Privacy protection and e-document management in public administration

Dr. Iur. **Olga SOVOVA**[1], Ph. D.
Miroslav SOVA[2], MIT
Dr. **Zdenek FIALA**[3], Ph. D.

Abstract

The paper reviews and critically examines sharing e-document-based information between public administration and private sector. The documents are not only generated and archived, but also shared among public administrators. The private sector supports digitisation and computerization of public administration. The protection of privacy of persons and confidential information, especially economic about legal entities, together with the necessity of circulation of information within the national state and cross-border, bring new legal and technical challenges. The paper examines legal issues of the right of informational self-determination, privacy protection of the e-data information exchange between the public and private sector. The paper concludes that new relations to technologies form an inevitable and fundamental sign of a post-industrial society, but the professionalism of the public administration together with the duty of confidentiality and the right for privacy together with appropriate legal regulation should guarantee that technologies be used solely for legal interference with the right for informational self-determination.

Keywords: *public administration; private sector; informational self-determination; privacy protection; e-data exchange; paper document digitisation.*

JEL Classification: K24

1. Introduction

Working with information is one of the fundamental areas of managerial activities within private and public management. Information Management is a unifying discipline, which enables improvement of qualities of everyday work. Both contemporary theory and practice speak about a global information technology society, which takes many forms. Its specific types and characteristics also depend on historical and geographical conditions.[4]

[1] Olga Sovová - the Police Academy of the Czech Republic in Prague, sovova@polac.cz
[2] Miroslav Sova - the Police Academy of the Czech Republic in Prague, Miroslav.Sova@ysoft.com
[3] Zdeněk Fiala - the Police Academy of the Czech Republic in Prague, fiala@polac.cz
[4] Bell, David *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Special anniversary ed. New York, N.Y.: Basic Books 1999.p. xiv. Wilson, M. I, Kellerman, A., Corey, K. E. *Global Information Society: Technology, Knowledge, and Mobility*. Lanham: Rowman & Littlefield Publishers, Inc. 2013. p. vii. Zoubek, Vladimír Postmoderní problémy globální společnosti. In: *Bezpečnost v podmínkách organizací a institucí ČR: sborník z mezinárodní konference*. 1 Vyd.. Prague Soukromá vysoká škola ekonomických studií 2005, p. 76.

Information society is a social system in which the various fields of economy, science, technology, etc. intertwine and form a unitary one, without which the individual cannot develop to optimal parameters[5].

On the other hand, entry of information technologies and the partnership with private companies in the public administration is not only connected with advantages, but also particular risks. Both we will discuss further.

A large advantage of modern technologies is the possibility to increase efficiency of providing exchange of information within and outside the public administration, increased transparency of its costs and increased possibilities of private public partnership (PPP)[6]. Information technologies have, and will have, a significantly larger impact onto the area of responsibility of providing public administration because shared and electronically available documentation is on one side an advantage for providers and their employees; however, on the other side, indisputably creates a more space for proof of misconduct.[7]

We determine the **hypothesis** that we expect to identify two types of **possible breaches** to protected data:

- breaches to client´s privacy **by public administration and**
- breaches to the privacy **by third party companies and the public**.

Like personal safety, privacy also guarantees representation of important principles, as do fundamental values regarding individual liberties, however the safety of the general public in certain situations prevails and particular eventualities may come into conflict with those fundamental rights.[8] Thus it will be critical to monitor and correct the technologies used through the legal regulation. Based on two examples – the basic pillars of e-Government in the Czech Republic and the digitisation and the Internet of Things at public universities - we examine the above- mentioned issues and challenges and propose ideas how to minimize risks and avoid intrusions to personal rights.

Primarily the **methods of interpreting the law**, i.e. analyses of legislation and doctrinal opinions and law shall be used. Within the individual parts of the paper the methods of interpretation proceed from the general to the specific. The practical examples of connecting private and public services when using information technologies will be critically examined and discussed. Following an analysis of all this information, certain developmental tendencies in the near future could be predicted. The practical examples and their detailed examination are based on practical experience of the authors.

---

[5] Popescu, Alina, *The Right to Information and the Information Society*, in Ioana Nely Militaru, Adriana Moțatu, *Diversity and Interdisciplinarity in Business Law*, ADJURIS – International Academic Publisher, Bucharest, 2017, p. 274.

