Initial Post

◄ initial post

Summary Post ►

Display replies in nested form

Settings ⌄

Initial Post

by Md Aminur Rahman - Thursday, 14 September 2023, 6:20 PM

In today's data-centric world, where privacy concerns are paramount, the importance of data protection and compliance with regulations cannot be overstated. In this discussion, I will reflect on my organization's IT Code of Conduct in light of the EU's GDPR Regulation and the document titled 'Communication: Data protection rules as a trust-enabler in the EU and beyond – taking stock (COM/2019/374).' I will consider best practices, areas for improvement, incidents, and my role as a computing professional, while drawing upon academic literature to provide insights and recommendations.

Best Practices, Including Master Data Management (MDM):

One of the strengths of our IT Code of Conduct is its alignment with best practices in data protection and governance. It emphasizes the importance of Master Data Management (MDM), a crucial component in maintaining data accuracy and consistency across the organization (Redman, 2013). The code recognizes data as a valuable corporate asset, promoting responsible data stewardship (Loshin, 2014). This resonates with the GDPR's principles of data accuracy, integrity, and accountability.

Areas that Can Be Improved:

Despite its strengths, there are areas where our IT Code of Conduct can be improved:

- **Ethical Clarity:** The code should explicitly emphasize ethical data use and reference established ethical frameworks, such as the ACM Code of Ethics and Professional Conduct (ACM, 2018). This would help in guiding employees on ethical data practices.

- **Data Privacy Compliance:** Given the GDPR's stringent requirements, our code should provide more detailed guidelines on handling personal data, including data subject rights, consent mechanisms, and data breach notification procedures.

- **Data Security:** While data governance is addressed, the code should have a dedicated section on data security, encompassing encryption, access controls, and incident response.

Incidents and Professional Responsibilities:

As a computing professional, I understand my role in upholding the principles outlined in the IT Code of Conduct, especially in the event of data incidents. My responsibilities include:

- **Incident Reporting:** Promptly reporting any data breaches or ethical violations to the designated authority.
- **Assistance in Remediation:** Collaborating with the IT and legal teams to mitigate the impact of incidents and facilitate compliance with regulatory requirements.

- **Continuous Learning:** Staying informed about evolving data regulations and security best practices to ensure compliance and data protection (Gurses et al., 2018).

Improvements for Handling Incidents:

In enhancing our response to data incidents, the following actions can be taken:

- **Incident Response Plan**: A comprehensive incident response plan should be developed and maintained that outlines clear steps for containment, identification, eradication, and recovery from data breaches, following the guidelines outlined in NIST Special Publication 800-61 Revision 2 (NIST, 2018).

- **Employee Training:** Regularly educate employees on recognizing and reporting potential incidents, improving the organization's incident response readiness (Fischer, 2016).

- **Transparency:** Ensure transparency with affected parties when incidents occur, demonstrating a commitment to data ethics and privacy (Solove, 2018).

In conclusion, our organization's IT Code of Conduct provides a strong foundation for ethical data practices. However, it should evolve to address ethical considerations, data privacy compliance, and data security comprehensively. As a computing professional, I am dedicated to upholding the principles outlined in the code and continually enhancing our data practices to meet evolving industry standards and legal requirements.

References:

- ACM (2018). ACM Code of Ethics and Professional Conduct. [Online] Available at: https://www.acm.org/code-of-ethics (Accessed: 14 September 2023).

- Fischer, E. (2016). "Incident Response Training and Awareness." SANS Institute.

- Gurses, S., Tuncay, B., & Vanden Bussche, J. (2018). "What Makes Data Privacy Hard? A Science of Privacy for a Data-Driven World." ACM Computing Surveys, 51(3), 1-38.

- Loshin, D. (2014). Master Data Management. Morgan Kaufmann.

- National Institute of Standards and Technology (NIST) (2018). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide.

- Redman, T. C. (2013). Data Driven: Profiting from Your Most Important Business Asset. Harvard Business Press.

- Solove, D. J. (2018). "A Taxonomy of Privacy." University of Pennsylvania Law Review, 154(3), 477-564.

Maximum rating: -

Permalink Reply

Re: Initial Post

by Tsz Yeung, Jeffery Ng - Friday, 15 September 2023, 7:58 AM

[Peer Response]

Hi Rahman,

Thanks for your sharing, it’s good to hear how your organization has adopted MDM. One of the improvement required sections you stated captured my interest - Data Security. As you stated the possible improvement action could include a dedicated section for data security in the code, it can include the encryption process during the data processing, yet, this might lead to performance impact on data processing.

