Compliance and Data Security in Document Management Systems

K. Kurteva
Department of Electronics, Faculty of Electronic Engineering and Technologies
Technical University of Sofia
8 Kliment Ohridski blvd., 1000 Sofia, Bulgaria
katerina.krasteva1@gmail.com

2023 XXXII International Scientific Conference Electronics (ET) | 979-8-3503-0200-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ET59121.2023.10279617

Abstract – **This paper discusses the critical aspects of compliance and data security in document management systems (DMS). The importance of adhering to regulatory requirements and implementing robust security measures to protect sensitive information is discussed. Compliance with regulatory standards and data encryption are highlighted. The importance of access control, user permissions, audit trails, activity logs, version control and document history in the context of document management are explained. The role of secure storage and backup, as well as data retention for robust DMS implementation are mentioned.**

Keywords – **audit, data security, DMS, compliance, GDPR**

I. Introduction

In today's digital era, organisations across various industries are increasingly relying on document management systems (DMS) to streamline their operations and enhance collaboration between the different units. The main motivation for such DMS expansion is the improved efficiency of the working process they provide. However, as the volume of digital documents continues to grow, the need of robust compliance and data security measures within these systems is very important. Ensuring the confidentiality, integrity and availability of sensitive information has become a top priority for organisations to protect against unauthorised access and legal repercussions. [1]

This approach discusses the critical aspects of compliance and data security in document management systems. Compliance refers to the adherence to regulatory standards, industry-specific guidelines as well as legal requirements governing the handling and storage of sensitive information. On the other hand, data security is often related to the measures implemented to safeguard data from unauthorised access and data loss. Both compliance and data security are interlinked and crucial for maintaining the trust of stakeholders and mitigating risks associated with information management. [11]

In recent years, the regulatory landscape has become more stringent, with data protection regulations such as the General Data Protection Regulation (GDPR) imposing significant responsibilities on organisations handling personal and sensitive data. Failure to comply with these regulations can lead to severe penalties. Reputation and legal consequences are also observed. Therefore, organisations must understand the regulatory requirements relevant to their industry and ensure their document management systems align with these standards.

Furthermore, data security is a fundamental aspect of document management systems. It encompasses various measures such as data encryption, access control, audit trails, secure storage and employee training. Protecting data from unauthorised access, accidental loss or intentional tampering is crucial to maintain confidentiality and prevent the misuse of sensitive information. Data breaches and security incidents can result in financial losses and the loss of customer trust.

Key topics related to compliance and data security in document management systems are discussed. By understanding and implementing these measures, organisations can ensure the integrity and security of their documents within DMS.

The subsequent sections will delve into each topic in more detail, providing insights, best practices and recommendations for organisations seeking to enhance their compliance and data security measures within their document management systems.

II. Discussion

A. Compliance with the General Data Protection Regulation (GDPR)

In the European Union (EU), the General Data Protection Regulation (GDPR) [12] has emerged as a comprehensive framework for data protection and privacy. It establishes strict guidelines for the collection, storage, processing and transfer of personal data of EU citizens. Compliance with the GDPR is of utmost importance for organisations operating within the EU or handling the personal data of EU residents.

The GDPR introduces several key principles that organisations must adhere to when managing personal data. These principles include lawfulness and transparency in data processing, purpose limitation, data minimization, accuracy, storage limitation and confidentiality. Organisations must ensure that personal data is collected and processed lawfully, with a legitimate purpose and minimal data collection, and stored securely while maintaining its accuracy [3, 8].

One of the fundamental aspects of GDPR compliance is obtaining explicit consent from individuals for data processing activities. This requires organisations to provide clear and easily understandable information about the purposes of data processing and the types of personal data collected. Document management systems play an important role in facilitating compliance with this requirement by enabling organisations to manage consent forms, track consent status and document consent-related activities.

979-8-3503-0200-4/23/$31.00 ©2023 IEEE

Data subject rights are another important aspect of the GDPR. Individuals have the right to access their personal data, rectify inaccuracies, request erasure (the "right to be forgotten"), restrict processing and receive their data in a portable format. Document management systems can assist organisations in handling these rights effectively by providing efficient mechanisms to do so. By leveraging the capabilities of document management systems, organisations can streamline the process of responding to data subject requests and ensure compliance with GDPR obligations.

