Mandatory Data Breach Notification Policy Analysis 3

Janae Craig

Old Dominion University

Malik Gladden

CYSE 425

October 15, 2023

Mandatory Data Breach Notification Policy

Cyber security is a basic concern in our increasingly digital world, and organizations have carried out different systems to defend sensitive data. One such procedure is the Mandatory Data Breach Notification Policy, which expects organizations to illuminate individuals when their data is compromised. While this policy is pivotal for improving transparency and safeguarding individuals' rights, it raises ethical issues regarding costs, benefits, and potential limitations. This essay investigates the ethical implications of the Mandatory Data Breach Notification policy, focusing on its effect on individual rights and whether it adequately addresses ethical concerns.

The Mandatory Data Breach Notification policy carries both ethical costs and benefits. On the positive side, it improves transparency and accountability (Duggineni, 2023). Commanding organizations to report data breaches expeditiously enables individuals to make vital moves to safeguard themselves from potential harm, like fraud, which aligns with ethical principles of transparency and autonomy, as individuals reserve the option to know when their data is at risk (Duggineni, 2023). In any case, there are ethical costs related to this policy, too. One concern is the potential for false alarms or overly broad notifications, which could prompt superfluous panic among individuals. Ethical considerations expect notifications to be exact and not inflict damage, like unjustifiable stress or fear (Duggineni, 2023). Finding some harmony between giving timely information and staying away from pointless panic is a difficult ethical dilemma.

The Mandatory Data Breach Notification policy plans to safeguard individuals' rights, principally the right to privacy and education. It guarantees that individuals are educated when their data is uncovered, permitting them to make fitting moves to relieve potential harm (Ahmed,

et al., 2020). This aligns with the ethical principle regarding individuals' autonomy and right to control their personal information. Notwithstanding, the policy additionally forces limitations on organizations (Ahmed, et al., 2020). They are burdened with distinguishing, reporting, and overseeing data breaches, which can be costly and time-consuming. It raises ethical issues about whether the policy burdens organizations unjustly, potentially discouraging innovation and investment in cyber security measures (Ahmed, et al., 2020). Another ethical test is finding harmony between safeguarding individual rights and not overly burdening organizations.

The Mandatory Data Breach Notification policy is a huge step toward advancing individuals' rights in the digital age. It acknowledges that individuals reserve a privilege to know when their data is compromised and gives a mechanism to implement that right (Allen, et al., 2021). In any case, questions emerge about whether the policy adequately safeguards individuals' rights. One ethical concern is the variation in data breach notification laws across jurisdictions. Inconsistencies can prompt unequal protection of individuals' rights depending upon their location (Allen, et al., 2021). Ethical considerations require a more harmonized way to guarantee consistent protection of individuals' rights regardless of geographical location.

In conclusion, the Mandatory Data Breach Notification policy has critical ethical implications. While it upgrades transparency and accountability, it additionally presents difficulties connected with false alarms, potential organizational burdens, and variations in jurisdictional approaches. Ethical principles of transparency, autonomy, and fairness should direct the implementation and evolution of this policy. Finding harmony between safeguarding individual rights and avoiding unnecessary burdens on organizations is significant for guaranteeing that cyber security policies align with ethical standards in our digital age.

References

Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. Science and Technology, 13(2), 29-35. https://www.researchgate.net/profile/Sasidhar-Duggineni/publication/372193665_Impact_of_Controls_on_Data_Integrity_and_Information_Systems/links/64a8d256b9ed6874a5046bc3/Impact-of-Controls-on-Data-Integrity-and-Information-Systems.pdf

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., ... & Jha, S. K. (2020). A survey of COVID-19 contact tracing apps. IEEE access, 8, 134577-134601. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9144194

Allen, F., Gu, X., & Jagtiani, J. (2021). A survey of fintech research and policy discussion. Review of Corporate Finance, 1, 259-339. https://www.gc.cuny.edu/sites/default/files/2021-07/wp20-21_1.pdf