DATA PRIVACY ADVANTAGE

MAKE DATA PRIVACY A BUSINESS ADVANTAGE

OUR PRIVACY ESSAY SERIES

Welcome to "The Data Privacy Advantage Newsletter", which will be a monthly resource hub of practical information, advice, and content that will help organizations make Data Privacy a business advantage.

FIVE ORGANIZATIONAL DATA PRIVACY RISKS CAUSED BY DIGITAL ILLITERACY

THE DATA DIVA

Debbie Reynolds, "The Data Diva," is a world-renowned technologist, thought-leader, and advisor to multinational corporations for handling global Data Privacy.

DEBBIE REYNOLDS GLOBAL DATA PRIVACY EXPERT

WWW.DEBBIEREYNOLDSCONSULTING.COM

FIVE ORGANIZATIONAL DATA PRIVACY RISKS CAUSED BY DIGITAL ILLITERACY

Our Privacy Essay Series

In today's digital age, the sheer volume of data generated, processed, and circulated daily is overwhelming. While technology equips organizations with invaluable resources and unparalleled new opportunities, it may also usher in hidden Data Privacy risks. A significant hurdle that these organizations grapple with is Digital Illiteracy.

In the context of Data Privacy, Digital Illiteracy refers to the lack of understanding and skills needed to navigate the digital world securely and responsibly. Digital Illiteracy includes the inability to fully understand how personal and organizational data is collected, stored, used, and shared online and how to safeguard that data from misuse. Digital Illiteracy is not just about a lack of understanding of how to use technology but also about the implications of data uses that impact individuals and organizational privacy.

Considering the rapid pace of digital transformation and the evolving uses of technology, organizations must ensure that individuals within their organizations are digitally competent. We will explore the five key areas where Digital Illiteracy poses the greatest Data Privacy risks to organizations and provide effective strategies for mitigating these risks.

Digital Illiteracy Risk #1: Lack of Awareness of Application Data Usage

Many organizations use a variety of applications to increase productivity, improve customer service, and optimize operations. However, each application uses data differently, which may be challenging to understand, especially for individuals with low digital literacy. A lack of awareness of how these applications use, store, and share data could expose sensitive organizational information to third parties, even passively. This could result in severe privacy breaches and associated financial and reputational damage. Therefore, educating employees about application data usage and the potential implications for Data Privacy is crucial. Once individuals know how data is used in digital systems, they can become more aware of the danger signs and ask the right questions.

Organizations can address the "Lack of Awareness of Application Data Usage" risk by:

- Conducting assessments of application usage and their alignment with Data Privacy best practices

- Implementing measures to limit the access of applications to sensitive data

- Implement organizational measures for applications that cannot be made more compliant with technology

Digital Illiteracy Risk #2: Misunderstanding Data Classification

Data classification involves categorizing data based on its sensitivity, value, and criticality to the organization. This process is vital to determine appropriate data handling and security measures. Digital illiteracy can lead to misunderstanding or ignorance of the importance of data classification, resulting in inadequate protection of sensitive data.

When individuals do not understand the differences between public, confidential, privileged, personal, and highly sensitive data, they may inadvertently expose crucial information. This could involve sharing confidential files publicly or failing to adequately secure sensitive data within the enterprise that may result in unauthorized access or a data breach. Therefore, raising digital literacy levels to ensure a solid understanding of data classification is crucial in managing Data Privacy risks within any organization.

To mitigate the "Misunderstanding Data Classification" risk, organizations can:

- Establish clear data classification guidelines and share them with all employees

- Train employees on the importance of data classification and it's role in ensuring Data Privacy

- Regularly review and update data classification policies to address evolving risks

Digital Illiteracy Risk #3: Sharing Sensitive Information Without Caution

In the digital age, sensitive data can be shared swiftly and effortlessly, often without a second thought to the potentially dire consequences of a misstep. However, sharing sensitive information without proper caution can lead to serious Data Privacy breaches.

Digital Illiteracy can result in employees sharing sensitive organizational or personal data via insecure channels or sharing data with people not authorized to see sensitive data. As a result, organizations must ensure that their employees fully understand the risks associated with sharing sensitive information and how to do so safely.