The GDPR also emphasizes the importance of data security and imposes strict requirements for the protection of personal data. Organisations must implement appropriate technical and organisational measures to ensure the confidentiality, integrity and availability of personal data. Document management systems can contribute to GDPR compliance by offering robust security features such as access controls, encryption, secure storage and audit trails.

To demonstrate GDPR compliance, organisations must maintain comprehensive documentation of their data processing activities, policies, procedures and security measures. Document management systems can serve as a centralized repository for storing and managing this documentation and making it easily accessible for internal and external audits. Furthermore, the versioning and revision history capabilities of document management systems enable organisations to track and document changes made to privacy policies, consent forms and other relevant documents over time. [4, 6]

It is crucial for organisations to regularly review and update their data protection practices ensuring ongoing compliance with the GDPR. This includes periodic risk assessments, data protection impact assessments (DPIAs) for high-risk processing activities and maintaining a register of data processing activities.

B. Data Encryption

Data encryption is a “must has” for data security in DMS. Encryption involves converting data into a coded form that can only be accessed and deciphered with the appropriate decryption key. By encrypting sensitive information, organisations can protect the confidentiality and integrity of their data, ensuring that it remains secure even if it is intercepted or accessed by unauthorised individuals.

In document management systems, data encryption is typically applied at multiple levels to provide comprehensive protection. At the storage level, the data stored in the system's databases or file repositories is encrypted to prevent unauthorised access to the underlying files. This ensures that even if the physical storage media or the database itself is compromised, the encrypted data remains unreadable and unusable.

In transit encryption is another crucial aspect of securing data in document management systems. When documents are transmitted over networks, such as the internet or internal intranets, they are vulnerable to interception and unauthorised access. By employing encryption protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), organisations can establish secure communication channels, encrypting the data while it is in transit. This safeguards the documents from eavesdropping or tampering during transmission, maintaining the confidentiality and integrity of the information.

End-to-end encryption is an advanced encryption technique that ensures that data remains encrypted throughout its entire lifecycle, from creation to storage and transmission. This approach provides an additional layer of security, even if the document management system itself is compromised, the encrypted data remains protected.

Key management is a critical component of data encryption in DMS. Encryption keys are used to encrypt and decrypt the data, and their security is paramount. Organisations must establish robust key management practices, including secure key storage, key rotation and key access controls. Document management systems often include built-in key management features or integrate with external key management solutions to ensure the secure handling of encryption keys. [2, 5]

Data encryption also plays a vital role in compliance with various data protection regulations. For example, the GDPR mandates the implementation of appropriate technical and organisational measures to ensure the security of personal data. Encryption is specifically mentioned as one of the measures that can be implemented in DMS to protect personal data from unauthorised access and demonstrate organisation’s commitment to data security and compliance with regulatory requirements. [7]

While data encryption provides strong protection, it is essential for organisations to consider other aspects of security, such as access controls, user authentication and auditing, in conjunction with encryption.

C. Access Control and User Permissions

Access control and user permissions are fundamental components of document management systems that ensure proper authentication and authorisation of users accessing the system and its documents. By implementing robust access control mechanisms, organisations can enforce the principle of least privilege, granting users access only to the documents and functionalities necessary for their roles and responsibilities. This helps protect sensitive information, maintain data integrity and prevent unauthorised access or modifications.

DMS employ various access control techniques to manage user permissions effectively. These techniques include:

1. User Authentication: User authentication is the process of verifying the identity of users accessing the document management system. This typically involves the use of usernames and passwords but can also include additional authentication factors such as biometrics or multi-factor authentication. Strong authentication mechanisms help ensure that only authorised users can access the system, reducing the risk of unauthorised access.

2. Role-Based Access Control (RBAC): RBAC is a commonly used access control model that assigns permissions to users based on their roles within the organisation. Each role is associated with a predefined set of permissions that determine the actions a user can perform within the document management system. RBAC simplifies access control administration by grouping users into roles and granting permissions to those roles, rather than assigning

permissions to individual users. This approach streamlines the management of user permissions and reduces the risk of inconsistent access control.

3. Access Control Lists (ACLs): ACLs provide a more granular level of access control by specifying permissions for individual documents or document categories. With ACLs, administrators can define access rights, such as read, write, modify or delete for specific users or groups. This level of flexibility allows organisations to tailor access permissions based on the sensitivity of the documents and the needs of different user groups.

