Scientific Research Publishing

Voice of the Publisher, 2023, 9, 334-347
https://www.scirp.org/journal/vp
ISSN Online: 2380-7598
ISSN Print: 2380-7571

Breach Notification in the General Data Protection Regulation

M'Bia Hortense De-Yolande, Théo Doh-Djanhoundji, Gabo Yves Constant

Université Virtuelle de Côte d'Ivoire, Abidjan, Cote d'Ivoire
Email: deyolande.mbia@uvci.edu.ci, theodore.doh-djanhoundy@uvci.edu.ci, yvesconstantgabo@uvci.edu.ci

How to cite this paper: De-Yolande, M. H., Doh-Djanhoundji, T., & Constant, G. Y. (2023). Breach Notification in the General Data Protection Regulation. *Voice of the Publisher, 9,* 334-347.
https://doi.org/10.4236/vp.2023.94026

Received: September 12, 2023
Accepted: December 23, 2023
Published: December 26, 2023

Abstract

The EU General Data Protection Regulation (GDPR) introduced new standards for data breach notification. Articles 33 and 34 of the Regulation require that in the event of a data breach, the supervisory authority and data subjects must be informed. This paper discusses the European legal framework for data breach notification and its implications for organizations, data subjects, and supervisory authorities. By analyzing the main provisions, deadlines, and requirements of the Regulation, it examines the problems and possibilities of the data breach notification system provided for in the Regulation. It highlights the transformative impact of the breach notification provisions on data security, privacy, and liability. By examining breaches from the perspectives of legal obligations, organizational responsibilities, and individual and user rights, we aim to shed light on the complex dimensions of this critical element of data protection and its profound impact on data protection practices in the digital age. Ultimately, this study serves as a benchmark for the GDPR's breach notification provisions with the US California Consumer Protection Act and the Canadian Privacy and Electronic Documents Act. As technology continues to evolve with artificial intelligence, big data, blockchains, and the Internet of Things, new security gaps and data processing methods will emerge that will set new standards for data breach notification.

Keywords

GDPR, Breach Notification, Data Protection, Security, Privacy

1. Introduction

Enforced on May 25, 2018, the General Data Protection Regulation (hereinafter GDPR), is designed to harmonize data protection laws across EU member states and empower individuals with greater control over their data. The text introduced the obligation to notify a personal data breach (hereinafter "breach") to

the competent national supervisory authority (article 4 (21), GDPR) or, to the lead authority in the case of a cross-border breach. In certain cases, the person whose personal data were affected by the breach has to be informed. The GDPR provides for mandatory notification for all controllers unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Processors also have an important role to play and must notify their controllers of any breach (Article 33 (2)). The General Data Protection Regulation contains provisions on when and to whom a breach must be notified and what information must be provided as part of the notification. The information required for notification can be provided gradually, but in any case, controllers should respond to a breach in a timely manner.

Breach refers to a security incident that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data. Some key terms and concepts are related to breach notification under the GDPR such as personal data, supervisory authority, or data controller. Personal data breaches can have varying levels of impact, ranging from minor breaches with limited consequences to major breaches that may lead to significant risks to individuals' rights and freedoms.

Breaches that have far-reaching consequences for individuals, organizations, and society as a whole can be categorized according to three information security principles: breach of confidentiality, breach of integrity, and breach of availability (Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0 (European Data Protection Board, 2023)).

A breach of confidentiality occurs when personal data is disclosed or accessed without permission. An integrity breach occurs when personal data is inadvertently altered and an availability breach is referred to as the accidental or unauthorized loss of access to or destruction of personal data (European Data Protection Board, 2023).

Availability breach may not be so obvious compared to confidentiality and integrity, as a loss of availability occurs when data has been accidentally deleted or by an unauthorized person or, in the case of securely encrypted data, the decryption key has been lost. Permanent loss of availability occurs when the administrator cannot restore access to the data. Loss of availability may also occur if the normal functioning of the organization has been significantly disrupted, e.g. due to a power outage or denial of service attack (GDPR, Recitals 75 and 85).