[6] See Paschal, Samson Masalu Peter, *Public-Private Partnerships: No Investment without an Investor-State Dispute Settlement or Investment Court System*, in Ioana Nely Militaru, Adriana Moțatu, *Diversity and Interdisciplinarity in Business Law*, ADJURIS – International Academic Publisher, Bucharest, 2017, p. 88.

[7] Kleinig, J., Mameli, P., Mille, S., Salane, D., Schwart, A. *Security and Privacy. Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States*. p. 9. ANU E Press. The Australian National University Canberra. 2011. ISBN 978-1-9218-6257-1.

[8] Details can be found in Pavlíček, V. a kol. *Ústava a ústavní řád České republiky. Komentář*. I. a 2. díl. Praha: Linde 1999.

In today's globalized society, notably according to current European Union (EU) standards, third parties, e.g. public administrators and private operators of technological facilities are subject to standardized requirements, such as the protection of personal data, client record and files keeping, the accounting regarding public administration provision, management as well as the archiving of documents related to their activities. In this case the legal entity or individual who is also a business proprietor is in frequently in wider conflict which often takes the form of a clash of different, often conflicting, legal obligations. These divergences among competing responsibilities regularly have an impact on the exercise and protection of fundamental rights. The paper brings research proposals de lege ferenda, especially which with regard to the needs of the General Data Protection Regulation (GDPR).[9]

2. E-government in the Czech Republic

Introduction of information technologies and information management in public administration are connected with the challenge of improving services of public administration towards the public and clients. The modern administration should be user friendly and offer addressees an easy way to communicate. **OECD describes the e-Government** as follows. "*eGovernment supports administrative processes, improves the quality of the services and increases internal public sector efficiency. Digital public services reduce administrative burden on businesses and citizens by making their interactions with public administrations faster and efficient, more convenient and transparent, and less costly. In addition, using digital technologies as an integrated part of governments' modernisation strategies can unlock further economic and social benefits for society as a whole.*" [10]

The **Czech Republic** started preparatory works for introduction of digitisation and computerisation in late nineties of the 20th century. Series of important law on digitisation has been adopted.

The Law No. 365/2000 Coll., on Information Systems of the Public Administration, started the real drive towards getting full values of information technologies not only within the public administration itself, but especially towards the public. The Law No. 308/2008 Coll., on Electronic Legal Acts and the Authorized Conversion of Documents (law on digitisation), introduced a completely new system of information exchange between the public administration, courts and other bodies of the public power (further public administration) on one hand and the private sector, addressees of the public administration on the other hand.

---

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available om-line: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. 12.11.2017.

[10] Backround Paper: Implementing E-Government in OECD Countries. Experiences and Challenges. p. 2. Available on-line: http://www.oecd.org/mena/governance/36853121.pdf. 12.11, 2017

Data mailboxes. The above-mentioned law on digitisation stipulates on **compulsory electronic legal acts of the public administration.** Any acts must be issued in a digital form and delivered via internet accessible tools. The system of electronic data mailboxes has been launched in 2009. The object of the system is to ensure quick and safe communication and accessibility of public administration at any time and from any place in the world. The Ministry of Interior as a responsible public authority opens data mailboxes to all public administration and legal entities and entrepreneurs registered in the public commercial register. Also legal professions, as public notaries or attorneys-at-law, must use the data mailbox.

The Czech Constitution Court, Supreme Court and the Supreme Administrative Court delivered several important decisions dealing with the delivery via the data mailbox. The both courts repeatedly ruled, that data mailbox affidavit of delivery is considered to be a public record as well as the paper receipt of delivery[11].

The table shows selected numbers of public administration bodies and private persons according to the administrative structure of the Czech Republic. All these entities use compulsory data mailboxes for mutual communication.

Territorial Public Administration	
Regions	14
Municipalities	6 258
Legal entities	666 124
Justice	
Courts	99
State Prosecution Office	97
Attorneys- at- law	10 000
State Public Administration	
Ministeries	14
Other Public Offices	16
Universities	
Public universities	22
State universities	2
Datamailboxes	
No of datamailboxes	845 919
Messages sent	497 540 141
Success rate of delivery	99,51 %

Source: Czech Statistical Office

[11] Decisions : Comstitutional Court II. ÚS 3042/14 available on–line : https://nalus.usoud.cz/Search/Search.aspx Supreme Administrative Court 6 Ans 1/2013, svaiůable on-line : http://www.nssoud.cz/main0Col.aspx?cls=JudikaturaSimpleSearch&pageSource=0&menu=188 Supreme Court , 8 Tdo 517/2014, 30 Cdo 2514//99, available on–line : http://www.nsoud.cz/JudikaturaNS_new/ns_web.nsf/WebSpreadSearch. 12.11.2017.