Organizations can address the "Sharing Sensitive Information Without Caution" risk by:

- Limit access to sensitive data within organizations to only those who "need to know" the information

- Training employees on secure data-sharing practices for sensitive data

- Establishing clear policies and consequences for negligent sharing of sensitive data

Digital Illiteracy Risk #4: Insufficient Data Disposal Practices

Proper data disposal impacts Data Privacy risks. No longer needed data should be disposed of securely to prevent unauthorized access or misuse. It is also key for organizations to understand that holding Personally Identifiable Information (PII) indefinitely is no longer acceptable without a purpose. In this context, Digital Illiteracy may result in insufficient organizational triggers for when data disposal may be warranted.

Also, employees might delete files or emails containing sensitive information without understanding that the data may still be retrieved from the device or server. Alternatively, employees may discard old hardware without properly wiping the data, leaving sensitive information accessible. Training in secure data disposal techniques is necessary to mitigate this risk.

Organizations can mitigate the "Insufficient Data Disposal Practices" risk by:

- Implementing trigger events, policies, and procedures for when data has reached the "end of life" and needs disposal

- Implement and regularly assess data disposal practices to ensure compliance

- Promoting awareness of the potential consequences of improper data disposal

Digital Illiteracy Risk #5: Limited Knowledge of Data Privacy Regulations

Data Privacy regulations impose strict requirements on how organizations handle personal data, and non-compliance can result in severe penalties.
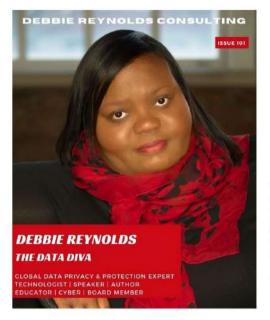
However, Digital Illiteracy can lead to a limited understanding of these regulations, resulting in non-compliance. Employees might not understand the requirements for data consent, data subject rights, or breach notification, leading to violations. Organizations must invest in education about Data Privacy regulations tailored to improve Digital Literacy.

Organizations can address the "Limited Knowledge of Data Privacy Regulations" risk by:

- Providing regular training on relevant Data Privacy regulations and updates

- Creating a clear, easy-to-understand summary of Data Privacy laws for employees

- Explain how new technologies (like implementing AI or Biometrics) may add more Data Privacy risks to organizations

Digital Illiteracy poses significant Data Privacy risks to organizations when it is not properly addressed. Addressing these risks requires a comprehensive approach that includes raising awareness of application data usage, improving understanding of data classification, educating on the safe sharing of sensitive information, training in secure data disposal practices, and improving knowledge of Data Privacy regulations. By investing in Digital Literacy, organizations can make Data Privacy a Business Advantage.

CONTACT US

DEBBIE REYNOLDS CONSULTING, LLC
HTTPS://WWW.DEBBIEREYNOLDSCONSULTING.COM
DATADIVA@DEBBIEREYNOLDSCONSULTING.COM
+1-(312) 513-3665

HTTPS://WWW.LINKEDIN.COM/IN/DEBBIEAREYNOLDS/
HTTPS://WWW.YOUTUBE.COM/CHANNEL/UCVZ2NIE9BW43AH1QZVJH2UQ/VIDEOS
HTTPS://THEDATADIVATALKSPRIVACYPODCAST.BUZZSPROUT.COM/

Debbie Reynolds, "The Data Diva" has made a name for herself as a leading voice in the world of Data Privacy and Emerging Technology with a focus on industries such as AdTech, FinTech, EdTech, Biometrics, Internet of Things (IoT), Artificial Intelligence (AI), Smart Manufacturing, Smart Cities, Privacy Tech, Smartphones, and Mobile App development. With over 20 years of experience in Emerging Technologies, Debbie has established herself as a trusted advisor and thought leader, helping organizations navigate the complex landscape of Data Privacy and Data Protection. As the CEO and Chief Data Privacy Officer of Debbie Reynolds Consulting LLC, Debbie brings a unique combination of technical expertise, business acumen, and business savvy to her work.