Breaches can have significant adverse effects on individuals, organizations, and society as a whole which can result in physical, material, or non-material damage (Dhillon, 2015). More specifically, a data breach can be caused by specially developed malware that leads to millions of direct debits and credit cards being exposed. For example, in March 2021, Facebook lost 533 million user data from 106 countries that were published in a hacker forum. In March 2021, Facebook lost 533 million users records from 106 countries were posted onto a hacking forum. Likewise, Syniverse, which is part of the global telecommunica-

tions infrastructure company, also disclosed in a report to the US Securities and Exchange Commission (SEC) on 27 September 2021 that hackers had gained access to 500 million records (Komnenic, 2023). According to a report published by the Identity Theft Resource Center (ITRC), there were a record 1862 data breaches in the US in 2021. This number broke the previous record of 1506 set in 2017 and represented a 68% increase compared to the 1108 breaches in 2020 (Chin, 2023). This may include loss of control over their personal data, discrimination, identity theft or fraud, financial loss, unauthorized revocation of pseudonymization, and loss of confidentiality of personal data protected by professional secrecy.

The current study analyses breach notification provisions outlined in Articles 33 and 34. Chapter 1 emphasizes breach notification to the supervisory authority and data subjects. Chapter 2 discusses the responsibility and documenting breaches. The last chapter brings about a comparison between GDPR and California Consumer's Protection Act and Canada's PIPEDA framework pertaining to breach notification.

2. GDPR's Breach Notification Framework

Data breaches are closely linked to an interconnected world (Monsone, 2023). Therefore, the ability to combat the situation depends on whether regulators and governments can put in place rules stringent enough to reverse the trend. The GDPR, which is a comprehensive set of rules, introduced the obligation to notify a personal data breach to the competent national supervisory authority or, in the case of a cross-border breach, to the lead authority and, in certain cases, to notify individuals whose personal data has been affected by the breach. The GDPR also contains provisions on when and to whom a data breach must be reported and what information must be provided as part of the notification. The information required for notification may be provided in stages, but in any event, controllers must respond to any breach in a timely manner.

2.1. Notification to the Supervisory Authority

Under GDPR, controllers and processors have specific obligations when it comes to breach notification or when a personal data breach occurs. Here's an overview of their respective obligations:

Data controller's obligations

Article 33 emphasizes the prompt and transparent notification of breaches to supervisory authorities. Article 33 (1) of the GDPR requires controllers to notify supervisory authority about the breach within 72 hours unless the breach is likely to result in a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within that timeline, the reasons for the delay should be stated. When a physical or technical incident arrives, the ability to restore the availability of and access to personal data in a timely manner is essential.

The notification must therefore contain comprehensive and relevant details to enable the authorities to assess the situation and take appropriate action. Notification to the Supervisory authority should include the following information

- The nature of the breach.
- The categories and approximate number of persons and files involved.
- Contact information for the Data Protection Officer (if applicable) or other point of contact for further information.
- A description of the likely consequences of the breach.
- A description of the steps taken or proposed to be taken to address the breach, including any mitigation measures.

The supervisory authority shall have the right to request additional information from the controller on the infringement in order to assess the risks and consequences.

In the notification, the controller should describe the severity of the impact on the rights and freedoms of natural persons as a result of the unavailability of personal data.

However, depending on the circumstances, notification of the breach to the supervisory authority may or may not be required (European Data Protection Board, 2023). An example of a security breach is a temporary loss of availability that can later be restored, such as the case of infection by ransomware (malware that encrypts the data of the controller until a ransom is paid) ((Cybersecurity & Infrastructure Security Agency & MS-ISAC, 2020)).

If the controller fails to act in a timely manner and a breach is found to have occurred, this can be considered a failure to notify under Article 33 of the GDPR.

However, it would be a failure to comply with Article 33 of the GDPR if the controller fails to notify the breach to the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when choosing encryption software, operators should carefully consider the quality and correct implementation of the encryption offered and should also familiarise themselves with how their encryption product works. For example, a device may be encrypted when it is switched off, but not when it is in standby mode. Some products that use encryption have "default keys" that each customer must change in order to be effective.