4. Hierarchical Permissions: Document management systems often support hierarchical permissions, where permissions can be inherited from parent folders or categories to child documents or subfolders. This simplifies permission management by allowing administrators to set permissions at higher levels, which automatically apply to the documents or folders within the hierarchy. Hierarchical permissions ensure consistency and ease of administration, especially in scenarios where multiple documents need to have the same access restrictions.

5. Audit Trails and Logging: An essential aspect of access control is the ability to track and monitor user activities within the document management system. Audit trails and logging mechanisms record user actions, such as document access, modifications or deletions, along with timestamps and user identifiers. These logs serve as valuable forensic evidence in case of security incidents and help organisations identify potential security breaches or policy violations.

It is important for organisations to regularly review and update user permissions in line with changes in personnel, job roles or security requirements. Regular audits should be conducted to ensure that user permissions align with the principle of least privilege and that any unauthorised access attempts or suspicious activities are promptly detected and addressed.

By implementing robust access control mechanisms and user permissions in DMS, organisations can establish a secure environment for document storage, collaboration and management. These measures ensure that only authorised users can access sensitive information, reducing the risk of data breaches and maintaining the confidentiality and integrity of documents.

D. Audit Trails and Activity Logs

Audit trails and activity logs play a critical role in DMS by providing a comprehensive record of user activities and system events. These logs capture detailed information about document access, modifications, deletions and other relevant actions, along with corresponding timestamps and user identifiers. By implementing robust audit trail mechanisms, organisations can enhance the security and the transparency of their document management processes.

Audit trails and activity logs play a crucial role in document management systems, serving various purposes to enhance security, compliance and system performance. [9]

One of the primary purposes of audit trails is security monitoring. They capture detailed information about user activities within the system, enabling the detection of security incidents, unauthorised access attempts and potential breaches. By monitoring these logs, organisations can promptly respond to mitigate risks and ensure the integrity and confidentiality of their documents.

Audit trails also contribute to establishing accountability within the system. They serve as a reliable source of information for investigating policy violations, data breaches or disputes. By analysing these logs, organisations can identify responsible individuals, track the sequence of events and determine the extent of the impact.

Additionally, activity logs and audit trails assist in monitoring system performance and troubleshooting. They provide valuable insights into user behavior, system events and performance metrics. By analysing these logs, administrators can detect patterns, anomalies or/and bottlenecks that may affect system performance, user experience or/and data integrity. Proactive monitoring based on activity logs helps ensure the smooth operation of the document management environment.

To maximize the effectiveness of audit trails and activity logs, organisations should follow best practices such as maintaining detailed logs, ensuring secure storage and protection, regularly monitoring and analysing logs and defining appropriate retention and archiving periods.

By leveraging audit trails and activity logs, organisations can enhance security, compliance and system performance in their document management systems.

To ensure the effectiveness of audit trails and activity logs, organisations should consider the following best practices:

1. Logging Granularity: DMS should capture a sufficient level of detail in audit logs to provide meaningful insights into user activities and system events. This includes recording information such as user actions, timestamps, IP addresses, document identifiers and any relevant data.

2. Secure Storage and Protection: Audit trails and activity logs contain sensitive information about user actions and system events. It is crucial to store and protect these logs in a secure manner, ensuring confidentiality and integrity. Encryption, access controls and regular backup procedures should be implemented to safeguard the logs from unauthorised access and tampering.

3. Regular Monitoring and Analysis: Organisations should establish processes for regular monitoring and analysis of audit trails and activity logs. Automated tools or log analysis systems can help identify patterns, anomalies or suspicious activities that may indicate security incidents or policy violations. Proactive monitoring allows organisations to detect and respond to potential threats in a timely manner, minimizing the impact on document security.

4. Retention and Archiving: Depending on regulatory requirements and business needs, organisations should define appropriate retention periods for audit trails and activity logs. These logs should be retained for a sufficient duration to support investigations or legal proceedings. Archiving mechanisms can be employed to ensure long-term storage and accessibility of historical log data.

E. Version Control and Document History

Version control and document history are essential features in DMS that enable organisations to effectively manage document revisions, track changes and maintain a clear record of document history.

Version control allows the systematic management of document versions and ensures that the most up-to-date and accurate version is accessible to users. It helps prevent confusion and errors that may arise from working with outdated or conflicting document versions. With version control, users can easily identify and access the latest iteration of a document, ensuring collaboration is streamlined and efficient.

Document history provides a comprehensive record of changes made to a document over time. It captures details such as who made the changes, when the changes occurred and the nature of the modifications.