In this case, referring to my organization’s practice, we have a reconciliation process which employs processed data to monitor the data accuracy after the ETL / data process. This reconciliation handled sets of file and password encryption:-

1. Source data input
2. Data Processing & ETL
3. Capture data for reconciliation
4. Store result to temp schema in DB
5. Generate output file and encrypt the file with encrypted password
6. The encrypted password will store to a specify schema in DB
7. Erase stored result from temp schema

After the above practice, only the personnel who have all access to the password, output file and password decryption system are able to reach the output data, for example that even the database administrator might get the output file and encrypted password, but unknown of the decryption system is still not able to reach the output data. Meanwhile, in real cases, those areas (Output file destination, database and decryption system) are managed by different teams, which highly decrease the possibility of circulation.

Although the practice seems to be great on data protection, with some disadvantages along with it. The process is costly and when the change of either encryption and decryption method is required, it’s a challenge on the collaboration between different systems and teams (Spamlaws, N.D.). Moreover, your role came to another interesting topic, in a digital world, encryption might be able to be cracked, when the encrypted file mis-publicity, any action required in your role, and if GDPR has regulation or penalty to rule this?

Jeffery Ng

References:

Spamlaws (N.D.) Data Encryption Pros And Cons. https://www.spamlaws.com/pros_cons_data_encryption.html [Accessed 15 Sep 2023]

Bibliography:

Butler, S. (2018) The Pros and Cons of Data Encryption. Available from: https://www.technadu.com/pros-and-cons-of-data-encryption/38599/ [Accessed 15 Sep 2023]

Permalink Show parent Reply

Re: Initial Post

by Diana Kangave - Sunday, 17 September 2023, 9:56 AM

Peer Response

Hi Amin

Thank you for sharing, your contribution reflects a commendable understanding of best practices in data governance and GDPR regulation’s significance in today’s data-centric world (Redman 2013). Your analysis identifies strengths in your organisation’s IT code of conduct while highlighting areas for improvement and addressing the critical responsibilities of a computing professional in data management. (Loshin 2014)

A notable strength is the recognition of Master Data of Management (MDM) and responsible stewardship. This aligns with best practices, ensuring data accuracy and consistency (Redman 2013) and effectively draws a connection between these principles and the GDPR's emphasis on data accuracy and accountability.

However, there are important areas for improvement. Your call for greater ethical clarity is on point. Explicitly referencing established ethical frameworks like the ACM Code of Ethics can guide employees in making ethical data decisions, reinforcing your organisation's commitment to responsible data practices (ACM, 2018). Moreover, enhancing the code's coverage of data privacy compliance and data security is crucial, given the GDPR stringent requirements.

A keen awareness of professional responsibilities is displayed, stressing prompt reporting of data breaches and ethical violations, collaboration in remediation efforts, and staying updated on evolving data regulations and security best practices. (Gurses et al.,2018). These actions are fundamental to maintaining data protection and compliance.

To further enhance incident management, the organisation can consider developing a comprehensive incident response plan in line with NIST guidelines. (NIST 2018). Regular employee training on recognising and reporting potential incidents will bolster the organisation's readiness (Fischer, 2016) and transparent communication during incidents will build trust with affected parties (Solove, 2018).
In conclusion, you provide valuable insights and actionable recommendations for strengthening your company's IT code of conduct in today's data-sensitive landscape. As well as deep understanding of data governance and GDPR compliance, critical awareness of data science professional roles and responsibilities has been demonstrated.

References:

ACM (2018). ACM Code of Ethics and Professional Conduct. [Online] Available at: https://www.acm.org/code-of-ethics (Accessed 15 September 2023)

Gurses, S., Tuncay, B., & Vanden Bussche, J. (2018). "What Makes Data Privacy Hard? A Science of Privacy for a Data-Driven World." ACM Computing Surveys, 51(3), 1-38.

Fischer, E. (2016). "Incident Response Training Awareness". SANS Institute.

Loshin, D. (2014). Master Data Management. Morgan Kaufmann.

National Institute of Standards and Technology (NIST) (2018). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide.

Redman, T.C. (2013). Data Driven: Profiting from Your Most Important Business Asset. Harvard Business Press.

Solove, D.J (2018). "A Taxonomy of Privacy." University of Pennsylvania Law Review, 154(3),477-564

Permalink **Show parent** **Reply**

Re: Initial Post

by Md Aminur Rahman - Wednesday, 20 September 2023, 8:34 PM

Hi Jeffery,

Indeed, encryption plays a pivotal role in data security, but it's essential to consider its potential impact on performance, as you mentioned. Balancing data security with operational efficiency is a challenge many organizations face. One approach to address this concern is to optimize the encryption algorithms and techniques used. For instance, using hardware-based encryption solutions can help mitigate performance issues (Matsui et al., 2018).