Encryption may be considered sufficient by security experts at the moment, but obsolete in a few years, meaning it is questionable whether the data would be sufficiently encrypted by such a product and whether it would provide an adequate level of protection (European Data Protection Board, 2023).

Processor obligations

In the context of privacy, the processor shall assist the controller in complying with its obligations under Articles 32 to 36, taking into account the nature of the processing and the information available to the processor. Article 33 (2) of the GDPR explicitly provides that where a controller uses a processor and the pro-

cessor becomes aware that personal data processed on behalf of the controller have been compromised, the processor must notify the controller "without undue delay". The controller will use the processor to achieve its objectives because the processor must determine whether a breach has occurred and notify the controller. Thus, in theory, the controller should be considered to be "informed" if it receives information from the processor about the breach. This provision allows the controller to deal with the breach and to assess whether it is under an obligation to notify the supervisory authority under Article 33 (1) and whether it is under an obligation to notify data subjects under Article 34 (1).

The General Data Protection Regulation does not set a clear time limit within which the processor must notify the controller, but only states that the processor must do so "without undue delay". Processors are therefore invited to notify controllers without undue delay and to provide controllers with further information and details of the breach. This is essential for the controller to fulfill its obligation to notify the regulator within 72 hours. The contract between the controller and the processor should set out how the requirements of Article 33 (2) will be met, in addition to the other requirements of the GDPR. This may include a requirement for the processor to provide advance notice, which supports the controller's obligation to report to the Supervisory Authority within 72 hours. If the processor provides services to multiple controllers affected by the same event, the processor must report details of the event to each controller. Notifications may be made by the processor on behalf of the controller if the controller has given the processor appropriate authorization and is in accordance with the contractual arrangements between the controller and the processor. Such notifications must be made in accordance with Sections 33 and 34 of the GDPR. However, it is important to note that the controller remains legally responsible for providing the notification. The GDPR not only requires controllers to notify regulators of a breach but also mandates controllers to notify affected individuals of a breach.

2.2. Communicating the Breach to Data Subjects

If a personal data breach is likely to result in a high risk to individual rights, the GDPR requires the controller to communicate without undue delay, the incident to data subjects (Article 34). The notification to data subjects should explain the nature of the breach and the potential consequences, along with recommended measures to mitigate the risks (Article 34 (2)).

Therefore, communications to data subjects should include the following information.

- The nature of the data breach.
- The categories and approximate number of persons and records affected by the breach.
- The likely consequences of the breach.
- The measures taken or proposed to be taken to remedy the breach.

- Contact details where individuals can obtain further information and assistance.

However, communication with the data subject is not required in the following cases

- The controller has put in place appropriate technical and organizational safeguards to prevent unauthorized access to the data (e.g. encryption).
- The rights and freedoms of the individual are no longer at risk because appropriate measures have been taken before an unauthorized person gained access to the data.
- Immediately after the data breach occurred, the controller took measures to ensure that there was no longer a high risk to the rights and freedoms of individuals.

In principle, the relevant breach should be communicated to the affected data subjects directly. However, in some cases, a public communication or similar measure is more appropriate in order to avoid any disproportionate effort (Article 34 (3) (c) GDPR). In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand to those individuals who may have been affected by a breach.

Overall, Article 34 reflects the GDPR's commitment to ensuring that individuals' rights are respected and that they are informed about breaches that could affect their data, enabling them to make informed decisions and take appropriate steps to safeguard their privacy and security.

If a controller decides not to communicate a breach to the affected individual, Article 34 (4) GDPR explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34 (3) GDPR have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

Overall, individuals' or data subjects' rights to be informed are a key aspect of data protection regulations like the GDPR. This right emphasizes transparency in how organizations collect, process, and handle individuals' data. The right to be informed requires organizations to provide clear, constant, concise, and easily understandable information to data subjects about how their data will be used. This information should be provided at the time of data collection and when significant changes occur in data processing practices. In summary, the data subject's right to be informed underscores the importance of transparency in data processing practices. By providing clear and accessible information, organizations not only comply with legal requirements but also build trust, empower data subjects, and contribute to a culture of responsible data handling.