The benefits of version control and document history extend beyond maintaining accurate records. These features enable organisations to revert to previous versions of a document if necessary, facilitating recovery and mitigating the risks associated with data loss or corruption. Furthermore, document history allows the identification of contributors and facilitates collaboration by providing visibility into individual contributions, facilitating teamwork and accountability.

Version control and document history also support compliance and regulatory requirements. Organisations operating in regulated industries often need to demonstrate the integrity and accuracy of their documents. By maintaining a complete version history, organisations can provide evidence of document changes and track compliance with regulatory standards.

Effective implementation of version control and document history requires the establishment of clear workflows and processes. This includes defining roles and responsibilities for document owners, implementing review and approval mechanisms and ensuring proper documentation of changes. User-friendly interfaces and intuitive features within the document management system are crucial to encourage user adoption and adherence to version control practices.

F. Secure Storage and Backup

Secure storage and backup are crucial components of a comprehensive document management system. They ensure the protection, availability and integrity of critical data. By implementing secure storage practices and robust backup mechanisms, organisations can safeguard sensitive information and mitigate the risk of data loss.

A reliable data backup strategy is essential for preserving data integrity and availability. Regular and scheduled backups create copies of data and store them in secure off-site locations. In the event of hardware failures, system crashes or accidental deletions, data can be restored from the backups. [9]

Implementing redundancy and replication techniques enhances data availability and durability. Redundancy involves storing data in multiple locations or on multiple storage devices. If one storage medium fails, data remains accessible from alternative sources. Replication creates exact copies of data and distributes them across different storage systems, ensuring data integrity and accessibility even in the face of hardware failures. [13]

Strict access controls play key role in secure storage. User authentication and authorisation ensure that only authorised individuals have the necessary permissions to access and modify stored data. This prevents unauthorised access and modifications and data breaches, safeguarding the confidentiality and integrity of sensitive information.

G. Data Retention and Disposal

Proper data retention and disposal practices are essential for maintaining data integrity, ensuring compliance with regulatory requirements and minimizing the risk of unauthorised access or data breaches. Implementing effective data retention and disposal strategies within a DMS allows organisations to manage data lifecycle and adhere to legal and industry-specific obligations.

Data retention policies outline the specific guidelines and timeframes for retaining different types of data. These policies are typically influenced by legal requirements. By defining clear retention periods, organisations can ensure that data is kept for the appropriate duration and disposed of in a timely manner, reducing the risk of unnecessary data storage and potential legal liabilities.

Adhering to regulatory requirements is important for organisations across various industries. Different regulations, such as the GDPR in the European Union, prescribe specific rules for data retention and disposal. Compliance entails understanding the applicable regulations, implementing policies that align with the requirements and ensuring that data is retained and disposed of accordingly to maintain compliance and avoid penalties.

Proper data disposal is crucial to prevent unauthorised access or retrieval of sensitive information. When data reaches the end of its retention period or is no longer needed, secure disposal methods must be applied. This includes techniques such as data wiping or physical destruction of storage media. By securely disposing of data, organisations can minimise the risk of data breaches and protect the confidentiality of sensitive information.

Maintaining proper documentation and conducting regular audits are essential components of data retention and disposal practices. Auditing these processes ensures that data retention and disposal practices are followed consistently and effectively, identifying any gaps or areas for improvement.

H. Employee Training and Awareness

It is essential for organisations to invest in comprehensive training programs and foster a culture of cybersecurity awareness among employees. By equipping employees with the necessary knowledge and skills, organisations can reduce the risk of human errors and enhance data security.

Cybersecurity training should cover various aspects related to DMS usage, data security and best practices. This includes educating employees about potential threats, such as phishing attacks, social engineering and malware, and providing guidance on how to identify and respond to such threats effectively. Training should also cover topics like password security, secure file sharing and the importance of regular software updates to ensure the ongoing protection of sensitive data.

Employees should be trained on proper data handling procedures within the DMS. This includes understanding data classification, access control and secure sharing

practices. Employees should be aware of their roles and responsibilities in maintaining data confidentiality and integrity.

Employees should be educated on the importance of promptly reporting any security incidents or potential vulnerabilities they encounter within the document management system. This encourages a proactive approach to addressing security concerns and enables the organisation to respond swiftly to mitigate risks. Training should outline the reporting mechanisms, emphasizing the need for timely and accurate reporting to the appropriate IT or security personnel.