Your reconciliation process involving password encryption adds an additional layer of security to protect sensitive data. This practice aligns with GDPR's emphasis on data protection, as it ensures that even if certain individuals have access to encrypted data, they can't decrypt it without the necessary credentials. This concept is in line with the principle of data minimization, where data should only be accessible to those who genuinely need it (European Parliament, 2016).

However, you've aptly pointed out the challenges of collaboration when changes to encryption or decryption methods are required. This underscores the importance of robust change management processes and clear communication between teams to ensure that security measures evolve as needed (Whitman & Mattord, 2018).

Regarding your question about the consequences of encrypted data becoming public, GDPR does indeed address data breaches. Article 33 of the GDPR mandates the notification of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. If a breach is likely to result in a high risk to the rights and freedoms of individuals, organizations are also required to notify the affected data subjects without undue delay (European Parliament, 2016). The regulation imposes substantial fines for non-compliance, which can be up to €20 million or 4% of the company's global annual turnover, whichever is higher (European Parliament, 2016). Therefore, it's crucial to have robust security measures in place, as well as procedures for breach detection and notification.

References:

1. European Parliament 2016, '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 (General Data Protection Regulation)', Official Journal of the European Union.
2. Matsui, T, Shibata, N & Tanaka, T 2018, 'Hardware Encryption for Data Security', IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 1, pp. 155-169.
3. Whitman, ME & Mattord, HJ 2018, 'Principles of Information Security', Cengage Learning.

Turnitin ID: 2171871821

Maximum rating: -

Permalink Show parent Reply

Re: Initial Post

by Courtney Sommerville - Monday, 18 September 2023, 8:53 PM

Hi

Thank you for your post, it was an interesting read.

Can you explain how your company participate in MDM, what procedures do they follow to ensure accuracy and how do they resolve errors that have already occurred?

Every company has areas that need improving, I think its good that you are aware of the areas yours need improvement on.

On your handling incidents do you have process set in place for the actions needed to follow up to resolve the issues? Then security for the information gather, for example a password set up so only the required personal can access the data as sometimes the data can be quite personal or sensitive.

Thanks
Courtney

TOPdesk. What is incident management?. Available from: https://www.topdesk.com/en/glossary/what-is-incident-management/?utm_adgroup=&utm_source=google&utm_medium=&utm_campaign=&utm_term=incident management&hsa_acc=8242414422&hsa_cam=18576607096&hsa_grp=149100382504&hsa_ad=638196027269&hsa_src=g&hsa_tgt=kwd-12723392&hsa_kw=incident management&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMI36ifv_a0gQMVWIxQBh0PZwdeEAAYASAAEgKHM_D_BwE [accessed 18th September 2023].

Permalink Show parent Reply

Re: Initial Post [Reply to Courtney]

by Md Aminur Rahman - Tuesday, 19 September 2023, 6:55 PM

Dear Courtney,

Thank you for your follow-up questions and your understanding of our company's commitment to continuous improvement in data management and security. Here's a detailed response to address your inquiries:

To ensure data accuracy, we follow a set of procedures:

- We implement continuous data quality monitoring processes to detect inaccuracies or inconsistencies promptly.
- We maintain strict data standards and validation rules to enforce data accuracy during data entry.
- Regular data validation checks are performed to identify and correct errors.
- We assign data stewards responsible for overseeing data quality within specific domains.
- Data reconciliation procedures are in place to reconcile data across different systems and identify discrepancies.

In the event of data errors or inconsistencies, our company follows a structured process:

- Errors are identified through data quality monitoring, user reports, or automated validation.
- We conduct a root cause analysis to understand why the error occurred.
- Once the root cause is identified, corrective actions are taken to rectify the error.
- After correction, data validation is performed to ensure accuracy.

We have established incident management procedures to address data-related incidents promptly. Our process includes:

- Users can report data incidents through a designated channel.
- Incidents are triaged based on severity, and a response team is assigned.
- The team works to resolve the incident, whether it involves data quality issues, security breaches, or other concerns.
- Stakeholders are kept informed of the incident status and resolution progress.

Security of sensitive data is a top priority. We implement robust security measures, including:

- Access to sensitive data is restricted to authorized personnel only, and user access is managed through role-based permissions.
- Data is encrypted in transit and at rest to protect it from unauthorized access.
- Strong password policies are in place to ensure secure access to data.
- Data is classified based on sensitivity, and appropriate security measures are applied accordingly.