3. Accountability and Record Keeping

One of the requirements of the GDPR is to document data breaches regardless of

whether the supervisory authority is aware of them. This chapter discusses the documentation of a data breach, the role of the data protection officer, and the consequences of failing to comply with the obligations to notify data breaches.

3.1. Breaches Documentation

Article 33 (5) of the GDPR requires data controllers to keep records of personal data breaches. Supervisory authorities are therefore entitled to request access to the logs in order to assess compliance with the law. It is therefore recommended that controllers keep internal records of all breaches. Article 33 (5) sets out the information to be provided in the register.

- Reason for the infringement.
- The personal data concerned.
- The effects and consequences of the breach.
- The measures taken by the controller.

However, as the GDPR does not specify a retention period for such records, the controller must determine the appropriate period to meet the requirements of Article 33 (5) of the GDPR. Indeed, the controller may be required to provide the supervisory authority with evidence of compliance with the law in relation to notification. Obviously, if the file does not contain personal data, the data retention limitation principle of the GDPR does not apply, otherwise it must be taken into account. In particular, where a breach is not notified, the justification for this decision must be documented, including the reasons why the controller considers that the breach is unlikely to result in a risk to the rights and freedoms of individuals. Alternatively, if the controller considers that one of the conditions of Article 34 (3) of the GDPR is met, the controller must be able to provide sufficient evidence.

Where a controller notifies a supervisory authority of a security breach, but the notification is delayed, the controller should be able to justify the delay; documenting this can help demonstrate that the delay in notification is not unreasonable. Notices to notify affected individuals of a breach should be made in a transparent, effective, and timely manner. In order to comply with Articles 33 and 34 of the GDPR, the procedures to be followed after a breach should be defined, including the methods for breach containment, management and remediation, risk assessment, and breach notification. Establishing a documented notification procedure will benefit both management and processors. In this regard, it is also helpful to demonstrate that employees are aware of the existence of these procedures and mechanisms and know to respond to a breach to demonstrate GDPR compliance. As a result, supervisory authorities can exercise their powers (Article 58 GDPR) or impose fines (Article 83 GDPR) if breaches are not properly documented.

3.2 Role of the Data Protection Officer

The data protection officer plays a key role in preventing or preparing for a data

breach. Both the controller and the processor may have a data protection officer in accordance with the requirements of Article 37 of the GDPR or for good practice. Article 39 of the GDPR sets out the mandatory tasks of the data protection officer but does not prevent the controller from assigning other tasks where necessary.

The mandatory tasks of the data protection officer, in particular with regard to data breach notification, include, inter alia, providing data protection advice and information to the controller or processor, and providing advice, and monitoring compliance with the regulation. The DPO will also cooperate with the supervisory authority and act as a contact point for the supervisory authority and data subjects. When notifying a data breach to the supervisory authority, Article 33 (3) (b) of the GDPR requires the controller to provide the name and contact details of the data protection officer or another point of contact. As regards the documentation of breaches, the controller or processor may wish to obtain the opinion of his or her DPO as to the structure, establishment, and administration of this documentation, as the DPO could also be additionally responsible for maintaining such records. These factors mean that the DPO has an essential role to play in assisting in the prevention or preparation of a breach by advising and monitoring compliance, as well as during a breach. It plays a cross-cutting role that enables it to mitigate the risks of a breach.

3.3. Discussion of Potential Penalties for Non-Compliance with Breach Notification Obligations

As a consequence of the above developments, all appropriate technical protection and organizational measures should be taken to establish without delay whether a personal data breach has occurred and to inform without delay the supervisory authority and the data subject or data subject. The fact that the notification has been made without undue delay should be established taking into account in particular the nature and seriousness of the personal data breach and its consequences and adverse effects on the data subject. Such notification may lead to the intervention of the supervisory authority in accordance with its tasks and powers under the General Data Protection Regulation. If the requirements of Articles 33 and/or 34 of the GDPR are met and the controller fails to notify the breach to the supervisory authority or the data subject, or both, the supervisory authority is faced with the decision to consider all available remedies. These remedies include the imposition of an appropriate fine, which may be imposed together with a corrective measure (Article 58 (2) of the GDPR) or on its own. If a fine is imposed, it can be up to €10,000,000 or up to 2 percent of its annual worldwide turnover (Article 83 (4) (a) GDPR).

