Outlook

RE: Request for Guidance: Use of Email for Transmitting (Special Category) Personal Data in Public Printing and Scanning Services

From Eleri Karu - AKI <eleri.karu@aki.ee>
Date Fri 2025-08-15 14:30
To Camilo Botero <camilo@princh.com>

Dear Camilo Botero

The Data Protection Inspectorate has received your inquiry regarding the use of email as a transmission channel for personal data, including special category data, in the context of document printing and scanning services offered by public libraries.

The Inspectorate can only provive general explanations based on the General Data Protection Regulation (GDPR). These explanations reflect the Inspectorate's understanding of the relevant provisions and practices but do not constitute legal advice. The Inspectorate only issues binding legal assessments during supervisory proceedings. As no proceedings have been initiated at this time, we are unable to provide a preliminary assessment without knowing all the facts.

The use of standard (unencrypted) email for transmitting personal data—particularly special category data—raises significant concerns under Article 5(1)(f), Article 9, and Article 32 of the GDPR. These provisions require that personal data be processed in a manner that ensures appropriate security, including protection against unauthorized access or disclosure. While the GDPR does not categorically prohibit the use of email, it requires that the chosen communication method be proportionate to the risks involved. In practice, unencrypted email is generally not considered sufficient for transmitting sensitive or special category data unless additional safeguards are in place.

Under Article 32 GDPR, controllers and processors must implement appropriate technical and organisational measures. In the context of email-based printing and scanning services, the following are typically expected:

- TLS encryption for email transmission is a baseline expectation, but it does not provide end-to-end protection.
- End-to-end encryption is strongly recommended, especially when special category data is involved.
- Access controls, logging, and data minimisation should be implemented on both the sending and receiving systems.
- Data retention policies should ensure that documents are not stored longer than necessary.
- The absence of end-to-end encryption may be considered a risk that requires mitigation, particularly if the data includes health, legal, or financial information.

For public libraries offering these services could fall under the lawful basis under Article 6(1)(e) (task carried out in the public interest). For special category data, Article 9(2)(g) (substantial public interest) or Article 9(2)(a) (explicit consent) may apply, depending on the context and safeguards in place. Explicit consent may be required if no other Article 9 condition is clearly applicable. The Inspectorate recommends reviewing the relevant sections of the GDPR and Inspectorate's website for further clarification because it is the obligation of the data controller to provide a legal basis. For any further clarification of the roles, you should also decide this on your own or consult a legal firm.

Given the involvement of special category data, third-party processors, and potentially insecure transmission channels, a DPIA is likely required under Article 35 GDPR.

If you deem that a DPIA is necessary, the assessment should cover at least the following:

- Risks of unauthorized access or data breaches during transmission.
- The adequacy of encryption and access controls.
- The legal basis for processing and data minimisation practices.
- The roles of all parties involved and contractual safeguards.

Sincerely

Eleri Karu

Data Security Expert
eleri.karu@aki.ee
+372 627 4146

ERAELU KAITSE JA RIIGI LÄBIPAISTVUSE EEST
Tatari 39 | 10134 Tallinn | Eesti
LinkedIn | YouTube

ANDMEKAITSE INSPEKTSIOON

From: Camilo Botero <camilo@princh.com>

Sent: Wednesday, July 30, 2025 2:28 PM
To: info - AKI <info@aki.ee>
Subject: Request for Guidance: Use of Email for Transmitting (Special Category) Personal Data in Public Printing and Scanning Services

---

Dear Data Protection Inspectorate,
I am contacting you to request your authoritative guidance regarding the use of email as a transmission channel for personal data, including special category data, in the context of document printing and scanning services offered by public institutions, specifically public libraries.

Context:
In many EU Member States, public libraries provide services that allow patrons to print or scan personal documents using solutions provided by third-party service providers. These third-party solutions commonly operate in the following ways:

a) Printing: Users submit documents to be printed by emailing them to a designated email address. This inbox is managed by the third party and processed by their server, which extracts the attachments (and sometimes the email body) and routes the content to the print queue at the library.
b) Scanning: Users scan a document at the library scanner, and the system sends the digital version (typically a PDF) to the user's email.

In both scenarios, personal data, including potentially special category data under Article 9 of the GDPR, is transmitted via standard email protocols, without additional client-side encryption or secure portal mechanisms.

Given the sensitivity and structure of this processing operation, I would greatly appreciate your guidance on the following specific legal and technical questions:

1) Legality of Email as a Transmission Channel:
In your view, is the use of standard (unencrypted) email by or on behalf of public institutions a legally appropriate and GDPR-compliant method for transmitting personal data, including special category data, under Article 5(1)(f), Article 9, and Article 32 GDPR?
2) Minimum Safeguards:
2.1) What technical and organisational measures (TOMs) would you consider minimally necessary in this context to meet the standard of "appropriate security" under Article 32 GDPR? Specifically:
2.2) Is encryption (at rest and/or in transit) mandatory or strongly recommended?
2.3) Would the use of TLS-based email transmission be considered sufficient?
2.4) Does your authority view the absence of end-to-end encryption as a risk that must be mitigated?

3) Legal Basis and Special Category Conditions:
Assuming special category data is involved (e.g. health, financial, or legal documents):
3.1) What lawful basis under Article 6 and special condition under Article 9 would be appropriate for this type of public service provision?
3.2) Must explicit consent be obtained, or could another ground under Article 9(2) be applicable?
4) Role Distribution and Responsibilities:
4.1) How should the roles and responsibilities under GDPR be assigned in this setup?
4.2) Is the library the controller and the third-party provider the processor, even if the email address to provide the service belongs to the third party?
4.3) During the transmission phase—specifically from the moment the end-user sends the document until it is received by the provider's server—who holds primary responsibility for ensuring compliance with data protection obligations and safeguarding the data?
4.4) Are there specific contractual clauses or controller–processor agreements you would expect to be in place under Article 28 GDPR?
5) DPIA Requirements:
5.1) Would this type of data flow (involving potentially sensitive documents, use of third parties, and transmission via email) trigger a legal obligation to carry out a Data Protection Impact Assessment under Article 35 GDPR?
5.2) If so, what specific risks should such a DPIA assess and mitigate?

Your expert view will be instrumental in ensuring alignment with national interpretations and enforcement expectations. I would be very grateful for your response and for any existing guidance your authority has published on this matter.