Technical and legal advantages of data mailboxes:

- quick, safe, encrypted exchange of sensible legal documents
- accessible anytimeand anywhere, also from mobile devices
- certainty of delivery; the law stipulates for the legal fiction of delivery
- the owner of the data mailbox may authorize unlimited number of persons with the right of access to the data mailbox; their rights could be limited
- private entities can exchange documents, provided they have activated the pre-paid postal service; the cost of it are half the price of any registered paper mail.

Risks of data mailboxes:

- the fiction of delivery may cause missing a deadline in court or administrative proceedings
- too many authorized persons
- authorized persons use the same password
- misuse of rights of access
- the owner of the data mailbox is liable for any malpractice
- no legal regulation of data storage
- data could be stored unprotected
- the pre-paid postal service is rarely used.

3. Digitisation and co-operation between public and private sector

Cooperation between public and private sectors oftentimes implies exchange of digital information obtained from digitising paper documents. Public authorities and other institutions often digitise and preserve paper documents created internally or received from an external source by employing various software tools. Digital documents are often made accessible not only within the boundaries of the institution, but also externally to private firms. In this section, we examine how paper document digitisation is achieved in the context of public universities and the advantages, challenges and risks of document digitisation with focus on sharing sensitive data with private companies.

Example scenarios of digitisation at public universities. Typically, education institutions including public universities manipulate with large volumes of paper documents that are digitised at some point. Such paper documents include student records, research materials and publications, contracts, and many others. In this paper, we consider two hypothetical examples of common digitisation processes applicable at public universities that will help us illustrate the concepts discussed in this section of this paper.

A typical example from the public university setting is digitisation of paper student enrolment forms and enrolment supporting documentation. The example can be summarised in the following 4 steps:

- students submit filled out enrolment forms together with supporting documents containing sensitive data (e.g. personal identification

documents, income declarations, medical records, etc.) to a university's admission office
- an admission officer at the office scans the enrolment forms and supporting documents.
- scanned enrolment forms and supporting documents are stored in the university's student records system
- the university shares selected digital documents from the student record with a private company for statistical analysis of educational measurement.

Another typical example of document digitisation from the public university setting is lodgement of **research-related expenses** by PhD students or academics. The example can be summarised in the following 3 steps:
- an academic incurs an expense related to their research projects
- the academic scans an invoice or a receipt which proves the expense
- the academic submits the scanned invoice or a receipt to the faculty accounting office for processing.

Public authorities and universities often receive and produce paper documents that are captured in a digital format using a **document capture device** such as a flatbed scanner or a high-speed multifunctional device (a multifunctional device is typically of larger size and combines, A3 and A4 paper size colour printing, copying, scanning and faxing capabilities). In the context of public universities, paper documents such as student applications and application supporting documents such as personal identification documents are placed one by one on the glass or are scanned in a batch through a feeder of a multifunctional device, which is typically shared by multiple users from one office – in our example several officers from the admissions office would share a multifunctional device to scan paper documents related to a different student application.

In addition to traditional document capture devices, the omnipresence of **camera-enabled mobile devices** such as mobile phones or tablets results in a convenient way to digitise paper documents. In our example scenario of PhD students or researchers, who may not have ready access to a multifunctional device or a scanner, expenses can be captured using a mobile device even outside the university premises. The mobile device's integrated camera application or a specialised mobile document capture application such as Genius Scan [12] or Microsoft Office Lens[13] is used to capture the image of a receipt or an invoice before submitting it to the faculty accounting office.

Typically, once documents are digitised, they are sent by a scanner or a multifunctional device to a file server, for example, to a "network drive" shared across a department or entire university, and stored in a folder structure corresponding to the student's identification number. In our example of processing student records, each student may be assigned a special folder corresponding to her student number, where student application and supporting documents are stored.

[12] See available on-line: https://www.thegrizzlylabs.com/genius-scan. 12. 11. 2017.

[13] See available on-line : https://mspoweruser.com/office-lens-app-now-lets-you-save-a-scanned-business-card-as-a-virtual-contact-file/. 12.11.2017.