In some cases, failure to report a breach may reveal the absence or inadequacy of existing security measures. The supervisory authority also has the possibility to sanction both the failure to notify the breach (Articles 33 and 34 of the GDPR) and the lack of security measures under Article 32 of the GDPR.

As we can notice, the GDPR introduces significant fines for non-compliance with breach notification obligations under the elaborate provisions. The severity of the fines depends on the nature of the breach and the extent of non-compliance. Organizations can be fined up to €10 million or 2% of their global annual turnover, whichever is higher, for breaches related to inadequate breach notification. For more severe violations, such as failing to notify affected individuals or supervisory authorities when required, organizations can face fines of up to €20 million or 4% of their global annual turnover, whichever is higher. Different countries and regions have their own data protection regulations with varying penalties for breach notification non-compliance. The extraterritorial nature of the GDPR makes this fine applicable both within Europe and abroad for European companies that are based in other countries. Penalties can include fines, enforcement orders, injunctions, and even criminal charges in some cases. In summary, the potential penalties for non-compliance with breach notification obligations extend beyond financial fines. Compliance with breach notification requirements is not only essential for regulatory adherence but also for maintaining a positive reputation, fostering customer loyalty, and minimizing legal and financial risks.

4. GDPR Breach Notification Standards and Other Legal Instruments

This section discusses other practices and analyses possible future developments in the area of data breach notification. The General Data Protection Regulation (GDPR) is one of the most comprehensive pieces of legislation, but other pieces of legislation also contain important requirements for data breach notification. Here, we compare the GDPR's provisions with the data breach standards of two other important frameworks: the reformed California Consumer Protection Act (CCPA) and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) (Department of Justice, 2023).

4.1. Breach Notification Obligations under CCPA and PIPEDA

The California Consumer Protection Act (CCPA), passed on 1 January 2020, and the Personal Information Protection and Electronic Documents Act (PIPEDA) (Department of Justice, 2023), coming into force on 22 September 2022, focus on personal data and apply to organizations doing business in California and Canada. These two bills set out a set of consumer rights that require organizations to reassess their collection and use of personal data and change their business processes to comply with consumer rights. PIPEDA provides for mandatory reporting of data protection incidents where there is a "risk of serious harm" to an individual and requires private sector organizations to maintain a data protection incident register (Baker & MacKenzie, 2022). CCPA and PIPEDA have some similarities to the General Data Protection Regulation (GDPR), or it is GDPR that has similarities to one of the bills, however, there are also differences.

Similarities

- The GDPR, CCPA, and PIPEDA define personal data and data breach notification very broadly.
- These three laws expand the obligation to protect personal data to meet formal compliance requirements.
- The CCPA, PIPEDA, and GDPR allow for potentially high fines.
- The GDPR and PIPEDA require mandatory reporting of privacy incidents where there is a risk of a "serious infringement" of an individual's rights and require private sector organizations to keep records of privacy incidents.
- The GDPR and PIPEDA require notification of authorities, while the CCPA focuses on notifying affected individuals.

Under PIPEDA, an organization must notify the Office of the Privacy Commissioner and data subjects of any breach of the security of personal information under its control if, in the circumstances, the breach is likely to result in a real risk of significant harm to the individual. Although PIPEDA does not specify a particular time period within which the OPC must be notified of a breach, section 10.1 (2) of PIPEDA requires that the notification contain certain information and be made in a particular form and manner as soon as the organization becomes aware of the breach.

Differences

Unlike the GDPR, which repealed the EU Data Protection Directive, the CCPA does not repeal or replace existing data protection laws in California (such as the Whistleblower Act).

