scanning infrastructure must ensure that personal data is transmitted only in encrypted form. This provision applies to printing from the virtual desktop (vAP).

Preparatory considerations for application scenarios

- Who prints/scans and what is being printed/scanned?
  - Are only individual employees affected or one or more departments or even the entire Institute/Facility?
  - What level of protection apply to the data to be printed/scanned? (MPG Data Protection Level Concept, forthcoming Guideline on the Classification of Values for IT Security)
- What is the current configuration of my printer infrastructure?
  - Wireless printers/printers in the hallway, personal office printers (wireless/via cable), is there a central or local printer management in place?
- Have any security measures been taken yet? Are there any gaps remaining? Can I fix them within a short time with few available (financial, human) resources? (E.g. what can be done with the existing infrastructure, do I only need to configure it?)
  - Do I need new technology? If this is the case, for the entire Institute/Facility or only for certain individuals? (pursuant to the GDPR implementation costs, type/scope of data processing, "risk assessment")
- State of technology, adequacy: Does it make better sense to equip a few people with the required technology or to equip the entire Institute/Facility?
- Is user training required as an additional organizational measure? (Prompt collection of printouts, necessity for printouts, etc.)
- And, last but not least: Is this only relevant to the administration/virtual desktop? What are the regulations for the rest of the Institute/Facility? Are employee data or personal data of third parties (test persons, contact lists, applicant data, ...) also being printed out in other areas of the Institute/Facility?

Possible technical and organizational measures

- Encryption of data traffic in line with the state of technology,
- separate printer network, use of print servers,
- encrypted hard disks inside the printers,
- data protection-compliant erasure/disposal of printer hard disks,
- authentication vis-à-vis the printer (PIN, RFID chip, ...),
- follow-me technology,
- user training/raising awareness,
- deletion of the printer queue at regular intervals or in case of error,
- regulations for printing in the home office,
- placement of printers in protected areas

The Data Protection Officer for the Max Planck Society
Tel.: +49-89-2108-1554 Email: datenschutz@mpg.de

Organisationshandbuch: Chapter XVII
Intranet: https://max.mpg.de/Zentrale-Beauftragte/Datenschutz/Pages/Datenschutz_EN.aspx