II. Conclusion

The implementation of comprehensive compliance and data security measures in document management systems plays a strong role in protecting sensitive information, meeting regulatory requirements and mitigating potential risks for organisations. Throughout this paper, we have examined several crucial aspects of compliance and data security, including document classification and access controls, regulatory compliance, data encryption, access control and user permissions, audit trails and activity logs, version control and document history, secure storage and backup, data retention and disposal and employee training and awareness.

By adopting a proactive approach to compliance and data security, organisations can establish a robust framework that ensures the confidentiality, integrity and availability of their documents. Document classification and access controls enable organisations to categorize and restrict access to sensitive information, ensuring that only authorised individuals can retrieve and modify it. Regulatory compliance, such as adhering to the European Union's GDPR, demonstrates a commitment in protecting personal data and privacy rights.

In conclusion, implementing robust security measures such as data encryption, access control, audit trails and document history features enhances the protection and integrity of sensitive information in document management systems. Additionally, secure storage, backup mechanisms, data retention policies, employee training and regular audits contribute to a culture of compliance and data security. By adopting a comprehensive approach and staying vigilant in monitoring and adapting to emerging threats and regulatory landscapes, organisations can safeguard data and ensure the long-term sustainability of their operations.

Acknowledgment

ECoVEM project, 620101-EPP-1-2020-1-BG-EPPKA3-VET-COVE (2020 – 2024), European Centre of Vocational Excellence in Microelectronics. The project is co-funded by the European commission, program Erasmus+ KA2 Skill Alliances. "The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsi-ble for any use which may be made of the information contained therein".

References

[1] I. Syamsuddin, A. Yunianta, "Design and usability assessment of DocManS: A document management system with security and social media features", International Journal of Advanced and Applied Sciences, 9(1) 2022, pp 48-54

[2] K. Romanenko, E. Ischukova, "Overview of security issues in electronic document management systems", Journal of Informatization and communication, Vol. 2, 2023, DOI: 10.34219/2078-8320-2023-14-2-76-79

[3] M. Mustafa, S. Ahmad, "Development Model for the Implementation of Information Leakage Protection Program in Public Sector Agencies", Journal of Pharmaceutical Negative Results 14(2) 2023 pp 1073-1077

[4] L. Piras, M. Al-Obeidallach, M. Pavlidis, H. Mouratidis, A. Tsohou, E. Magkos, A. Praitano "A Data Scope Management Service to Support Privacy by Design and GDPR Compliance", Journal of Data Intelligence, Vol. 2, No. 2 (2021) pp. 136-165

[5] R. Congiu, L. Sabatino, G. Sapi, The "Impact of Privacy Regulation on Web Traffic: Evidence From the GDPR", Information Economics and Policy, Vol. 61 (2022), DOI: 10.1016/j.infoecopol.2022.101003

[6] S. Cortina, P. Valoggia, B. Barafort, A. Renault, "Designing a Data Protection Process Assessment Model Based on the GDPR", Communications in Computer and Information Science, Vol. 1060 (2019), DOI:10.1007/978-3-030-28005-5_11

[7] F. Konobevcev, "Digitalization of Personnel Document Management", Management of the Personnel and Intellectual Resources in Russia Vol. 11(6) , 2022

[8] Kock A., Schulz B., Kopmann J. and Gemünden H., "Project portfolio management information systems' positive influence on performance –the importance of process maturity", International Journal of Project Management 38 (2020) 229–241

[9] Yinghui Xu, Xi Chen, Chuang Li, Lianzhu Ge1, Haiyan Zhao and Tianying Jiang, "Enterprise data security compliance strategy: A study based on typical cases", 2022 International Conference on Educational Science and Social Culture (ESSC 2022), Volume 157, 03015, DOI: 10.1051/shsconf/20231570 3015

[10] D. Chikurtev, S. Bogdanov, N. Spasova, V. Ivanov, "Prerequisites for a self-sustaining embedded system with artificial intelligence", Proc. of 29th International Scientific Conference Electronics, 2020.

[11] Brocke J. and Lippe S., "Managing collaborative research projects: A synthesis of project management literature and directives for future research", International Journal of Project Management, Vol. 33 (5) (2015), pp. 1022-1039, DOI: 10.1016/j.ijproman.2015.02.001

[12] 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) (2016)

[13] European Data Protection Supervisor (EDPS) Opinion No. 3/2018 on online manipulation and personal data (2018)