- Unlike the GDPR, the CCPA and PIPEDA are based on the individual's place of residence.
- The CCPA does not prohibit the processing of personal data by default.
- The GDPR and CCPA both emphasize immediate notification, with the GDPR requiring notification within 72 hours and the CCPA within 45 days. PIPEDA requires notification to take place "as soon as practicable" (10.1 (6)) after an organization becomes aware that a breach has occurred (Baker & McKenzie, 2022).
- CDPA does not include data minimization requirements.
- CCPA does not impose any data retention obligations on businesses, PIPEDA does.
- CDPA does not require the appointment of a data protection officer.
- CCPA does not create a right to rectification.
- CCPA does not create specific restrictions on international transfers.
- GDPR focuses on risks to the rights and freedoms of individuals. The CCPA requires notification on the basis of unauthorized access and specific types of personal data exposure. PIPEDA focuses on breaches that pose a risk of substantial harm.

To summarize, all three frameworks have a common goal, to promote transparency, accountability, and the protection of individuals' rights in the event of a

data breach. While they differ in terms of the triggering, timing, and scope of notifications, they together emphasize the importance of organizations taking responsible steps to inform affected individuals and regulators. Some countries, such as Brazil (LGPD) and India, have enacted data protection legislation similar to the GDPR, demonstrating the impact of the Regulation in shaping global data protection frameworks.

Breach notification plays a critical role in promoting public trust and compliance within the context of data protection regulations like the General Data Protection Regulation (GDPR). It fosters transparency, accountability, and responsible data handling, which are essential for maintaining a healthy relationship between organizations and their customers. By promptly informing affected individuals about a breach, organizations show that they value open communication and are willing to share information, even when incidents occur. This proactive approach minimizes the potential harm caused by the breach and signals to the public that the organization is taking immediate action to address the situation. By notifying affected individuals, they are empowered to take measures to protect themselves. This empowerment enhances individuals' trust in the organization's commitment to their well-being. Prompt breach notification allows individuals to take preventive actions, such as changing passwords or monitoring their accounts.

4.2. Possible Future Developments in Data Breach Notification

Data breach notification and data protection are likely to evolve in the future with advances in technology (Hadgis et al., 2022), changes to the legal framework, and increased public awareness. Many countries have been inspired by the GDPR while some are in the process of introducing data protection laws based on the regulation. This harmonization of global standards will have cross-border implications, as it will require companies to develop harmonized procedures for reporting data breaches. However, in a few years' time, these rules may no longer be in place and new rules or standards for data breach notification may be required.

As we are in an interconnected world, organizations will invest more in advanced technologies like artificial intelligence, machine learning, and behavioral analytics to prevent breaches and detect suspicious activities. Demand for privacy-enhancing technologies such as anonymization and data encryption will increase. Upgrading these technologies will have an impact on breach notification and risk assessment practices. Automation will also play a role in breach notification processes (Bykowski, 2022).

Tools for identifying affected individuals, generating notifications and managing responses are becoming increasingly sophisticated. Cybersecurity and privacy professionals must keep abreast of evolving breach notification practices, regulations, and technologies to effectively manage incidents. Collaboration between organizations, industries, and governments is essential to share threat in-

formation and best practices for breach response and notification.

The development of uniform data breach notification standards across countries can simplify the management of cross-border data breaches. The definition of "personal data" may evolve to include more types of data, leading to more comprehensive data breach notification obligations. Real-time data breach notification could become standard practice, allowing individuals to be notified immediately rather than within the 72 hours currently required by the GDPR.

Before the world copes with other realities, for now, more countries have adopted regulations inspired by GDPR rules, leading to a more harmonized global approach to breach notification and data protection.

Today's information-driven world requires the public and private sectors to work together to share threat intelligence, improve breach detection, and streamline reporting processes. Organizations could conduct thorough assessments to determine potential harm before notifying individuals, striking a balance between transparency and responsible disclosure.

As a preventive data protection solution, organizations could invest in educating consumers about data breach notification (Zanella, 2015) so that they understand their rights and can take appropriate action if their personal data is accessed without permission.

Regulatory frameworks could adapt more quickly to new technological developments to ensure that data breach notification requirements remain up to date. These possible changes reflect a dynamic situation where security breach notification practices are constantly evolving to adapt to evolving technology, regulation, public expectations, and consumer rights. Stakeholders who remain proactive and adaptive will be better able to cope with these changes and maintain their strong commitment to data protection and privacy.