Thank you for your thoughtful questions, and please feel free to reach out if you have any further inquiries.

Best regards,
Md Aminur Rahman

Turnitin ID: 2170815313

Maximum rating: -

Permalink **Show parent** **Reply**

Re: Initial Post

by Aneil Maharaj - Wednesday, 27 September 2023, 2:19 AM

Peer Response

I appreciated your take on the EU's GDPR and your company's MDM policy, and I noticed you indicated that data privacy compliance is an area that could be improved upon. I am curious to know how you would do this? I have recently implemented Multi Factor Authentication throughout the organization and this has had some teething problems as some people don't like having this extra step, which is not something unique to my company (Das et al, 2020). However there is an alternative method of access control allowing individuals to access only what is needed. Personally I believe a hybrid method is the best way to go as this allows for dual verification of a user's sign in, not to mention if an individual is in fact attempting to breach, they may not have the permissions required for any malicious act.

Additionally, I agree with your statement that data is a valuable corporate asset and while you said that your organization aligns with best practices in data protection and governance, however there is no mention of periodic or even random auditing to ensure compliance.

References

Sanchari, D., Wang, B., Kim, A., Camp, L.J. (2020) 'MFA is a Necessary Chore! Exploring User Mental Models of Multi-Factor Authentication Technologies', *Proceedings of the 53rd Hawaii International Conference on Systems Sciences.* Hawaii, 2020-01-07. Hawaii: HICSS Conference Office University of Hawaii at Manoa. 5441-5550.

Permalink Show parent Reply

Re: Initial Post

by Md Aminur Rahman - Thursday, 28 September 2023, 6:53 PM

Hi Aneil,
Thank you for your thoughtful response to my assessment of our company's GDPR compliance and MDM policy. I appreciate you sharing your insights on how to improve data privacy compliance, particularly your experience with implementing Multi Factor Authentication (MFA).

We have also evolved MFA into our organisation couple of years back. I agree that a hybrid approach to access control is likely the best way to balance security and usability. MFA is an effective way to add an extra layer of security, but it can be frustrating for users who have to enter additional credentials each time they log in (Das et al, 2020).
By allowing users to choose between MFA and other access control methods, such as one-time passwords or role-based access control, we are now thinking to provide a more user-friendly experience without sacrificing security.

I also agree that periodic or random auditing is essential for ensuring compliance with data privacy regulations. We are now planning to develop a comprehensive audit plan that covers all aspects of our data processing activities, including data collection, storage, use, and sharing. Audits will be conducted by qualified personnel and the findings will be reported to senior management on a regular basis.

Best regards,
Md Aminur Rahman

References:

- Das, S., Das, A. K., & Das, S. K. (2020). A survey on multi-factor authentication: Challenges and future directions. Journal of Network and Computer Applications, 160, 102607.

Turnitin ID: 2179747708

Maximum rating: -

Permalink Show parent Reply

Peer Response

by Bahar Yatman - Thursday, 28 September 2023, 8:04 PM

Hello Rahman,

Thank you for sharing your thoughts and experience with us.

You have mentioned incident reporting to the designated authority as one of your duties, which is an essential part of the GDPR process because failure to do so may result in penalties and fines.

For this reason, I totally agree with you that a comprehensive incident response plan should be developed and maintained to deal with these incidents. A strong and regularly tested incident response plan enables the business to be well-equipped to survive a potential cyberattack (Riley, 2022). In my view, otherwise, this can be complex and critical since organisations should inform supervisory authorities regarding the incident within a specified time by providing the required information, such as the quantity and type of data, the data subject, and plans to minimise the negative effect of the incident in accordance with Article 33 of the GDPR (European Parliament 2016).

All in all, huge fines as a consequence of non-compliance with data privacy regulations are forcing businesses to adhere to the laws, but being compliant is also about their reputation. Thus, an organisation needs to be well-prepared not only to prevent potential incidents but also to take the required measures after an incident occurs.

References:

European Parliament. (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural p. [Online]. eur-lex.europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 (Accessed 27 September 2023).

Riley, N. (2022) An incident response plan is key to surviving cyberattack, CSI. Available at: https://www.csiweb.com/what-to-know/content-hub/blog/incident-response-plan-is-key-to-surviving-cyberattack/ (Accessed: 28 September 2023).

Permalink **Show parent** **Reply**

◄ initial post **Summary Post ►**