Many organisations rely on e-mail as the main destination of scanned documents as e-mail is generally understood to be the prevalent communication tool for most organisations. In case where e-mail is used as scan destination, the capture device delivers the scanned documents as an e-mail attachment to a pre-defined or user-defined recipient(s). In many cases, scans are self-sent to the e-mail address of the person who scanned the document. Subsequently, the person manually processes the scanned document on her PC in some way. This manual processing could be any action from forwarding the document to a different recipient for reviewing or filing, or renaming the file and manually uploading it to a corresponding location on a file server or a university-specific Document Management System (DMS) or an Enterprise Content Management system (ECM) whose usage is being widely adopted in the Education sector[14] . DMS or ECM systems may be hosted on university premises or in the cloud. Commonly used DMS and ECM systems used in the Education domain include M-Files[15], Dropbox Education,[16] Hyland OnBase.[17]

However, for public universities where a DMS or ECM is in use, manual delivery of scanned files to these systems is not the only option. Delivery of scanned documents to a DMS or ECM is possible by sending scanned documents directly from a capture device to the destination system or by first sending it to the servers of specialised enterprise document workflow software, which routes it to a location in the DMS or ECM. We will discuss the latter case in more detail in the subsequent section.

It is important to **distinguish between "ad-hoc" and "automated" document digitisation**. In the former case, the institution does not recognise that processes that yield digital documents from paper take place on an on-going basis and every time a need to digitise paper documents, the **institution leaves the results of the digitisation process solely in the hands of its employees, students and other persons who digitise paper documents**. In such case, whoever digitises a paper document is responsible for applying a manual series of steps in order to deliver the document to the correct destination in the correct location and correct document format. In the latter case, the institution standardises the on-going digitisation processes and employs specialised enterprise digital document workflow software such as Nuance Autostore[18] or YSoft SafeQ[19] in order to pre-

[14] See available on-line: https://search.proquest.com/openview/0023c3b763af09c9a94f74a7e3cbea68/1?pq-origsite =gscholar&cbl= 1796412, http://ieeexplore.ieee.org/document/5694910/, https://cuit.columbia.edu/ecm, http://sites.uco.edu/technology/ ecms/index. asp, https://campustechnology.com/articles/2016/08/16/university-of-tennessee-migrates-to-an-enterprise-content-management-system.aspx. 12. 11. 2017.

[15] See available on-line: https://www.m-files.com/en/resources/content/application/education. 12.11.2017.

[16] See available on-line :https://www.dropbox.com/education.12.11.2017.

[17] See available on-line: https://www.m-files.com/en/resources/content/application/educatio. 12.11.2017.

[18] See available on-line :https://www.nuance.com/print-capture-and-pdf-solutions/document-capture-and-workflow/ autostore.html. 12.11.2017.

[19] See available on-line:https://www.ysoft.com/en/document-capture.12.11.2017.

define automated paper document digitisation workflows that are available and repeatable.

By digitising paper documents, institutions can significantly increase business productivity while reducing overall costs of associated with paper-based document processes. Replacing paper-based document processes with automated document workflows results in time and money savings by eliminating otherwise repetitive manual tasks.

Automated digitisation leads to improved data quality and accuracy as human error associated with manual steps in otherwise a manual human process is removed. Physical space and cost savings and removal of manual labour associated with paper document archiving are also the results of digitisation. Digital documents can be easily indexed and saved in a format suitable for long-term archival, such as the ISO PDF/A standard.[20] Replacing paper document archives with digital document archives therefore results in simpler access to document even after extremely long periods of times (e.g. 100s of years); something which can be extremely challenging with paper.

Furthermore, **document security is significantly improved with digital documents**. Paper documents can float around organisation without any control - possibly without the ability to trace the author, contributors and whether the document is an original or how many copies of the document have been made. Non-authorised staff could thus gain access to sensitive documents.

Lifecycle of digital documents, on the other hand, is traceable since the point of capture of a paper document until delivery into its destination and beyond. Particularly with automated document digitisation workflows, the creator of the digital document (i.e. the person digitising the document) can be determined at the time of capture directly by the capture device. Information about who created and modified a document can not only be recorded directly in the document metadata such as in the case of PDF documents,[21] but also as metadata in the document destination. ECM and DMS offer access controls, rules and workflows that can determine how and by whom a digitised document can be accessed and control the lifecycle of the document. These mechanisms can **prevent document leakage beyond the boundaries of the public institution and ensure authenticity of digital documents**. To further ensure digital documents have not been tampered with, mechanisms such as digital signatures available for PDF documents[22] can be applied. In our enrolment application example, the identity of the officer digitising the paper application and supporting documents can be determined by the scanner and then propagated all the way to the student records system. The system is capable of digitally signing the scanned document and ensure that only other authorised personnel can access, print and share the documents beyond the university boundaries.