Ultimately, strengthening accountability will require a holistic approach that includes not only technology and policy but also cultural change in the organization. By prioritizing these strategies, organizations can better protect sensitive data, demonstrate compliance with regulations such as the GDPR, and build trust with customers and stakeholders.

5. Conclusion

This study provides an in-depth analysis of the provisions on breach notification in Articles 33 and 34 of the GDPR. The study has examined the practical implications of these provisions, highlighted the obligations of controllers and processors through the data subject's right to information, and finally examined the notification rules under other legislation. Notification under the Data Protection Regulation has changed the data protection landscape by empowering individuals and requiring organizations to meet higher standards of data protection and has set a precedent for responsible and ethical data processing worldwide. It is important to recognize the continued relevance and evolution of these practices in the digital age. Breach notification practices are an important part of a re-

sponsible and ethical data management ecosystem. They emphasize transparency, accountability, and empowerment, and act as a bridge of trust between organizations and the individuals whose data they process.

The evolution of beach notification practices is closely linked to technological and regulatory developments. Thus, reporting practices must adapt to respond to new threats such as cyber-attacks (Li & Liu, 2021), new data breaches, AI-based attacks, and the evolution of big data. The global nature of data flows also underscores the need for uniform breach notification standards across jurisdictions. Collaboration between governments, industry, and international organizations is shaping the landscape of the future by promoting consistent and effective breach management practices. In our dynamic digital world, breach notification practices are a constant reminder that data protection is an ongoing effort, not a one-off endeavor (de Carvalho et al., 2020). By taking proactive measures, organizations can not only meet legal requirements but also their ethical responsibility to protect individuals' privacy. Collaboration between government, industry, and cybersecurity experts will play an important role in shaping breach notification practices and ensuring the protection of individuals' privacy. While data breach notification obligations pose challenges, they also provide an opportunity for organizations to improve their data protection practices, build trust among stakeholders, and demonstrate their commitment to protecting people's data.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Baker & MacKenzie (2023). *Global Data Privacy & Security Handbook. General Data Security Breach Notification Requirements.* https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/new-zealand/topics/general-data-security-breach-notification-requirements

Bykowski, K. (2022). *Automated Incident Responses: Everything You Need to Know.* https://swimlane.com/blog/automated-incident-response/

Chin, K. (2023). *Biggest Data Breaches in US History.* https://www.upguard.com/blog/biggest-data-breaches-us

Cybersecurity & Infrastructure Security Agency & MS-ISAC (2020). *Ransomeware Guide.* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

de Carvalho, R. M., Prete, C. D., Martin, Y. S. et al. (2020). Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects. *SN Computer Science, 1,* Article No. 217. https://doi.org/10.1007/s42979-020-00218-8

Department of Justice (2023). *Personal Information Protection and Electronic Documents Act (PIPEDA).* https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf

Dhillon, G. (2015). *The Changing Faces of Cybersecurity Governance. What to Do before and after a Cybersecurity Breach?* https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf

European Data Protection Board (2023). *Guidelines 9/2022 on Personal Data Breach Notification under GDPR.* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

Hadgis, K. M., Hirsch, W. R., Parks, G. T. et al. (2022). *Data Privacy: Evolving Updates to the Global Landscape.* https://www.morganlewis.com/pubs/2022/09/data-privacy-evolving-updates-to-the-global-landscape

Komnenic, M. (2023). *98 Biggest Data Breaches, Hacks, and Exposures.* https://termly.io/resources/articles/biggest-data-breaches/

Li, Y. C., & Liu, Q. H. (2021). A Comprehensive Review of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments. *Energy Reports, 7,* 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Monsone, F. (2023). *Five Years on: The Legacy of GDPR.* https://technative.io/five-years-on-the-legacy-of-gdpr/

Zanella, P. (2015). *Data Breach Legislation Calls for Increased Education.* https://www.zensar.com/about/pr-news/data-breach-legislation-calls-increased-education/