[20] See available on-line: https://www.pdfa.org/publication/iso-19005-pdfa. 12.11.2017.
[21] See available on-line : https://www.iso.org/news/2012/03/Ref1525.htm 12.11.2017.
[22] See available on-line http://central-government.governmentcomputing.com/features/the-end-of-paper-the-leveraging-of-pdf-59584 28, 12.11.2017.

As the effects of document theft are amplified with digital documents and employee document theft is not uncommon in the workplace [23] digitisation introduces a number of challenges and risks to look out for.

The **risk of digitisation** is always connected computing devices on a university's premises. Since the trend of ubiquitous computing and Internet of Things[24] in education is on the rise[25] many devices on university campuses are connected to the university network or even directly to the Internet. Document capture devices such as multifunctional printers are no exception and just "*like any networked device, if not properly managed, they can expose sensitive campus data to unauthorized access and misuse."*[26].

4. Conclusion

Our hypothesis that the data exchange and storage is a very sensible matter that could lead up to the breaches of privacy and the duty of confidentiality has been fully verified.

The human participation forms the riskiest factor.

That is why the public authorities and university IT administrators must therefore not only secure the connection between the capture device and the network, but also choose digital document workflow software which supports **high level of security** including encryption of digital documents transferred from the capture device to their destination. Furthermore, IT administrators can **prevent employee document theft** by restricting the destinations where document capture devices can send scanned documents.

The **legal liability** of corporate governing bodies and public officers should ensure that the **privacy protection precautions** are adopted in any public and private entity. The rigorous rules of accessing and exchanging the protected data must be adopted as compliance programme required by GDPR for the reasonable data protection.

As the **main challenge for the next future** we identified the necessity of legal regulation of sensible date storage for universities, private companies and sole entrepreneurs.

---

[23] See available on-line :https://www.gvsu.edu/e-hr/how-to-avoid-employee-data-theft-62.htm. 12.11.2017.

[24] The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Definition available on-line: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT 12.11.2017.

[25] See available on-line : http://education.governmentcomputing.com/features/2017-the-year-uk-education-was-digitalised-568538. 12.11.2017.

[26] https://security.berkeley.edu/resources/best-practices-how-articles/network-printer-security-best-practices. Available on-line. 12.11.2017.

Despite of the fact, that the human factor is the riskiest factor in the digitisation and e-government it is always the human being who brings the necessary progress and new ideas.

Bibliography

1. Bell, David. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Special anniversary ed. New York, N.Y.: Basic Books 1999. 507 p.
2. Kleinig, J., Mameli, P., Mille, S., Salane, D., Schwart, A., *Security and Privacy*. *Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States*. p. 9. ANU E Press. The Australian National University Canberra. 2011.
3. Paschal, Samson Masalu Peter, *Public-Private Partnerships: No Investment without an Investor-State Dispute Settlement or Investment Court System*, in Ioana Nely Militaru, Adriana Moțatu, *Diversity and Interdisciplinarity in Business Law*, ADJURIS – International Academic Publisher, Bucharest, 2017.
4. Popescu, Alina, *The Right to Information and the Information Society*, in Ioana Nely Militaru, Adriana Moțatu, *Diversity and Interdisciplinarity in Business Law*, ADJURIS – International Academic Publisher, Bucharest, 2017.
5. Wilson, M. I, Kellerman, A., Corey, K. E. *Global Information Society: Technology, Knowledge, and Mobility*. Lanham: Rowman & Littlefield Publishers, Inc. 2013. 283 p.
6. Zoubek, Vladimír. *Postmoderní problémy globální společnosti*. In: Bezpečnost v podmínkách organizací a institucí ČR: sborník z mezinárodní konference.. Vyd. 1. Praha: Soukromá vysoká škola ekonomických studií 2005. 208 p.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available om-line: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. (consulted on 12.11.2017)
8. Czech Statistical Office, available on-line : https://www.czso.cz/csu/czso/home. (consulted on 12.11.2017).
9. Backround Paper: Implementing E-Government in OECD Countries. Experiences and Challenges. p. 2. Available on-line: http://www.oecd.org/mena/governance/ 36853121.pdf (consulted on 12.11.2017).